Contents

Navigating the administration interface ........................................... 10
  Common administration operations .............................................. 10
Setting up ...................................................................................... 13
  Initial configuration ..................................................................... 13
    Viewing or setting the appliance identification ......................... 13
    Viewing the appliance specification ......................................... 14
    Viewing network interface and routing settings ....................... 15
    Configuring name resolution settings ...................................... 16
    Configuring mail settings ....................................................... 16
    Modifying JVM settings ......................................................... 16
    Configuring a bonded NIC ...................................................... 17
    Changing the appliance IP address .......................................... 22
    Changing the appliance hostname .......................................... 26
    Localizing the appliance ....................................................... 29
    Configuring the appliance to use Tectia SSH and X.509 certificates .................................................................................. 31
    Configuring the banner color .................................................. 32
    Adding static routes .................................................................. 33
Managing standard data ................................................................. 34
  Setting up standard data categories .............................................. 34
    Viewing the standard categories .............................................. 34
  Compacting the datastore .......................................................... 41
    Running the utility .................................................................. 41
  Purging the history ...................................................................... 42
    The purge history script ........................................................ 42
    Purge process .......................................................................... 43
  Viewing the system taxonomy ...................................................... 43
    Viewing the system taxonomy ................................................ 44
    Storage and modification of the taxonomy ................................. 45
Users and security .......................................................................... 47
  Managing system users ............................................................... 47
    Enabling other users .............................................................. 47
    To enable other users ............................................................ 48
    Creating a new user ............................................................... 48
Amending a user's details ........................................ 49
Changing a user's password .................................. 49
Reactivating a user account .................................... 50
Deleting a user .................................................... 50
User permissions .................................................. 51
Managing groups .................................................... 51
Security groups ..................................................... 51
Listing all current groups ....................................... 52
Creating a new group ............................................ 52
Amending a group's details ..................................... 52
Deleting a group .................................................... 53
Group permissions ................................................. 53
System group permissions by category ....................... 55
Managing security policies ...................................... 67
Accounts and passwords ........................................ 67
Login page .......................................................... 68
UI security page – new in 8.3 SP2 ............................. 69
HTTPS configuration ............................................... 69
Generating a server key ......................................... 69
Uploading a server certificate ................................... 70
Self signing a server certificate ................................. 71
Uploading or downloading a CA certificate bundle ...... 71
Enabling or disabling HTTP and HTTPS access to the appliance .... 72
Managing LDAP ................................................... 72
LDAP Terms ........................................................ 73
Configuring LDAP ................................................ 74
LDAP group mapping ............................................. 76
Troubleshooting ..................................................... 77
Web authentication ............................................... 78
To configure the web authentication settings ............... 78
To configure RSA SecurID authentication (8.3 SP3 only) ... 79
Viewing active sessions .......................................... 81
Appliance audit ...................................................... 81
Reporting on audit events ....................................... 82
Event groups ......................................................... 83
Purging the audit Log .............................................. 83
Audit categories and events ........................................... 84

**Maintaining the appliance** ........................................ 90

Maintenance mode ....................................................... 90
  • Putting the appliance into maintenance mode ................. 90
  • Controlling the appliance ......................................... 91
Rebooting or shutting down the appliance .......................... 92
  • Controlling the appliance ......................................... 92
  • Disk space monitor ................................................. 93
Using appliance snapshot ............................................. 94
  • Archive disk space limit .......................................... 95
  • Creating a new appliance snapshot ............................... 95
  • Migrating your appliance snapshot to another appliance .... 96
Using appliance snapshot ............................................. 94
  • Archive disk space limit .......................................... 95
  • Creating a new appliance snapshot ............................... 95
  • Migrating your appliance snapshot to another appliance .... 96
Using the snapshot utility ............................................. 99
Baseline configuration .................................................. 100
  • Appliance Status Drop-down ..................................... 100
Configuring appliance status options ............................... 101
Configuring actions on changing appliance status ............... 102
Tripwire commissioning and configuration ......................... 106
Tripwire maintenance ................................................... 108
Configuring dependency visualizations ............................. 110
Notes: ........................................................................ 110
Structure of the file ....................................................... 110
Visualization definitions ............................................... 110
Dependency definitions .................................................. 112
Tooltip definitions ......................................................... 116
Configuring model maintenance settings ......................... 116
  • Modifying DDD, host, and software instance aging limits .... 118
  • When should DDD removal blackout windows be used? ....... 119
Configuring audit, snapshot and application options .............. 121
  • To set audit, snapshot and application options ............... 121
  • Visualization cache ................................................. 122
Configuring the NTP client ............................................. 123
  • Rebaseline the appliance after configuring the NTP client .... 124
Using command line utilities ........................................ 124
Duplicate or enhanced functionality in user interface ............. 126
Common options in the utilities ..................................... 126
tw_adduser ......................................................... 127
tw_baseline ......................................................... 128
tw_config_dashboards ............................................. 130
tw_convert_reports ............................................... 131
tw_cron_update ................................................... 132
tw_deluser ......................................................... 134
tw_disco_control .................................................. 135
tw_disco_exportPlatforms ........................................ 136
tw_disco_importPlatforms ........................................ 137
tw_ds_compact .................................................... 138
tw_excluderanges ............................................... 142
tw_imp_ciscoworks ................................................. 144
tw_imp_csv ......................................................... 146
tw_injectip ......................................................... 150
tw_listusers ....................................................... 153
tw_model_init ...................................................... 154
tw_passwd ......................................................... 155
tw_pattern_management ........................................... 156
tw_query ........................................................... 159
tw_reasoningstatus ............................................... 159
tw_remove_darkspace .............................................. 160
tw_scan_control ................................................... 162
tw_scheduled_snapshot ............................................ 166
tw_sign_winproxy_config ......................................... 168
tw_tax_export ...................................................... 169
tw_tax_import ...................................................... 170
tw_terminate_winproxy ............................................ 172
tw_tripwire_rebaseline ............................................ 173
tw_upduser ......................................................... 174

Discovery .......................................................... 176
Running discovery ................................................... 176
Controlling discovery ............................................... 176
Viewing discovery status .......................................... 181
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stalled discovery runs</td>
<td>184</td>
</tr>
<tr>
<td>Edge connectivity</td>
<td>186</td>
</tr>
<tr>
<td>Configuring discovery</td>
<td>188</td>
</tr>
<tr>
<td>To set Discovery Settings</td>
<td>188</td>
</tr>
<tr>
<td>Masking sensitive data</td>
<td>195</td>
</tr>
<tr>
<td>Setting up ports for OS fingerprinting</td>
<td>196</td>
</tr>
<tr>
<td>Managing the discovery platform scripts</td>
<td>197</td>
</tr>
<tr>
<td>Using scanner files</td>
<td>202</td>
</tr>
<tr>
<td>Adding privileged execution to commands</td>
<td>209</td>
</tr>
<tr>
<td>Extending discovery</td>
<td>217</td>
</tr>
<tr>
<td>Discovering mainframe computers</td>
<td>217</td>
</tr>
<tr>
<td>Extended discovery of IBMi</td>
<td>226</td>
</tr>
<tr>
<td>Extended discovery of Tomcat</td>
<td>226</td>
</tr>
<tr>
<td>Extended discovery of WebSphere</td>
<td>227</td>
</tr>
<tr>
<td>Extended discovery of WebLogic</td>
<td>230</td>
</tr>
<tr>
<td>Integrating with BMC Atrium Orchestrator</td>
<td>233</td>
</tr>
<tr>
<td>Power System discovery</td>
<td>235</td>
</tr>
<tr>
<td>Discovering VMware ESX and ESXi hosts</td>
<td>238</td>
</tr>
<tr>
<td>Improving discovery</td>
<td>242</td>
</tr>
<tr>
<td>Discovery Conditions</td>
<td>242</td>
</tr>
<tr>
<td>Credentials</td>
<td>244</td>
</tr>
<tr>
<td>About credential storage</td>
<td>245</td>
</tr>
<tr>
<td>User accounts on the target system</td>
<td>245</td>
</tr>
<tr>
<td>Device credentials</td>
<td>245</td>
</tr>
<tr>
<td>What is a Database Credential Group?</td>
<td>316</td>
</tr>
<tr>
<td>What is a Middleware Credential Group?</td>
<td>320</td>
</tr>
<tr>
<td>Management system credentials</td>
<td>321</td>
</tr>
<tr>
<td>Managing the credential vault</td>
<td>332</td>
</tr>
<tr>
<td>Monitoring credential usage</td>
<td>333</td>
</tr>
<tr>
<td>Consolidation</td>
<td>341</td>
</tr>
<tr>
<td>What is consolidated?</td>
<td>342</td>
</tr>
<tr>
<td>Configuring consolidation</td>
<td>342</td>
</tr>
<tr>
<td>When consolidation is running</td>
<td>344</td>
</tr>
<tr>
<td>Using appliance snapshot with consolidated appliances</td>
<td>345</td>
</tr>
<tr>
<td>Pattern management</td>
<td>346</td>
</tr>
<tr>
<td>Viewing details of all installed packages</td>
<td>347</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Uploading a TPL package to the appliance</td>
<td>347</td>
</tr>
<tr>
<td>Using pattern templates</td>
<td>348</td>
</tr>
<tr>
<td>Managing packages on the appliance</td>
<td>348</td>
</tr>
<tr>
<td>Pattern configuration and editing</td>
<td>350</td>
</tr>
<tr>
<td>Manual pattern execution</td>
<td>353</td>
</tr>
<tr>
<td>Template patterns</td>
<td>355</td>
</tr>
<tr>
<td>Technology Knowledge Update (TKU)</td>
<td>357</td>
</tr>
<tr>
<td>Uploading and activating a TKU</td>
<td>357</td>
</tr>
<tr>
<td>Integration points</td>
<td>359</td>
</tr>
<tr>
<td>What is an integration point?</td>
<td>359</td>
</tr>
<tr>
<td>Viewing integration points</td>
<td>359</td>
</tr>
<tr>
<td>Adding new JDBC drivers</td>
<td>362</td>
</tr>
<tr>
<td>Uploading new JDBC drivers</td>
<td>365</td>
</tr>
<tr>
<td>JDBC drivers</td>
<td>365</td>
</tr>
<tr>
<td>Importing data</td>
<td>369</td>
</tr>
<tr>
<td>Importing network device data</td>
<td>369</td>
</tr>
<tr>
<td>Importing data from CiscoWorks</td>
<td>369</td>
</tr>
<tr>
<td>Importing a CiscoWorks data file</td>
<td>370</td>
</tr>
<tr>
<td>Generating CiscoWorks data</td>
<td>370</td>
</tr>
<tr>
<td>Importing Hardware Reference Data</td>
<td>373</td>
</tr>
<tr>
<td>Importing a Hardware Reference Data file</td>
<td>373</td>
</tr>
<tr>
<td>Importing CSV data</td>
<td>374</td>
</tr>
<tr>
<td>Importing a CSV file</td>
<td>374</td>
</tr>
<tr>
<td>Notes on the CSV importer</td>
<td>376</td>
</tr>
<tr>
<td>CSV import examples</td>
<td>377</td>
</tr>
<tr>
<td>Context-sensitive reporting and linking</td>
<td>380</td>
</tr>
<tr>
<td>Configuring additional links</td>
<td>380</td>
</tr>
<tr>
<td>Configuration files</td>
<td>380</td>
</tr>
<tr>
<td>Link tags</td>
<td>381</td>
</tr>
<tr>
<td>Tags available</td>
<td>382</td>
</tr>
<tr>
<td>Example 00additional_links.xml file</td>
<td>384</td>
</tr>
<tr>
<td>Custom reporting</td>
<td>386</td>
</tr>
<tr>
<td>Configuration files</td>
<td>386</td>
</tr>
<tr>
<td>&lt;report&gt; elements</td>
<td>387</td>
</tr>
<tr>
<td>&lt;chart&gt; elements</td>
<td>391</td>
</tr>
<tr>
<td>&lt;chart-channel&gt; elements</td>
<td>392</td>
</tr>
</tbody>
</table>
The BMC Atrium Discovery Configuration Guide is intended for IT operations staff and managers who are using or setting up and managing BMC Atrium Discovery. It describes, for example, how to view details of your IT systems, both from an infrastructure and from a business perspective, how to add to and amend information in the database, and how to attach existing files to a data object (for example, for disaster recovery purposes).

<table>
<thead>
<tr>
<th>Goal</th>
<th>Related information</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure and update the BMC Atrium Discovery appliance.</td>
<td>Setting up</td>
<td>Be able to configure the appliance the first time you use it.</td>
</tr>
<tr>
<td>View standard data structures.</td>
<td>Managing standard data</td>
<td>Set up data specific to your organization (for example, add business information to the data automatically discovered by BMC Atrium Discovery).</td>
</tr>
<tr>
<td>Set up and configure system users, including creating new users, amending and deleting users and setting up passwords and security settings.</td>
<td>Users and security</td>
<td>Be able to quickly configure users and security settings to use in BMC Atrium Discovery.</td>
</tr>
<tr>
<td>Set up maintenance mode and take appliance snapshots or do command-line configuration.</td>
<td>Maintaining the appliance</td>
<td>Be able to configure the way the system is monitored and audited through the user interface or by using command line utilities.</td>
</tr>
<tr>
<td>Set up initial data and run the discovery process.</td>
<td>Discovery</td>
<td>Understand how to set up, run, and monitor the discovery process to optimize BMC Atrium Discovery in your environment.</td>
</tr>
<tr>
<td>Import data into BMC Atrium Discovery.</td>
<td>Importing data</td>
<td>Understand the import process, and how to exporting BMC Atrium Discovery data to other applications (for example, Microsoft Excel).</td>
</tr>
<tr>
<td>Run standard and customized reports.</td>
<td>Context-sensitive reporting and linking</td>
<td>Understand the reporting features of BMC Atrium Discovery and how to search for specific data to produce in reports.</td>
</tr>
</tbody>
</table>
Navigating the administration interface

The Administration page provides access to many commonly required setup operations. To access the Administration page, click Administration on the primary navigation bar. View-only tabs are also provided which enable you to view the current configuration of appliance identification, support information, software, hardware, network interfaces and routing.

Common administration operations

The Administration page is divided into the following sections:

- **Discovery**: provides links to the configuration and management pages for Discovery. The available links are:
  - Platforms: configure the commands used for each target operating system. This is described in Managing the discovery platform scripts.
  - SNMP Devices: view the network devices which can be discovered by BMC Atrium Discovery. This is described in Viewing SNMP devices.
  - Sensitive Data Filters: mask any sensitive data which may otherwise be seen in the command output. See Masking sensitive data.
  - Discovery Configuration: configure the Discovery process. This is described in Configuring discovery.
  - Discovery Consolidation: configure consolidation of discovery data between appliances. This is described in Consolidation.
  - Ciscoworks Import: import switch data from CiscoWorks. This is described in Importing network device data.
  - Vault Management: manage the Credential Vault. This is described in Managing the credential vault.
  - Credential Migration: migrate UNIX, Windows and SNMP credentials from a BMC Atrium Discovery 7.5 system to an 8.3 system. This is described in Migrating credentials.
  - Device Capture: capture an SNMP device using BMC Atrium Discovery to dump the MIB of an SNMP agent, which is then used to request that support be included in BMC Atrium Discovery for that SNMP device. This is described in Capturing SNMP devices.
- **Security**: provides links for the pages used to configure the security of the appliance and users. For more information, see Users and security.
  - Users: add, remove and modify users. This is described in Managing system users.
  - Groups: add, remove and modify groups. This is described in Managing groups.
  - Security Policy: configure the appliance security options. These are described in Managing security policies.
  - HTTPS: configure the HTTPS settings for the appliance. This is described in HTTPS configuration.
  - LDAP: view information about integrating BMC Atrium Discovery with LDAP. This is described in Managing LDAP.
  - Web Authentication: use Web Authentication plugins to authenticate user logins. This is described in Web authentication.
  - Active Sessions: view all users who are currently logged in. This is described in Viewing active sessions.
  - Audit: configure the appliance audit feature. This is described in Appliance audit.
- **Appliance**: provides links for the configuration pages for the appliance. The pages related to the initial set up of the appliance are described later in this section. These are:
  - Configuration: configure identification and network settings.
  - Control: restart services, reboot or shutdown appliance, and put appliance into maintenance mode. This is described in Maintaining the appliance.
  - Logs: manage logs and log levels. This is described in Log files.
  - Snapshot & Restore: operate the appliance snapshot and restore feature. This is described in Using appliance snapshot.
  - Baseline status: check and configure the appliance baseline. This is described in Baseline configuration.
  - Performance: view charts showing the appliance performance over the last 30 days. This is described in Appliance performance.
  - Support Services: create an archive of diagnostic information for customer support. This is described in Collecting additional data for support cases.
  - Miscellaneous: configure miscellaneous settings.
  - JDBC Drivers: configure JDBC drivers that are available for Database Discovery and for Export. This is described in Uploading new JDBC drivers.
- **Model**: provides links to the pages used to configure and maintain the model, and import and export data.
  - **View Taxonomy**: view the system taxonomy. This is described in [Viewing the system taxonomy](#).
  - **Model Maintenance**: configure model maintenance settings. This is described in [Configuring model maintenance settings](#).
  - **Custom Categories**: set up data categories. This is described in [Setting Up Standard Data Categories](#).
  - **CMDB Sync**: configure scheduled export synchronizations with BMC Atrium CMDB. This is described in [Preparing BMC Atrium CMDB for synchronization](#).
  - **Export**: Perform export functions. This is described in [Introduction to BMC Atrium Discovery Export](#).
  - **HRD Import**: import Hardware Reference Data. This is described in [HRD Import](#).
  - **Knowledge Update**: upload and install the latest Knowledge Update. This is described in [Uploading and activating a TKU](#) for more information.
  - **CSV Import**: import generic data in CSV format. This is described in [CSV Import](#).
  - **Application Mapping Import**: import application mapping definitions. This is described in [import application mapping definitions](#).
  - **Search Management**: view any search in progress, and depending on your privileges, cancel searches. This is described in [Using the Search Service](#).
  - **Channels**: manage existing channels and create new channels.
Setting up

This section details the configuration steps you perform after installing BMC Atrium Discovery and configuring the appliance for the first time.

- Initial configuration

Initial configuration

When you configure the system for the first time, you must set up the DNS server and enable the naming service. This ensures that BMC Atrium Discovery can resolve hostnames correctly. You can also configure mail settings to enable the appliance to send e-mail reports about the status of the appliance.

By default, the appliance uses DHCP to obtain an IP address. If you need to configure your appliance to use a static IP address, specify a hostname for it, or change localization settings you need to access the command line. For information on those tasks, see the following sections:

- Configuring a bonded NIC
- Changing the appliance IP address
- Changing the appliance hostname
- Localizing the appliance
- Configuring the appliance to use Tectia SSH and X.509 certificates
- Configuring the banner color
- Adding static routes

Viewing or setting the appliance identification

You can view or set details of the appliance identity, support information (displayed in the Help drop-down on each BMC Atrium Discovery page), and read-only information on the appliance software and hardware configuration. This includes information about whether the appliance is correctly specified for its intended use.

⚠️ Consolidation and Scanning Appliances

You cannot change the name of an appliance if it is configured as a consolidation or scanning appliance. See Consolidation for more information.

To view or edit the appliance identification:

1. Click Administration.
2. From the Appliance section, click **Configuration > Identification**.
   The Identification page displays details of the appliance identity, support information, software and hardware.

3. Edit the fields that you want to change.
   The following fields can be edited:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the appliance.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the appliance.</td>
</tr>
<tr>
<td>Admin Email</td>
<td>An e-mail address for the person or group responsible for the administration of the appliance.</td>
</tr>
<tr>
<td>Banner color</td>
<td>The color for the top banner in the user interface. Setting a banner color makes it easy for users in the field to identify the appliance they are using for various purposes (for example, development, test, and production environments). The appliance name is displayed on the colored banner. See <a href="#">Configuring the banner color</a> for more information.</td>
</tr>
<tr>
<td>Support URL</td>
<td>The URL to use in the help drop down.</td>
</tr>
<tr>
<td>Support URL Title</td>
<td>The title for the support URL.</td>
</tr>
<tr>
<td>Support URL Label</td>
<td>The label for the support URL.</td>
</tr>
<tr>
<td>Support URL Description</td>
<td>The descriptive text label for the support URL.</td>
</tr>
</tbody>
</table>

**Viewing the appliance specification**

From the user interface you can view the appliance specification table, which displays the amount of CPU, RAM, SWAP, and DISK resources used by various classes of appliance deployments (such as Proof of Concept, Baseline, Datacentre, and Consolidated Enterprise).

The appliance specification table is primarily aimed at Virtual Machine deployments of BMC Atrium Discovery and shows the minimum resources required for adequate performance. For installation on hardware platforms, which are generally intended for high performance or capacity deployments, or for consolidation appliances, a higher specification is recommended. See [Installing BMC Atrium Discovery](#) for more information.

To view the appliance specification:

1. Click **Administration**.
2. In the Appliance section, click **Configuration > Identification**.
   The Appliance Configuration page displays the following sections:
   - Appliance
   - Support
   - Software
   - Hardware

At the bottom of the Hardware section, the application specification table displays the number of discovered Operating System Instances, and the amount of processor, memory, swap space and filesystem resources detected. Also displayed is the threshold value of these parameters for each class of deployment.

![Application Specification Table](image)

If the appliance does not have sufficient resources for one or more classes of appliance deployment, the following types of messages are displayed:

- **Message at the top of the application specification table**: Specifies which resources do not meet the minimum resource specification. For example, if sufficient resource is not available for DISK, the warning message **Below minimum specification (Disk Capacity)** is displayed.
- **Warning message at the bottom of the application specification table**: Specifies that the appliance has insufficient resources and points to the documentation link for information about hardware specifications.

In the application specification table, the classes of the appliance deployment that do not meet the minimum hardware specification are highlighted in red. The classes of appliance deployment that meet or exceed the respective minimum hardware specification are highlighted in green.

See the **Configuring the Virtual Appliance** section for more information about classes of appliance deployment and related topics.

### Viewing network interface and routing settings

You can view details of the network interfaces and routing details configured on the appliance.

1. Click **Administration**.
2. From the Appliance section, click **Configuration > Interfaces & Routing**.
   The Interfaces & Routing page displays details of the configured interfaces and configured routes.
Configuring name resolution settings

1. Click Administration.
2. From the Appliance section, click Configuration > Name Resolution.
3. In Search, enter the name of the domain to be searched.
4. In Name Servers, enter the IP address of the name server.
   Multiple IP addresses can also be specified, separated by a space.
5. New in version 8.3 SP2. From the Time Out drop-down, select the required time out for DNS requests. This can be any value between 1 and 10 seconds. The default is 5 seconds. Larger values can affect Discovery performance and are not recommended.
6. New in version 8.3 SP2. From the Retries drop-down, select the required number of retries after DNS look up failure. This can be any value between 1 and 5. The default is 2. Larger values can affect Discovery performance and are not recommended.
7. Click Apply to save the changes.

Configuring mail settings

1. Click Administration.
2. From the Appliance section, click Configuration > Mail Settings.
3. Select Mail Enabled.
4. In From Address, enter the e-mail address used for sending e-mail.
5. In SMTP Server, enter the details of the SMTP server.
6. In SMTP Port, enter the SMTP port number.
7. If the SMTP server requires authentication, select Required in the Authentication section.
   Then enter the user name and password for the SMTP server.
8. Click Apply to save the changes.

⚠️ If you configure the appliance mail server settings for an invalid mail server, using mail.send() in a pattern introduces a delay of approximately three minutes while the appliance attempts to contact the SMTP server.

Modifying JVM settings

In some unusual situations, you might encounter errors caused by JVMs running out of memory. You can adjust the amount of memory allocated to individual JVMs up to a limit of 1024MB (the default value is 512MB). You should increase the JVM memory only if directed by Customer Support in response to errors.

1. Click Administration.
2. From the Appliance section, click **Configuration > JVM Settings**.
   The JVM Settings page lists the default and current values for the minimum and maximum memory settings for each JVM.
3. To adjust a setting, select the value from the menu in the Change To column, as shown in the following illustration.

   ![JVM Settings screenshot]

   **This diagram illustrates how to change the default JVM memory size up to a maximum of 1024 MB.**
4. Click **Apply**.
5. Restart the appliance.

### Configuring a bonded NIC

Network Interface Card (NIC) bonding (also known as *teaming*) enables you to join two NICs as a single physical device so that they appear as one interface. This is usually performed to provide failover capabilities or load balancing. Bonding can be configured on the BMC Atrium Discovery hardware appliance. It is not something that you should consider on a virtual appliance, because failover and load balancing should be provided by the virtualization platform.

#### Network configuration

When changing network configuration on your appliance, you should always be able to access the system console in case the new configuration does not work correctly.

#### Netadmin does not work with bonded NICs

If you configure your appliance to use bonded NICs, you can no longer use the **netadmin** user to perform any networking configuration.

The BMC Atrium Discovery appliance relies on `eth0` having an IP address. When the appliance starts, it requires an IP address on `eth0` for configuration and start-up services. In a default bonded NIC configuration, the IP address would be assigned to the bond point `bond0`, and the BMC Atrium Discovery services would be unable to start without additional configuration.
The `ifconfig` output for bonded NIC cards is shown in the following example. Note that `bond0` has an IP address but `eth0` and `eth1` do not.

```
bond0   Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
        inet addr:192.168.0.25 Bcast:192.168.0.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
        RX packets:58071 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1465 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:4315472 (4.1 Mb) TX bytes:120360 (117.5 Kb)
eth0    Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
        inet addr:192.168.0.25 Bcast:192.168.0.255 Mask:255.255.255.0
        UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
        RX packets:26447 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1262 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1992430 (1.9 Mb) TX bytes:95078 (92.8 Kb)
        Interrupt:16
eth1    Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
        inet addr:192.168.0.25 Bcast:192.168.0.255 Mask:255.255.255.0
        UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
        RX packets:31624 errors:0 dropped:0 overruns:0 frame:0
        TX packets:203 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2323042 (2.2 Mb) TX bytes:25282 (24.6 Kb)
        Interrupt:17
```

### Creating a bond point called `eth0`

To create a bond point called `eth0` you need to:

1. Configure the network interface scripts in `/etc/sysconfig/network-scripts` to force the hardware to bond to the names `eth1` and `eth2` using their MAC addresses. Note the "SLAVE=yes" and "MASTER=eth0" options.
2. Create the `eth0` interface which is actually assigned the IP configuration options.
3. Configure the boot process to include the bonding module and to use `eth0` as the bond point, with the various options associated with that bond.

To do this, log in as the tideway user and perform the following steps:

1. Stop the tideway, omniNames and appliance services. Enter:

   ```bash
   [tideway@localhost] $ sudo /sbin/service tideway stop
   [tideway@localhost] $ sudo /sbin/service omniNames stop
   [tideway@localhost] $ sudo /sbin/service appliance stop
   ```
2. Change to the `/etc/sysconfig/network-scripts` directory and determine the MAC addresses (`HWaddr`) of the network cards that you want to bond. Enter:

```
[tideway@localhost] $ cd /etc/sysconfig/network-scripts
[tideway@localhost network-scripts] $ /sbin/ifconfig -a | grep HWaddr
eth0      Link encap:Ethernet  HWaddr 00:11:43:FD:9A:B1
eth1      Link encap:Ethernet  HWaddr 00:11:43:FD:9A:B2
[tideway@localhost network-scripts] $
```

In this example the MAC Addresses are as follows:
- `eth0` – `00:11:43:FD:9A:B1`

3. Change to the root user and using a text editor, edit, or create and edit `ifcfg-eth1` to contain the following:

```
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:11:43:FD:9A:B1 # The MAC address of eth1 as determined in the previous step.
TYPE=Ethernet
MASTER=eth0
SLAVE=yes
```

4. Using a text editor, edit or create and edit `ifcfg-eth2` to contain the following:

```
DEVICE=eth2
BOOTPROTO=none
ONBOOT=yes
HWADDR=00:11:43:FD:9A:B2 # The MAC address of eth2 as determined in the previous step.
TYPE=Ethernet
MASTER=eth0
SLAVE=yes
```
5. Using a text editor, edit or create and edit ifcfg-eth0 to contain the following. Complete the IPADDR, NETMASK, and GATEWAY information

```
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
IPADDR=<required IP address>
NETMASK=<required netmask>
GATEWAY=<required gateway>
```

Note that options such as BROADCAST and NETWORK must be defined in ifcfg-eth0 if they are required.

6. Modify /etc/modprobe.conf. The lines that must be changed contain eth0 and possibly eth1. These need to be modified to specify that eth0 is now a bonded interface. For example, if the file looks like this:

```
alias eth0 e1000
alias eth1 e1000
alias scsi_hostadapter ata_piix
```

Depending on the options required, edit it to look like this:

```
alias eth0 bonding
options eth0 miimon=100 mode=balance-rr
alias scsi_hostadapter ata_piix
```

**Note**

The entries after options eth0 are the bonding options. They might not be required, or might be device specific, but the ones shown are good defaults. miimon=100 means check the link state every 100 milliseconds, and mode=balance-rr provides load balancing and tolerance. The balance-rr mode uses sequential order transmissions. There are other mode options available, some of which require changes to other items.

7. Reboot the system.
8. Log in as the tideway user and run the following command:

```
[tideway@localhost ] $ /sbin/ifconfig -a
```

The output should look like the following, note the **bond0** interface:

```
bond0  Link encap:Ethernet HWaddr 00:00:00:00:00:00
       inet addr:192.168.0.5  Bcast:192.168.0.255  Mask:255.255.255.0
       inet6 addr: fe80::250:56ff:fea7:362/64 Scope:Link
       UP BROADCAST MASTER MULTICAST  MTU:1500  Metric:1
       RX packets:0  errors:0  dropped:0  overruns:0  frame:0
       TX packets:0  errors:0  dropped:0  overruns:0  carrier:0
       collisions:0  txqueuelen:0
       RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
eth0  Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
       inet addr:192.168.0.5  Bcast:192.168.0.255  Mask:255.255.255.0
       inet6 addr: fe80::250:56ff:fea7:362/64 Scope:Link
       UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
       RX packets:21026 errors:0 dropped:0 overruns:0 frame:0
       TX packets:175 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0  txqueuelen:1000
       RX bytes:1405048 (1.3 MiB)  TX bytes:61541 (60.0 KiB)
eth1  Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
       UP BROADCAST RUNNING SLAVE  MULTICAST  MTU:1500  Metric:1
       RX packets:10529 errors:0 dropped:0 overruns:0 frame:0
       TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0  txqueuelen:1000
       RX bytes:703475 (686.9 KiB)  TX bytes:30280 (29.5 KiB)
eth2  Link encap:Ethernet HWaddr 00:11:43:FD:9A:B1
       UP BROADCAST RUNNING SLAVE  MULTICAST  MTU:1500  Metric:1
       RX packets:10498 errors:0 dropped:0 overruns:0 frame:0
       TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0  txqueuelen:1000
       RX bytes:701633 (685.1 KiB)  TX bytes:31793 (31.0 KiB)
```
9. Check `/var/log/messages` to check for a successful bonding:

```
Nov 18 15:47:18 localhost kernel: Ethernet Channel Bonding Driver: v3.4.0-1 (October
Nov 18 15:47:18 localhost kernel: bonding: MII link monitoring set to 100 ms
Nov 18 15:47:18 localhost kernel: bonding: eth0 is being created...
Nov 18 15:47:18 localhost kernel: bonding: MII link monitoring set to 100 ms
Nov 18 15:47:18 localhost kernel: bonding: eth0: enslaving eth1 as an active interface
Nov 18 15:47:18 localhost kernel: e1000: eth1 NIC Link is Up 1000 Mbps Full Duplex,
Nov 18 15:47:18 localhost kernel: bonding: eth0: link status definitely up for interface
Nov 18 15:47:18 localhost kernel: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Nov 18 15:47:18 localhost kernel: e1000: eth2 NIC Link is Up 1000 Mbps Full Duplex,
Nov 18 15:47:18 localhost kernel: bonding: eth0: enslaving eth2 as an active interface
```

The list of running kernel modules should include the `bonding` module.

10. Run the following command:

```
[tideway@localhost ] $ /sbin/lsmod | sort
ac                     38729  0
acpi_memhotplug        40517  0
asus_acpi              50917  0
ata_piix               57541  0
autofs4                63049  3
backlight              39873 1 video
battery                43849  0
*bonding               142537 0*
button                 40545  0
cdrom                  68713 1 ide_cd
crypto_api             42945 1 xfrm_nalgo
...                     
```

Changing the appliance IP address

⚠️ **The netadmin user is the preferred way of configuring networking**

The preferred way of administering any of the appliance network configuration is to use the `netadmin` user account. The netadmin user account enables you to change network, hostname and gateway settings without requiring root privileges. You can also use the netadmin user to reboot the appliance.

Setting a static IP address for the first interface (`eth0`) requires the following steps:
1. Obtain networking information.
2. Stop the tideway services
3. Edit the network configuration files.
4. Restart networking.
5. Restart the tideway services.

Obtaining networking information

You must obtain the following information before starting:

- IP Address: in this example 192.168.0.100
- Netmask: in this example 255.255.255.0
- Gateway: in this example 192.168.0.1

Consult your system administrator for this information.

Stopping the Tideway services

Before changing any networking configuration, you must stop the following services:

- tideway
- omniNames
- appliance

To do this, as the tideway user, enter the following:

```
[tideway@london01 ~]$ sudo /sbin/service tideway stop
[tideway@london01 ~]$ sudo /sbin/service omniNames stop
[tideway@london01 ~]$ sudo /sbin/service appliance stop
```

Editing the network configuration files

Edit Network Configuration Files Using the Console

Ensure you are on the console or have access to the console before making any networking changes.

The appliance is configured by default to use DHCP. To configure it to use a static IP address, you must edit the /etc/sysconfig/network-scripts/ifcfg-eth0 file as root. In addition to the network settings obtained previously, you need to determine the MAC address of the network card.

To do this:
1. Enter the following command:

```bash
[tideway@london01 ~]$ sudo /sbin/ifconfig eth0
eth0 Link encap:Ethernet HWaddr 00:0C:29:BB:34:6D
...
[tideway@london01 ~]$}
```

The MAC address is given after the heading `HWaddr`. In this example, the MAC address is `00:0C:29:BB:34:6D`.

The following example shows the default `ifcfg-eth0` file:

```ini
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

2. Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` and add the values obtained above. The file will look like this:

```ini
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:0C:29:BB:34:6D
TYPE=Ethernet
ONBOOT=yes
IPADDR=192.168.0.100
NETMASK=255.255.255.0
```

3. Add the gateway address to the `/etc/sysconfig/network` file.
   You can edit the appliance hostname, but you must ensure that it still resolves correctly. See Changing the appliance hostname for more information.

The file will look like this:

```ini
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=london01
GATEWAY=192.168.0.1
```
Restarting networking

You must restart networking to make sure that the changes have been applied correctly. To do this, enter:

```
[tideway@london01 ~]$ sudo /sbin/service network restart
[tideway@london01 ~]$
```

When networking starts, enter the following commands to ensure that the new networking information is showing correctly and that the appliance can resolve its own hostname correctly:

```
[tideway@london01 ~]$ /sbin/ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:0C:29:BB:34:6D
          inet addr:192.168.0.100 Bcast:192.168.0.255 Mask:255.255.255.0
... 
[tideway@london01 ~]$ ping `hostname`
PING london01 (192.168.0.100) 56(84) bytes of data.
64 bytes from london01 (192.168.0.100): icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from london01 (192.168.0.100): icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from london01 (192.168.0.100): icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from london01 (192.168.0.100): icmp_seq=4 ttl=64 time=0.041 ms
--- london01 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.041/0.045/0.050/0.003 ms
[tideway@london01 ~]$
```

If the appliance cannot resolve its own hostname (there is no response from the ping command), see Changing the appliance hostname for information on changing the hostname.

Restarting the Tideway services

The final test is to log in to the appliance user interface (UI) using a web browser. You can only do this after you have restarted the tideway services. Enter the following commands:

```
[tideway@london01 ~]$ sudo /sbin/service appliance start
[tideway@london01 ~]$ sudo /sbin/service omniNames start
[tideway@london01 ~]$ sudo /sbin/service tideway start
```

Next, attempt to log in to the appliance UI using a web browser.

Troubleshooting

If you cannot log in through a web browser, try stopping and restarting the services:
Try to ping the gateway or use traceroute to the gateway. In this example, 192.168.0.1 is the gateway address provided by your system administrator. Enter the following:

```
[tideway@london01 ~]$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=127 time=0.324 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=127 time=0.450 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=127 time=0.342 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=127 time=0.401 ms
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.324/0.379/0.450/0.051 ms
[tideway@london01 ~]$ traceroute 192.168.0.1
traceroute to 192.168.0.1 (192.168.0.1), 30 hops max, 40 byte packets
1  192.168.1.4 (192.168.1.4)  4.225 ms  4.377 ms  4.532 ms
2  192.168.0.1 (192.168.0.1)  0.265 ms  0.262 ms  0.252 ms
[tideway@london01 ~]$
```

If these tests fail, contact your system administrator.

### Changing the appliance hostname

⚠️ **The netadmin user is the preferred way of configuring networking**

The preferred way of administering any of the appliance network configuration is to use the netadmin user account. The netadmin user account enables you to change network, hostname and gateway settings without requiring root privileges. You can also use the netadmin user to reboot the appliance.

This section describes how to set the appliance hostname and to ensure that it is locally resolvable even if the IP address of the appliance changes.

You can set the hostname either locally, or using DHCP/DNS.
Setting the hostname locally

If you want the appliance to use the same hostname for all NICs, set the hostname in the /etc/sysconfig/network file.
If you want to use different hostnames for individual NICs, set the hostname in the /etc/sysconfig/network-scripts/ifcfg-ethX file. X is the number of the interface, for example eth0.

Add the following line to the file:

```
HOSTNAME=london01
```

where london01 is the new hostname.

If you do not have a DNS entry for the host, or you require a failsafe when DNS is unavailable, enter the hostname and FQDN in the etc/hosts file. Use the appliance's IP address if it is unlikely to change, or a loopback IP address other than 127.0.0.1 (which can interfere with the resolution of localhost and localdomain.

The following example uses london01 as the hostname, london.com as the domain name, and 192.168.0.100 as the IP address. Add only one of the example entries.

```
127.0.0.1           localhost.localdomain localhost
::1                 localhost6.localdomain6 localhost6

### Enter either this line if the IP address is known
192.168.0.100       london01.london.com london01

### Or this line to use a loopback address
127.0.0.2           london01.london.com london01
```

The following example uses the same host and domain names as above and shows commands to enter to ensure that the hostname is set correctly:
Setting the hostname using DHCP/DNS

Some networks are configured so that you can set your own hostname and update the DHCP and DNS servers accordingly.

To enable this for all NICs, set the `DHCP_HOSTNAME` in the `/etc/sysconfig/network` file.

To enable this for individual NICs, set the `DHCP_HOSTNAME` in the `/etc/sysconfig/network-scripts/ifcfg-ethX` file.

Where, `X` is the number of the interface. For example, `eth0`.

The following example uses `london01` as the hostname and `london.com` as the domain name.

```
DHCP_HOSTNAME=london01.london.com
```

When the appliance renews its IP address with the DHCP server, the DHCP server will also update the DNS server with the hostname and IP address of the appliance.

Diagnosing hostname problems

Some issues are indicative of incorrectly configured hostnames.

Visualizations and export do not display

This problem can be identified if you see a 500 Error - Internal Server Error! page in the user interface (UI) when attempting to load visualizations. You will also see the following error message in `$TIDEWAY/tomcat/logs/catalina.out`:
java.net.UnknownHostException: local_hostname: local_hostname

where, local_hostname is the hostname set on the machine.

To resolve this problem, see the previous section, Setting the hostname locally.

Cannot access the UI – 500 internal server error

This error can have many causes, as it results from one or more of the tideway services failing to start. A common cause however is that localhost cannot be resolved. If this is the case errors of the following form are displayed when restarting the tideway services.

[current date/time] [error] couldn't resolve WKServer address
[current date/time] [error] Couldn't resolve hostname for WebKit Server

Localizing the appliance

This section describes setting localization options such as the keyboard layout and the timezone. The UI however cannot be localized.

Setting the keyboard layout

The console keyboard layout can be temporarily changed using the loadkeys command to test that a keyboard layout works correctly.

To change the keyboard layout to a US layout, enter the following command:

[tideway@london01 ~]$ loadkeys us
[tideway@london01 ~]$ 

To change the keyboard layout to a UK layout, enter the following command:

[tideway@london01 ~]$ loadkeys uk
[tideway@london01 ~]$ 

After you have determined that the layout works correctly, you should make the change permanent. To do so, change the KEYTABLE, MODEL, and LAYOUT variables in the /etc/sysconfig/keyboard file. For example, to change the keyboard layout to a US layout, use the following:
The keyboard mapping files can be found in /lib/kbd/keymaps/i386/ but usually you can use the 2-letter ISO Country Code. See the ISO website to find the code for the country you require. For example, us (United States), uk (United Kingdom), de (Germany), and no (Norway).

Setting the system timezone

The system-wide timezone in Linux is defined by the files /etc/sysconfig/clock and /etc/localtime.

The file /etc/sysconfig/clock is used by the system during upgrades to ensure that /etc/localtime references the latest information. The ZONE value in /etc/sysconfig/clock must reference one of the timezone data files in /usr/share/zoneinfo/. These files contain all the timezone and daylight savings rules for a particular location (for example, /usr/share/zoneinfo/Europe/London contains all the data for London). These files are part of the base packages installed by the system (they are from the tzdata package in RHEL and Fedora).

The file /etc/localtime is either a copy of or a link to one of the timezone data files in /usr/share/zoneinfo/.

To set the timezone, as the root user, update the value of ZONE in /etc/sysconfig/clock and copy or link the relevant file from /usr/share/zoneinfo to /etc/localtime. You must restart the tideway service to bring the timezone change into effect. For example, to set the time to New York time:

```
[root@london01 ~] mv /etc/sysconfig/clock /etc/sysconfig/clock.old
[root@london01 ~] sed -e s/ZONE="[^"]*"/ZONE="US\//Eastern"/ /etc/sysconfig/clock
[root@london01 ~] mv /etc/localtime /etc/localtime.old
[root@london01 ~] ln -s /usr/share/zoneinfo/US/Eastern /etc/localtime
[root@london01 ~] /sbin/service tideway restart
```

Setting the system time

You can set the time using the date command. For example, to set the current date to ten past twelve on 4 July 2013, enter the following command:

```
date +"%Y-%m-%d\t%r"
```

It will output something like:

```
2013-07-04 10:12:00
```
1. [root@london01 ~]$ date -s "12:10:00 20130704"
Thu Jul  4 12:10:00 BST 2013
[root@london01 ~]$

The format for the date string is **HH:MM:SS YYYYMMDD**.

You can also configure the appliance to synchronize the internal clock to an ntp server. See Configuring the NTP Client for more information.

**Do not change the appliance time on to an earlier setting**

After BMC Atrium Discovery has been running and has created nodes in the datastore, you must not change the time to an earlier setting. The transaction scheme in the datastore is based on timestamps and setting an earlier time makes data appear out of date causing many transactions to fail.

Configuring the appliance to use Tectia SSH and X.509 certificates

The appliance can be configured to use Tectia SSH and x.509 certificates, as described in the following sections. These procedures assume that you have administrator level knowledge of Tectia SSH, and a Tectia SSH server installed on your network.

**Installing and configuring the Tectia SSH client**

Install the Tectia SSH client as described in the Tectia installation guide.

After you have installed and configured the client for the tideway user, you should able to access remote servers using sshg3 from the command line, though you may need to add /opt/tectia/bin to the PATH. You should test servers that require X.509 certificates and those that do not, if possible.

**Configuring discovery to use the Tectia SSH client**

To configure Discovery to use the Tectia SSH client:

1. Create a .tideway.py file in /usr/tideway and add the following entry:

   ```python
   SSH_CMD="/opt/tectia/bin/sshg3"
   ```
2. Restart the Tideway services.
   You will see deprecation warnings in the logs about use of the `tideway.py` file but you can ignore them.

Discovery will now use Tectia SSH instead of OpenSSH for connections to remote systems.

**Configuring the banner color**

You can set the color for the top banner in the user interface, making it easy for users in the field to identify, through a visual cue in a prominent banner, the appliance they are using for various purposes (for example, development, test, and production environments).

To configure the banner color:

1. On the **Administration** tab, click **Configuration** in the Appliance section.
2. In the Banner Colour section, select the option button corresponding to the color you want to display in the banner and click **Apply**.

![Banner Colour palette](image)

This screen illustrates the Banner Colour palette that enables you to select one of the default colors.

3. In the Name field, type a name that you want to display overlaying the colored banner.
   The selected banner color with the specified name persists so that all pages that you display in the user interface use the same scheme. The banner color also displays on the login page.

![Banner with specified name](image)

This screen illustrates the selected banner color and name persisting to another selected page in the user interface.
Adding static routes

Adding static routes to the BMC Atrium Discovery server is necessary only in rare occasions. Routing is configured on routing devices, therefore it should not be necessary to configure static routes on Red Hat Enterprise Linux servers or clients. However, if you require this type of configuration you can store the routes in a `/etc/sysconfig/network-scripts/route-interface` file. Static routes should only be configured for other subnets.

For example, static routes for the `eth0` interface would be stored in the file `/etc/sysconfig/network-scripts/route-eth0` with a format similar to the following:

```
ADDRESS0=137.72.95.60
NETMASK0=255.255.255.255
GATEWAY0=137.72.92.65
ADDRESS1=137.72.96.0
NETMASK1=255.255.255.0
GATEWAY1=137.72.92.65
```

In this example, two static routes are added to the IP 137.72.95.60, and network 137.72.96.0/24 to the gateway GATEWAY1=137.72.92.65.

Duplicate default gateways

If the default gateway is already assigned from DHCP, the IP command arguments format can cause one of two errors during start-up. These errors can also occur if you have another route to another network using the default gateway. The errors are safe to ignore.

For more information on configuring static routes, see the Red Hat Linux documentation. Further, you should take into consideration the warnings regarding support of OS customizations to your appliance.
Managing standard data

This section explains how to set up and view standard data on the BMC Atrium Discovery system. You must set up details of the specific data required by your IT/IS organization, such as the locations, product groupings, and status values that you use. Known as standard data categories, they are typically set up at initial deployment, but you can change them later if necessary. Additional standard data that you can view from the Setup menu includes the datastore partitions (discrete areas of data in the datastore) and the system taxonomy, which includes details of all the kinds of data object in the BMC Atrium Discovery system and the relationships between them.

- Setting up standard data categories
- Compacting the datastore
- Purging the history
- Viewing the system taxonomy

Setting up standard data categories

The standard data categories define areas of basic data, specific to your organization, that cannot be obtained from data discovery. This includes the locations, product groupings, status values and so on that are relevant to your organization. You would normally set up all this data when the system is first configured for your organization, but you can update it at any time if required.

Viewing the standard categories

To view the standard data categories, click the Custom Categories icon in the Model section of the Administration tab. The Custom Categories page is displayed.

Accessing data in the standard categories

1. The Custom Categories page shows tabs representing the categories of data that you can manage.
2. Click the category tab for the data that you want to view, create or edit. The categories are:

<table>
<thead>
<tr>
<th>Category</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttachmentCategory</td>
<td>Groupings of files attached to objects. See #Managing attachment categories.</td>
</tr>
<tr>
<td>Family</td>
<td>Groupings of Business Application Instances that are specific to your organization. See #Managing product families.</td>
</tr>
<tr>
<td>Lifecycle Status</td>
<td>Status values that can be associated with the IT components managed in your organization. See #Managing lifecycle status values.</td>
</tr>
<tr>
<td>Location</td>
<td>Physical locations in your organization which can be associated with a managed element or a person. See #Managing locations.</td>
</tr>
<tr>
<td>Organisational Unit</td>
<td>Logical divisions of your organization, such as a department or a business unit in your organization. See #Managing organisational units.</td>
</tr>
<tr>
<td>Recovery Time</td>
<td>Valid recovery times that can be applied to the IT components that can be managed in your organization. See #Managing recovery time values.</td>
</tr>
</tbody>
</table>

Each tab for the standard data shows the data types that are configured on the appliance, along with abbreviations, descriptions, whether that type is active or not, arrow keys to reorder the types, whether the type is standard in BMC Atrium Discovery or user defined, and a Delete button to delete that data type. The page also has a New button which enables you to create a new type, depending on the page you are viewing.

Managing attachment categories

BMC Atrium Discovery users can associate any file - such as a document, a spreadsheet, or a diagram - with an object in the BMC Atrium Discovery datastore in order to provide additional information. You can associate an attachment with a Software Instance, Business Application Instance, or Host. Files can be of any type and are not validated in any way by the BMC Atrium Discovery system. Attached files are uploaded to the BMC Atrium Discovery datastore so that they can be accessed easily for disaster recovery purposes.

When you select the Attachment Category page all existing categories are listed. From this page you can create a new category or display an existing one in detail.

Creating a new attachment category

1. From the Custom Categories page, select the Attachment Category tab. The existing attachment categories are displayed.
2. Click the New Attachment Category button. The Create Attachment Category page is displayed.
3. Complete the details of the attachment category.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of attachment category.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviation of category name.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of attachment category.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this category is currently active, No if it is not active.</td>
</tr>
<tr>
<td>Attachments</td>
<td>Relationship that defines the actual attachment objects in this category. This information is normally set up when the documents are attached to the objects, but you can search for and select one or more Attachment objects.</td>
</tr>
</tbody>
</table>

4. Click Apply to save the attachment category details.

**Viewing details of an attachment category**

1. From the Custom Categories page, select the Attachment Category tab. The existing attachment categories are displayed.
2. Click an entry to display the View Object page showing full details of the selected category.
   - To delete the selected category, click Delete.
   - To view audit details of the category, click History.

From the Attachment Category you can also view relevant attachments.

**Managing product families**

Product Families define the groupings of Business Application Instances that are specific to your organization.

When you select the Product Family page all existing families are listed. From this page you can create a new family or display an existing one in detail.

**Creating a new product family**

1. From the Custom Categories page, select the Families tab. The existing families are displayed.
2. Click New Family button. The Create Family page is displayed.
3. Complete the Attributes and Relationships of the product family.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of product family.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviation of product family name.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of product family.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this product family is currently active, No if it is not active. Defaults to Yes.</td>
</tr>
<tr>
<td>Standard</td>
<td>Yes if this product family is standard in your organization; No if it is not active. Defaults to Yes.</td>
</tr>
<tr>
<td>Applications in Family</td>
<td>Relationship that defines the Business Applications that are included in this product family. This information is normally set up when you set up the Business Applications, or can be set by a pattern, or you can search for and select one or more applications from here.</td>
</tr>
<tr>
<td>Family Owner</td>
<td>Relationship that defines the ownership of this product family. Search for and select the appropriate Person.</td>
</tr>
</tbody>
</table>

Click Apply to save the product family details.

4. Click Apply to save the product family details.

**Viewing details of a product family**

1. From the Custom Categories page, select the Families tab. The existing families are displayed.
2. Click an entry to display the View Object page showing full details of the selected family.
   - To delete the selected family, click Delete.
   - To view audit details of the family, click History.

**Managing lifecycle status values**

A lifecycle status object defines a specific status value that can be applied to the IT components managed in your organization. You can assign a status value to each managed element (for instance, each Software Product, Business Application Instance and Host).

You would normally set up all the lifecycle status values appropriate to your organization when you first set up the system, but you can update them at any time.

From the Lifecycle Status page all lifecycle status values are listed. From this page you can create a new lifecycle status or display an existing one in detail.

**Creating a new lifecycle status value**

1. From the Custom Categories page, select the Lifecycle Status tab. Existing lifecycle status values are displayed.
2. Click New Lifecycle Status button. The Create Lifecycle Status page is displayed.
3. Complete the Attributes and Relationships of the host type.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this lifecycle status value.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviated life-cycle status name.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of life-cycle status.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this lifecycle status is currently active, No if it is not active. Defaults to Yes.</td>
</tr>
<tr>
<td>Withdrawn State?</td>
<td>Yes if this lifecycle status value is Withdrawn, No if it is not. Defaults to No.</td>
</tr>
</tbody>
</table>

4. Complete the Relationships of the lifecycle status.

5. Click Apply to save the lifecycle status details.

**Viewing details of a lifecycle status**

1. From the Custom Categories page, select the Lifecycle Status tab. Existing lifecycle status values are displayed.
2. Click an entry to display the View Object page showing full details of the selected lifecycle status.
   - To delete the selected lifecycle status, click Delete.
   - To view audit details of the lifecycle status, click History.

**Managing locations**

A Location object defines a physical location in your organization which can be associated with a managed element or a person. You can create various levels of locations - for example, you can model buildings in sites, or rooms on floors.

You would normally set up all the location values appropriate to your organization when you first set up the system, however, you can update them at any time.

If you need to link locations to other nodes, you can do this by means of patterns. A template pattern is available to do this. For information on template patterns, see Template patterns. For information on modeling your business applications using patterns, see the Tideway web site and click the Community tab and follow the Documentation Resources link.

From the Location page all locations are listed. From this page you can create a new location or display an existing one in detail.

**Creating a new location**

1. From the Custom Categories page, select the Locations tab. Existing location values are displayed.
2. Click New Location. The Create Location page is displayed.
3. Complete the Attributes and Relationships of the location.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of location.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviated name of location.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of location.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this location is currently active, No if it is not active. Defaults to Yes.</td>
</tr>
<tr>
<td>Type</td>
<td>Select type of location (Major or Minor) from drop-down list.</td>
</tr>
<tr>
<td>Address</td>
<td>Address of location.</td>
</tr>
<tr>
<td>Phone</td>
<td>Telephone number of this location.</td>
</tr>
<tr>
<td>Subsidiary Locations</td>
<td>Relationship that defines other locations that are subsidiary to this one. Search for and select one or more locations.</td>
</tr>
<tr>
<td>Parent Location</td>
<td>Relationship that defines the parent location of this one. Search for and select the appropriate location.</td>
</tr>
<tr>
<td>Hosts at this Location</td>
<td>Relationship that defines the host systems that are in this location. Can be set by a pattern, or you can search for and select one or more hosts.</td>
</tr>
<tr>
<td>Subnets at this Location</td>
<td>Relationship that defines the subnets that are in this location. Can be set by a pattern, or you can search for and select one or more subnets.</td>
</tr>
<tr>
<td>Applications at this Location</td>
<td>Defines instances of Business Applications in this physical location. Search for and select one or more applications.</td>
</tr>
</tbody>
</table>

4. Click Apply to save the location details.

Viewing details of a location

1. From the Custom Categories page, select the Locations tab. Existing location values are displayed.
2. Click an entry to display the View Object page showing full details of the selected locations.
   - To delete the selected location, click Delete.
   - To view audit details of the location, click History.

Managing organizational units

An Organizational Unit object defines a logical division of your organization, such as a department or a business unit in your organization. You can create various levels of organizational unit - for example, you can model teams in functional areas. Managed elements in your organization (Software Product, Business Application and Host) can be associated with particular organizational units.

From the Organisational Unit page all organizational units are listed. From this page you can create a new organizational unit or display an existing one in detail.
Creating a new organisational unit

1. From the Custom Categories page, select the Organisational Units tab. Existing organizational units are displayed.
2. Click New OrganisationalUnit. The Create Organisational Unit page is displayed.
3. Complete the Attributes and Relationships of the organizational unit.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of organizational unit.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviated form of organizational unit name.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of organizational unit.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this organizational unit is currently active, No if it is not active. Defaults to Yes.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of organizational unit.</td>
</tr>
<tr>
<td>Subsidiary Units</td>
<td>Relationship that defines other organizational units that are subsidiary to this one. Search for and select one or more organizational units.</td>
</tr>
<tr>
<td>Parent Unit</td>
<td>Relationship that defines the parent organizational units of this one. Search for and select the appropriate organizational unit.</td>
</tr>
</tbody>
</table>

4. Click Apply to save the organizational unit details.

Viewing details of an organizational unit

1. From the Custom Categories page, select the Organisational Units tab. Existing organizational units are displayed.
2. Click an entry to display the View Object page showing full details of the selected organizational unit.
   - To delete the selected organizational unit, click Delete.
   - To view audit details of the organizational unit, click History.

Managing Recovery Time Values

A Recovery Time object defines a valid recovery time that can be applied to the IT components that can be managed in your organization. You can assign a recovery time to each managed element in your organization (Software Product, Business Application and Host).

You would normally set up all the recovery time values appropriate to your organization when you first set up the system, but you can update them at any time.

From the Recovery Time page all recovery time values are listed. From this page you can create a new recovery time or display an existing one in detail.

Creating a new recovery time

1. From the Custom Categories page, select the Recovery Times tab. Existing recovery times are displayed.
2. Click New Recovery Time. The Create Recovery Time page is displayed.
3. Complete the Attributes and Relationships of the recovery time value.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of this recovery time value.</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Abbreviation of recovery time value.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of recovery time value.</td>
</tr>
<tr>
<td>Active</td>
<td>Yes if this recovery time value is currently active. No if it is not active. Defaults to Yes.</td>
</tr>
</tbody>
</table>

4. Click Apply to save the recovery time details.

**Viewing details of a recovery time**

1. From the Custom Categories page, select the Recovery Times tab. Existing recovery times are displayed.
2. Click an entry to display the View Object page showing full details of the selected recovery time.
   - To delete the selected recovery time, click Delete.
   - To view audit details of the recovery time, click History.

**Compacting the datastore**

As the BMC Atrium Discovery datastore runs, many database entries are created and deleted. As this takes place, the database structure can become fragmented, meaning that there are ‘gaps’ in the data. This tends to make the database files grow over time, even if the amount of useful data remains constant.

The solution to this situation is to periodically compact the datastore using an offline copying compaction method. This compaction function defragments the databases, reclaiming the space wasted in the gaps.

**Warning**

Before compacting the datastore, back it up by performing an Appliance Snapshot. Failing to do so could result in data loss.

**Running the utility**

The `tw_ds_compact` utility compacts the datastore by copying the data files. The utility accesses the database files directly, outside the usual transactional environment. When you run the utility, you must choose a destination directory for the new database files.
Best Practice

Store the new databases on a different disk, to minimize thrashing between reading the old files and writing new ones. The new databases will generally be smaller than the originals, but you should ensure that there is at least the same amount of space as there is taken by the current databases.

For more information about the `tw_ds_compact` utility, examples of how to use the utility, and the options available for the command line, see `tw_ds_compact`.

Warning

Another script, `tw_ds_online_compact`, performs an 'on-line' compaction while the datastore is running. Bugs in the underlying Berkeley DB storage mean that the compaction may abort prematurely after filling the /usr partition or corrupt the data store. Do NOT use `tw_ds_online_compact`. Use `tw_ds_compact` to compact the datastore.

Purging the history

History information about each node and relationship is recorded in the datastore. This audit trail includes details of the changes made, the date and time of the changes and the user who made the changes. You can view the history of each object in the datastore and you can search for and display details of destroyed objects.

The purge history script

You can use the `tw_ds_purgehistory` script to purge the history. The command line options are described in the Table below.

<table>
<thead>
<tr>
<th>Command line option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--purge-older-than=int</td>
<td>Specify a number of days over which the history is purged. The default is 30.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Displays help on standard options, some brief usage information, and exits.</td>
</tr>
<tr>
<td>--list-partitions</td>
<td>Lists all partitions and exits.</td>
</tr>
<tr>
<td>--logfile=filename</td>
<td>The name of the log file into which log messages are written.</td>
</tr>
<tr>
<td>Command line option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `--loglevel=level`  | Logging level:  
  - **debug** - log all messages  
  - **info** - log critical, error, warning, and information messages.  
  - **warn** - log critical, error, and warning messages.  
  - **error** - log critical and error messages.  
  - **crit** - log only critical messages. |
| `--partition=string` | The name of the partition to purge or 'All' for all partitions. The default is all partitions. |
| `-p, --password=password` | The password that corresponds to the user name entered after the `--username` switch. Note that if you use this option your password is visible in clear text. You should avoid using this option; when you do not use it, you are prompted for the password and it is not echoed. |
| `-u, --username=username` | Username. This is a BMC Atrium Discovery command line user. |
| `-v, --version` | Displays BMC Atrium Discovery version information and exits. |

### Purge process

When it runs, the purge finds all historical entries older than the time specified with the `--purge-older-than` parameter. To ensure that the historical information is self-consistent, the creation time record for each node is maintained, and all state changes that occurred between the creation time and the purge time are rolled up into a single state change entry.

### Viewing the system taxonomy

The system taxonomy defines all kinds of data objects in the system and the relationships between them. The BMC Atrium Discovery Administrator can examine all of these objects, including their attributes, roles and relationships.

⚠️ None of this information can be changed from the BMC Atrium Discovery user interface.
Viewing the system taxonomy

1. Click **Administration**, and then click **View Taxonomy**.
   All base taxonomy objects are listed, along with the following information:
   - **Object Name**: the name of the object kind. The superclass of this object is displayed in brackets as a hyperlink.
   - **Description**: a description of this object type.
   - **Subclasses**: subclasses of this object type.
   - **Attributes**: attributes of this object type.
   - **Known relationships**: known relationships for this object. The object to which this relationship refers is displayed as a hyperlink at the end of the relationship name.

You can download the base taxonomy in XML format. To do this, right-click on the appropriate link and select **Save Target As**.

Further details of the data model can be found in the BMC Atrium Discovery taxonomy. To view the taxonomy, click the View Taxonomy icon on the Administration page of the BMC Atrium Discovery UI. A link to the current, full-size version of the diagrams below is also available in the online documentation.

⚠️ The relationships displayed in the taxonomy are not exhaustive. That is, all possible relationships are not displayed in the taxonomy. For example, the following containment relationships are valid:

- Group:Container:Containment:ContainedItem:SoftwareInstance
- Group:Container:Containment:ContainedItem:Host

The diagrams below shows the BMC Atrium Discovery Default Data Model with its different nodes, attributes and relationships between the different parts of BMC Atrium Discovery. It is split across 3 diagrams.

- **Main Diagram** – contains all the core entities used in modeling and discovery of Hosts.
- **Network and Printer Diagram** – contains entities used in the modeling and discovery of NetworkDevices and Printers.
- **Mainframe Diagram** – contains entities used in the modeling and discovery of Mainframes.

It is important to note that the model itself is not in separate sections, the three diagrams exist in order to more clearly convey information.
1. Inferred View Nodes and connection links – Blue.
2. Directly Discovered Data Nodes and connection links – Green.
5. Auxiliary Nodes and connection links – Brown – (used internally by BMC Atrium Discovery).

⚠️ The PNG images are static and represent the latest taxonomy. They do not reflect any on-site changes that may have been made to the taxonomy on your appliance.

Storage and modification of the taxonomy

Taxonomy definitions are configured using xml files which are held in the following directories:

1. /usr/tideway/data/installed/taxonomy/
2. /usr/tideway/data/custom/taxonomy/

The directories are parsed in the order given (installed before custom), and the files contained in these directories are parsed in alphabetical order, with numbers before letters. This order is important as later definitions for the taxonomy override those loaded earlier.

The standard base taxonomy file is contained in /usr/tideway/data/installed/taxonomy/00taxonomy.xml
This data layout changed in BMC Atrium Discovery 7.2. Upgrades from previous versions of BMC Atrium Discovery move the customer specific taxonomy definitions file /usr/tideway/data/customer/extensions.xml to /usr/tideway/data/custom/taxonomy/00extensions.xml

To add additional details to a node, we recommend using a detail node rather than extending the taxonomy. For more information, see Detail node.
Users and security

This section explains how to set up and change system users and system groups, including how to create users, change passwords and security settings, and set up groups.

- Managing system users
- Managing groups
- Managing security policies
- HTTPS configuration
- Managing LDAP
- Web authentication
- Viewing active sessions
- Appliance audit

Managing system users

The BMC Atrium Discovery Administrator is responsible for setting up details of all the users who are permitted to use the BMC Atrium Discovery system. Users are allocated a user name and a password, which they must enter in order to log on to the system. Each user is a member of one or more user groups, which defines the parts of the system that user is permitted to access. For example, users defined as members of the Admin group are able to create and edit user details, while members of the Public group cannot access these areas.

BMC Atrium Discovery can integrate with your corporate Lightweight Directory Access Protocol (LDAP) infrastructure. LDAP groups can be mapped to BMC Atrium Discovery groups and hence assigned permissions on the system. For information about setting up LDAP, see Managing LDAP.

As well as being the means of controlling user security, a user is actually set up on the system as a Person data object, and can subsequently be associated with other objects.

All actions on the system are recorded against a user’s ID for audit purposes. Users should always use their own ID and keep their security details safe.

Enabling other users

Typically, when you want to enable additional users to access BMC Atrium Discovery, you should log in as a user with the appropriate privileges. By default, in addition to the system user, the following additional users are configured in BMC Atrium Discovery:

- admin
- appmodel
- discovery

Best Practice
Each user has an initial password in BMC Atrium Discovery that is the same as the user name. BMC recommends that you change the password when you first log on as the system user. Not doing so will make it easier for someone to gain access to the BMC Atrium Discovery UI.

Use the system user only for configuration tasks which require system privileges.

To enable other users

1. Click the Administration tab.
2. In the Security section of the Administration page, click the Users icon.
3. For each user, click the Set Password link.
4. On the Set Password page, enter the new password in each text entry field, and then click Apply.
5. After you have changed the passwords for each user, log off from the system user account by clicking the logout icon at the top right of the page.

Creating a new user

The BMC Atrium Discovery Administrator can set up new users and assign them to groups. Before creating users, you must ensure that you have set up all the groups that you need. See Managing groups.

To create a new user

1. From the Users page, click Add at the bottom of the page.
2. In the Add User page, enter the following details for the new user:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Login ID of the user.</td>
</tr>
<tr>
<td>Full Name</td>
<td>Full name of user.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password to be allocated to this user. Repeat the password for security reasons.</td>
</tr>
<tr>
<td>Password Rules</td>
<td>A read only display of the rules which are used to validate the password strength.</td>
</tr>
<tr>
<td>Groups</td>
<td>Select one or more groups that this user will be a member of. By default, all new users are members of the public group.</td>
</tr>
</tbody>
</table>

3. To save the changes, click OK.

⚠️ User names are case sensitive. That is, user names with the same spelling but different case are permitted, for example, Johnson and JOHNSON are not recognized as duplicates.
Amending a user's details

You can change a user's name and the groups that they are a member of. The access defined by the group membership will apply the next time this user logs on.

To Amend a user's details

1. From the Users page, click **Edit** next to the user. The page is redisplayed showing editable fields.
2. Amend or overwrite **Full Name** field.
3. Select one or more **Groups** that this user is to be a member of.
4. To save the changes, click **OK**.

Changing a user's password

If users forget their passwords or if a password is not kept secure, you can assign a new password.

To set a new password for a user

1. From the Users page, click **Set Password**.
   The page is redisplayed, showing blank Password fields. The existing password is not displayed.
   If the password policy requires a password to be changed, the label "MUST be changed" is displayed next to the user.
2. Enter a new password for this user in the **Password** field. Confirm the password in the **Verify Password** field.
3. To save the changes, click **Apply**. The new password will apply the next time the user attempts to log on.
4. You can also specify that the user changes their password on their next login. To do this click **Must Change Password**.

This section describes the preferred way to set or reset user passwords. However, you can also change users passwords at the command line.

The `tw_passwd` utility enables you to change the password of a specified user interface user. To use the utility, enter the following command at command prompt:

```
tw_passwd username
```

where:

- **username** is the name of the UI user to change.
For example:

```
[tideway@DE-32 ~]$ tw_passwd fred
New password:
Retype password:
Password set for user 'fred'.
[tideway@DE-32 ~]$  
```

⚠️ Changing passwords for command line users

The `tw_passwd` utility is for changing UI users' passwords. To change the passwords for command line users, as the root user, use the Linux command `passwd`. This is described in Changing the root and user passwords.

Reactivating a user account

If a user's account is not used for a specified period of time, their account is deactivated. See Managing security policies for information on configuring account deactivation. To reactivate a deactivated user account you must be logged on as a member of the unlocker group and reactivating user accounts must be enabled in the security options page. You can also deactivate a user's account manually.

A deactivated account is never automatically reactivated.

To reactivate a locked user account

- Check that account reactivation is allowed (see Managing security policies)
- From the Users page, click Reactivate next to the user account to be reactivated.

Deleting a user

You can delete any existing user except for yourself or the default system-created users.

To delete an existing user

- From the Users page, click Delete next to the user to be deleted.
User permissions

User permissions in BMC Atrium Discovery are additive. That is, when you grant a user an additional permission (through adding the user to another group), that permission is added to the user's existing permissions. For example, if you grant appmodel permissions to a user with discovery permissions, the user gains no additional permissions because all of the appmodel permissions were already granted in the discovery permission set. Similarly, you cannot add readonly permissions to a system user in the hope of achieving a read only system user.

Managing groups

All users of the BMC Atrium Discovery system must be a member of one or more groups. Membership of groups defines the various BMC Atrium Discovery modules that a user is entitled to access. For example, users defined as members of the System group are able to create and edit user details, while members of the Public group cannot access these areas.

To login, a user must be in a group that has permissions security/user/passwd, appserver/login and appserver/module/home. Only four default groups have this permission: readonly, public, system and admin. Every user must be a member of one of these four groups, or a member of a custom group that has at least these permissions.

For example, a user who is only in the discovery group cannot login. You should put a user that requires access to discovery commands into the discovery and public groups.

The BMC Atrium Discovery Administrator is responsible for setting up details of all the user groups in the BMC Atrium Discovery system.

Each group is a collection of permissions. Permissions control granular access to BMC Atrium Discovery modules and are described in Group Permissions.

Security groups

The default user groups and their security access rights are as follows:

- **admin**: These users have the highest level of customer access to the system.
- **appmodel**: These users can write and edit patterns, and create nodes to model business applications. They cannot view credentials but can run discovery (in order to test patterns).
- **discovery**: These users have access to all of the discovery-related data. They can start and stop discovery, add and remove credentials, and enable or disable audit logging.
- **cmdb-export-administrator**: These users have access to all of the export-related data. They can build, modify, delete and run Exporters.
- **public**: These users have read/write access to all of the system although they cannot access the discovery credentials.
- **readonly**: These users have read only access to the system. They cannot view the credentials for logging into target hosts.
- **system**: These users have full access to the system.
• **unlocker**: These users are able to unlock and unblock user accounts which have been
locked or blocked after exceeding the number of permitted authentication failures. See
Managing security policies for more information.

**Listing all current groups**

1. Click **Administration**.
2. From the Security section, click **Groups**.
   The Groups page lists all the current groups and allows you to edit details, delete groups or
   create a new group.

**Creating a new group**

1. From the Groups page, click **Add** at the bottom of the page.
   The Add Group page is displayed. The page is arranged into functional areas, and then
   subdivided into columns. The arrangement of the columns from left to right is as follows:
   - Wildcard: contain items which when checked, select a number of permissions. When
     you mouseover a wildcard permission, it and the permissions it applies are highlighted
   - Read: read permissions relating to the functional area.
   - Write: write permissions relating to the functional area.
   - Misc: miscellaneous permissions relating to the functional area, such as appliance
     reboot.
2. In **Group name**, enter a name for the new group.
3. Select the checkboxes that indicate the BMC Atrium Discovery modules that members of this
   user group are allowed to access. The * wildcard matches anything, so selecting this
   checkbox will give unrestricted access to everything in the system.
4. To save the changes, click **OK**.
   Once the group is set up you can add users. See Managing system users.

**Amending a group's details**

You can change a group name and the modules that group members can access. The access
defined by the group membership will apply the next time users in this group log in.

1. From the Groups page, click **Edit** next to the user.
   The page is redisplayed showing editable fields.
2. Amend or overwrite the **Name** field.
3. Select one or more checkboxes corresponding with the BMC Atrium Discovery modules that
   members of this group can access.
4. To save the changes, click **OK**.
Deleting a group

You can delete any group provided you have created it initially. You cannot delete either the public or the system groups.

1. From the Groups page, click **Delete** next to the group to be deleted.
   The group is deleted and the system does not display any confirmation.

Group permissions

The following table shows the permissions assigned by default to each group in BMC Atrium Discovery. The individual permissions are described in **System Group Permissions by Category**.

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>*</td>
</tr>
<tr>
<td>appmodel</td>
<td>admin/category/createmodify</td>
</tr>
<tr>
<td></td>
<td>admin/log/info</td>
</tr>
<tr>
<td></td>
<td>admin/log/read</td>
</tr>
<tr>
<td></td>
<td>model/audit/purge</td>
</tr>
<tr>
<td></td>
<td>reasoning/events/read</td>
</tr>
<tr>
<td></td>
<td>reasoning/events/write</td>
</tr>
<tr>
<td></td>
<td>reasoning/pattern/config</td>
</tr>
<tr>
<td></td>
<td>reasoning/pattern/execute</td>
</tr>
<tr>
<td></td>
<td>reasoning/pattern/quickload</td>
</tr>
<tr>
<td></td>
<td>reasoning/pattern/write</td>
</tr>
<tr>
<td></td>
<td>reasoning/ranges/once</td>
</tr>
<tr>
<td></td>
<td>reasoning/ranges/read</td>
</tr>
<tr>
<td></td>
<td>reasoning/ranges/rescan</td>
</tr>
<tr>
<td></td>
<td>reasoning/ranges/write</td>
</tr>
<tr>
<td></td>
<td>reasoning/start</td>
</tr>
<tr>
<td></td>
<td>reasoning/startstop</td>
</tr>
<tr>
<td></td>
<td>reasoning/stop</td>
</tr>
<tr>
<td></td>
<td>ui/report/admin</td>
</tr>
<tr>
<td></td>
<td>vault/open</td>
</tr>
<tr>
<td>cmdb-export-administrator</td>
<td>admin/cmdb-exporter</td>
</tr>
<tr>
<td></td>
<td>vault/close</td>
</tr>
<tr>
<td></td>
<td>vault/credential_types/read</td>
</tr>
<tr>
<td></td>
<td>vault/credential_types/write</td>
</tr>
<tr>
<td></td>
<td>vault/credentials/read</td>
</tr>
<tr>
<td></td>
<td>vault/credentials/write</td>
</tr>
<tr>
<td></td>
<td>vault/open</td>
</tr>
<tr>
<td>discovery</td>
<td>consolidation/consolidation/write</td>
</tr>
<tr>
<td></td>
<td>consolidation/discovery/write</td>
</tr>
<tr>
<td></td>
<td>consolidation/read</td>
</tr>
<tr>
<td></td>
<td>discovery/credentials/test</td>
</tr>
<tr>
<td></td>
<td>discovery/filters/read</td>
</tr>
<tr>
<td></td>
<td>discovery/filters/write</td>
</tr>
<tr>
<td></td>
<td>discovery/kslave/read</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Group Name</th>
<th>Permissions</th>
</tr>
</thead>
</table>
|            | discovery/kslave/write  
|            | discovery/options/read  
|            | discovery/options/write  
|            | discovery/platforms/read  
|            | discovery/platforms/write  
|            | discovery/port/settings  
|            | model/audit/purge  
|            | reasoning/danger/read  
|            | reasoning/danger/write  
|            | reasoning/events/read  
|            | reasoning/events/write  
|            | reasoning/pattern/config  
|            | reasoning/pattern/write  
|            | reasoning/ranges/once  
|            | reasoning/ranges/read  
|            | reasoning/ranges/rescan  
|            | reasoning/ranges/write  
|            | reasoning/start  
|            | reasoning/startstop  
|            | reasoning/stop  
|            | ssh_key/read  
|            | vault/credential_types/read  
|            | vault/credential_types/write  
|            | vault/credentials/read  
|            | vault/credentials/write  
|            | vault/open  
| public     | appserver/login  
|           | appserver/module/*  
|           | model/audit/read  
|           | model/audit/write  
|           | model/datastore/main/read  
|           | model/datastore/main/write  
|           | model/datastore/partition/Audit/read  
|           | model/datastore/partition/Conjecture/read  
|           | model/datastore/partition/Conjecture/write  
|           | model/datastore/partition/DDD/read  
|           | model/datastore/partition/DDD/write  
|           | model/datastore/partition/Default/read  
|           | model/datastore/partition/Default/write  
|           | model/datastore/partition/Taxonomy/read  
|           | model/datastore/partition/_System/read  
|           | model/datastore/partition/_System/write  
|           | model/notification/publish  
|           | model/notification/subscribe  
|           | model/taxonomy/nodekind/read  
|           | model/taxonomy/relkkind/read  
|           | model/taxonomy/rolekind/read  
|           | reasoning/events/write  
|           | reasoning/status  
|           | reports/read  
|           | reports/write  
|           | security/user/passwd  

### System group permissions by category

The system group security permissions are shown by category in the following tables.

⚠️ There are no permissions that restrict access to patterns. All logged in users can view patterns.

### Security permissions

The following table shows the current group permissions relating to the security operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>security/group/read</td>
<td>Enables the user to view and configure group membership to a user.</td>
</tr>
<tr>
<td>security/group/write</td>
<td>• security/group/read: View the user group names and the corresponding permissions.</td>
</tr>
</tbody>
</table>
|                     | • security/group/write: View, edit, delete, and create new groups.  
|                     | You can manage user groups from the Groups page of the UI. To navigate to the page:                                                        |
|                     | 1. Click Administration.                                                                                                                 |
|                     | 2. From the Security section, click Groups.                                                                                               |
1. Click **Administration**.
2. From the Security section, click **HTTPS**.
   
   For more information, see Configuring HTTPS settings.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
</table>
| security/https/admin | Enables the user to configure the HTTPS settings, which include:  
|                 | • generating server keys and certificate signing requests  
|                 | • uploading and sign server certificates  
|                 | • uploading or downloading a CA certificate bundle  
|                 | • enabling and disabling HTTP or HTTPS web access to the appliance  
|                 | You can manage the HTTPS configuration from the HTTPS Configuration page of the UI. To navigate to the page:  
|                 | 1. Click **Administration**.  
|                 | 2. From the Security section, click **HTTPS**.  
|                 |   For more information, see Configuring HTTPS settings.  |
| security/options/read | Enables the user to view and configure the security options which include accounts and passwords, login page, and UI security page.  
| security/options/write | • security/options/read: View the security options for the appliance.  
|                     | • security/options/write: Configure the security options settings for the appliance.  
|                 | You can manage the options from the Security Policy page of the UI. To navigate to the page:  
|                 | 1. Click **Administration**.  
|                 | 2. From the Security section, click **Security Policy**.  
|                 |   For more information, see the Managing security policies page.  |
| security/user/activate | Enables the user to unlock and re-activate accounts for other users from the Users page of the UI. To navigate to the page:  
| security/user/passwd | Enables the user to change her or his **own** BMC Atrium Discovery password from the UI.  
|                       | For more information, see changing your password .  |
| security/user/read | Enables the user to view and configure the user security information related to system users, groups, security policies, HTTPS settings, LDAP, Web authentication settings, active sessions, appliance audit, and so on.  
| security/user/write | • security/user/read: View the user security information.  
|                     | • security/user/write: Configure the user security information.  
|                       | For more information, see the Managing users and security page.  |

### Credential vault permissions

BMC Atrium Discovery stores all passwords used to access customer devices in a credential vault which can be secured. The contents of the vault can be encrypted and secured using a passphrase.

The following table shows the current group permissions relating to the vault operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
</table>
| vault/open       | Enables the user to open, close, and set the passphrase for the credential vault from the Vault Management page of the UI. To navigate to the page:  
| vault/close      | 1. Click **Administration**.  
| vault/passphrase| 2. From the Discovery section, click **Vault Management**.  
|                 |   All three permissions are required to use the **Vault Management** page. |
### Permission Definition

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vault/credential_types/read</td>
<td>Enables the user to manage the following types of credentials which are based on the system to access:</td>
</tr>
<tr>
<td></td>
<td>• Device: To log on to hosts running a Unix, Linux operating system, or Windows operating system, or any SNMP enabled device such as routers and switches.</td>
</tr>
<tr>
<td></td>
<td>• Database: To query databases.</td>
</tr>
<tr>
<td></td>
<td>• Middleware: To query middleware such as web and application servers, and so on.</td>
</tr>
<tr>
<td></td>
<td>• Management System: For vCenter, vSphere, and mainframe credentials.</td>
</tr>
<tr>
<td></td>
<td>You can view and manage the credentials types from the Credentials page of the UI. To navigate to the page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Discovery.</td>
</tr>
<tr>
<td></td>
<td>2. Click Credentials.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Credentials page.</td>
</tr>
<tr>
<td>vault/credential_types/write</td>
<td></td>
</tr>
<tr>
<td>vault/credentials/read</td>
<td>Enables the user to view and manage credentials (For example, Windows proxies, vSphere credentials, and so on).</td>
</tr>
<tr>
<td></td>
<td>• vault/credentials/read: View the credentials.</td>
</tr>
<tr>
<td></td>
<td>• vault/credentials/write: Manage the credentials.</td>
</tr>
<tr>
<td></td>
<td>You can view and manage credentials from the Credentials page of the UI:</td>
</tr>
<tr>
<td></td>
<td>1. Click Discovery.</td>
</tr>
<tr>
<td></td>
<td>2. Click Credentials.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Credentials page.</td>
</tr>
<tr>
<td>vault/credentials/write</td>
<td></td>
</tr>
</tbody>
</table>

### Discovery permissions

The following table shows the current group permissions relating to the discovery operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>discovery/network/probe</td>
<td>Obsolete permission.</td>
</tr>
<tr>
<td>discovery/options/read</td>
<td>Enables the user to read the discovery options. These are separate from the main system settings.</td>
</tr>
<tr>
<td>discovery/options/write</td>
<td></td>
</tr>
<tr>
<td>discovery/credentials/test</td>
<td>Enables the user to test discovery credentials. For example, from the UI, you can test:</td>
</tr>
<tr>
<td></td>
<td>• Discovery credentials from the Credential Tests tab. For more information, see Testing credentials.</td>
</tr>
<tr>
<td></td>
<td>• Mainframe credentials from the Mainframe Credential Tests tab. For more information, see Testing mainframe credentials.</td>
</tr>
<tr>
<td>discovery/platforms/read</td>
<td>Enables the user to view and amend the platform discovery commands from the Discovery Platforms page.</td>
</tr>
<tr>
<td></td>
<td>• discovery/platforms/read: View the platform discovery commands.</td>
</tr>
<tr>
<td></td>
<td>• discovery/platforms/write: Amend the platform discovery commands.</td>
</tr>
<tr>
<td></td>
<td>You can view and amend the platform discovery commands from the Discovery Platforms page of the UI. To navigate to the page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Administration.</td>
</tr>
<tr>
<td></td>
<td>2. From the Discovery section, click Discovery Platforms.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Managing the discovery platform scripts.</td>
</tr>
<tr>
<td>discovery/platforms/write</td>
<td></td>
</tr>
</tbody>
</table>
Permission | Definition
---|---
discovery/host/access | Enables the user to query a host on the network. For more information, see [Query Builder](#).
discovery/filters/ read | Enables the user to view and modify sensitive data filters from the Sensitive Data Filters page of the UI. To navigate to the page:
1. Click [Administration](#).
2. From the Discovery section, click [Sensitive Data Filters](#).
   For more information, see [Masking sensitive data](#).
discovery/filters/ write |
discovery/kslave/ read | Enables the user to view and modify the Windows proxies.
You can manage Windows proxies from the Windows proxy management page of the UI. To navigate to the page:
1. Click [Discovery](#).
2. Click [Credentials](#).
3. Click [Windows Proxies](#). The Device Credentials page for Windows proxies (Windows proxy management page) is displayed.
   For more information, see [Managing Windows proxies](#).
discovery/kslave/ write |
discovery/port/ settings | Enables the user to configure the port settings that Discovery uses.
You can manage the port settings from the Discovery Configuration page on the UI. To navigate to the page:
1. Click [Administration](#).
2. From the Discovery section, click [Discovery Configuration](#).
   For more information, see [port settings](#).
ssh_key/write | Obsolete permission.

### Consolidation permissions

The following table shows the current group permissions relating to configuring consolidation and scanning appliances.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
</table>
| consolidation/ consolidation/write | Enables the user to change the configuration on the consolidation appliance (set as consolidation appliance and approve scanning appliances). You can manage consolidation from the Discovery Consolidation page on the UI. To navigate to the page:
1. Click [Administration](#).
2. From the Discovery section, select [Discovery Consolidation](#).
   For more information about consolidation, see the [Consolidation page](#). |
| consolidation/discovery write | Enables the user to add new consolidation targets to a scanning appliance from the Discovery Consolidation page on the UI. |
| consolidation/read | Enables the user to view the consolidation setup page from the Discovery Consolidation page on the UI. |
Datastore permissions

These permissions are a subsystem of the model. The following table shows the current group permissions relating to the datastore operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>model/datastore/main/read</td>
<td>Enables the user to read or write the datastore through the main user interface (UI).</td>
</tr>
<tr>
<td>model/datastore/main/write</td>
<td></td>
</tr>
<tr>
<td>model/datastore/partition/*/read</td>
<td>Enables the user to read or write to any partition which support user interaction. For more information, see the Partitions and History page.</td>
</tr>
<tr>
<td>model/datastore/partition/*/read</td>
<td></td>
</tr>
<tr>
<td>model/datastore/partition/name/read</td>
<td>Enables the user to read or write to the given partition. The name is one of:</td>
</tr>
<tr>
<td>model/datastore/partition/name/write</td>
<td>• Audit</td>
</tr>
<tr>
<td></td>
<td>• Conjecture</td>
</tr>
<tr>
<td></td>
<td>• DDD</td>
</tr>
<tr>
<td></td>
<td>• Default</td>
</tr>
<tr>
<td></td>
<td>• Taxonomy</td>
</tr>
<tr>
<td></td>
<td>• _System</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Audit permissions

These permissions are a subsystem of the model. The following table shows the current group permissions relating to the audit operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>model/audit/read</td>
<td>Enables the user to read the audit log.</td>
</tr>
<tr>
<td></td>
<td>Audit logs are stored in /usr/tideway/log. The files can be accessed directly from the appliance command line or in the log viewer from the UI. Logs can be downloaded from the appliance through the Support Services administration page.</td>
</tr>
<tr>
<td>model/audit/write</td>
<td>Enables the user to write to the audit log.</td>
</tr>
<tr>
<td>model/audit/purge</td>
<td>Enables the user to purge the audit log.</td>
</tr>
<tr>
<td></td>
<td>You can purge the audit log of all events that are over one month old (events less than one month old cannot be deleted) from the Audit Purge page. To navigate to the Audit Purge page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Administration.</td>
</tr>
<tr>
<td></td>
<td>2. From the Security section, click Audit.</td>
</tr>
<tr>
<td></td>
<td>3. Click Purge.</td>
</tr>
<tr>
<td></td>
<td>For more information, see purging audit logs.</td>
</tr>
<tr>
<td>model/audit/admin</td>
<td>Enables the user to administer the audit service.</td>
</tr>
<tr>
<td></td>
<td>You can configure the reporting on audit events from the Audit Logs page. To navigate to the Audit Logs page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Administration.</td>
</tr>
<tr>
<td></td>
<td>2. From the Security section, click Audit.</td>
</tr>
<tr>
<td></td>
<td>3. Click Audit Logs.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the Auditing the appliance page.</td>
</tr>
</tbody>
</table>
### Reasoning permissions

These permissions are a subsystem of the model. The following table shows the current group permissions relating to the reasoning operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>reasoning/start</td>
<td>Enables the user to start reasoning. You can start reasoning by using the <code>tw_scan_control</code> utility. For more information, see <a href="#">tw_scan_control</a>.</td>
</tr>
<tr>
<td>reasoning/startstop</td>
<td>Enables the user to start and stop reasoning. You can start and stop reasoning by using the <code>tw_scan_control</code> utility. For more information, see <code>tw_scan_control</code>.</td>
</tr>
<tr>
<td>reasoning/stop</td>
<td>Enables the user to stop reasoning. You can stop reasoning by using the <code>tw_scan_control</code> utility. For more information, see <code>tw_scan_control</code>.</td>
</tr>
<tr>
<td>reasoning/status</td>
<td>Enables the user to view the reasoning status information. You can view the reasoning status by using the <code>tw_reasoningstatus</code> utility. Typically this utility is used by Customer Support as a troubleshooting tool for investigating possible problems. For more information, see <code>tw_reasoningstatus</code>.</td>
</tr>
<tr>
<td>reasoning/ranges/read</td>
<td>Enables the user to view the Discovery Status page. The status of the discovery process displays on the Home tab in the Discovery Status summary. This page also displays the current status of the reasoning process. For more information, see Viewing discovery status page.</td>
</tr>
</tbody>
</table>
| reasoning/ranges/write| Enables the user to cancel consolidations or local scans. You can cancel consolidation or local scans from the Discovery Status page. To navigate to the Discovery Status page:  
  1. Click Discovery.  
  2. Click Discovery Status.  
     For more information, see Viewing discovery status. |
| reasoning/ranges/once| Enables the user to add or remove snapshot discovery ranges from the Discovery Status page. To navigate to the Discovery Status page:  
  1. Click Discovery.  
  2. Click Discovery Status.  
     To learn how to add discovery ranges, see Scanning IP addresses or ranges.  
     To learn how to exclude discovery ranges, see Excluding IP addresses and ranges from scanning. |
<p>| reasoning/events/read| An internal permission. Do not use this.                                                                                                              |
| reasoning/events/write| An internal permission. Do not use this.                                                                                                               |
| reasoning/events/state| Enables the user to configure patterns. For more information, see Pattern Configuration.                                                            |</p>
<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>reasoning/pattern/edit</td>
<td>Enables the user to edit patterns.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Pattern configuration and editing.</td>
</tr>
<tr>
<td>reasoning/pattern/execute</td>
<td>Enables the user to execute patterns.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Manual pattern execution.</td>
</tr>
<tr>
<td>reasoning/pattern/quickload</td>
<td>Enables the user to upload and activate patterns from the Pattern Management page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Discovery.</td>
</tr>
<tr>
<td></td>
<td>2. Click Pattern Management.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Pattern management.</td>
</tr>
<tr>
<td>reasoning/pattern/write</td>
<td>Enables the user to write patterns using pattern templates from the appliance.</td>
</tr>
<tr>
<td></td>
<td>The pattern templates can be downloaded from the Pattern Management page:</td>
</tr>
<tr>
<td></td>
<td>1. Click Discovery.</td>
</tr>
<tr>
<td></td>
<td>2. Click Pattern Management.</td>
</tr>
<tr>
<td></td>
<td>For more information, see using pattern templates.</td>
</tr>
</tbody>
</table>

**Search permissions**

These permissions relate to listing and cancelling searches using the Search Management Page. To navigate to the Search Management page:

1. Click Administration.
2. From the Model section, click Search Management.

For more information on viewing and cancelling searches, see **Using the Search Service**.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>model/search/list</td>
<td>Enables the user to view searches submitted by all users.</td>
</tr>
<tr>
<td>model/search/cancel</td>
<td>Enables the user to cancel searches submitted by all users.</td>
</tr>
</tbody>
</table>

**Taxonomy permissions**

These permissions are a subsystem of the model. The following table shows the current group permissions relating to the taxonomy operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>model/taxonomy/nodekind/read</td>
<td>Enables the user to read node kind information.</td>
</tr>
<tr>
<td>model/taxonomy/nodekind/write</td>
<td>Enables the user to write node kind information.</td>
</tr>
<tr>
<td>model/taxonomy/relkind/read</td>
<td>Enables the user to read relationship kind information.</td>
</tr>
<tr>
<td>model/taxonomy/relkind/write</td>
<td>Enables the user to write relationship kind information.</td>
</tr>
<tr>
<td>model/taxonomy/rolekind/read</td>
<td>Enables the user to read role kind information.</td>
</tr>
<tr>
<td>model/taxonomy/rolekind/write</td>
<td>Enables the user to write role kind information.</td>
</tr>
</tbody>
</table>
Application server permissions

The following table shows the current group permissions relating to the application server operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>appserver/login</td>
<td>Enables the user to log in to the appserver.</td>
</tr>
<tr>
<td>appserver/debug</td>
<td>Enables the user to debug the appserver.</td>
</tr>
<tr>
<td>appserver/module/name</td>
<td>Enables the user to access the given module. The name is one of:</td>
</tr>
<tr>
<td></td>
<td>• Application</td>
</tr>
<tr>
<td></td>
<td>• Discovery</td>
</tr>
<tr>
<td></td>
<td>• Home</td>
</tr>
<tr>
<td></td>
<td>• Infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Reports</td>
</tr>
<tr>
<td></td>
<td>• Setup</td>
</tr>
<tr>
<td></td>
<td>• System</td>
</tr>
<tr>
<td>appserver/module/*/</td>
<td>Enables the user to access any module.</td>
</tr>
<tr>
<td>appserver/sessionaccess</td>
<td>The user is allowed to see sessions.</td>
</tr>
</tbody>
</table>

Specific UI permissions

The following table shows the current group permissions relating to specific user interface operations.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ui/dashboard/admin</td>
<td>Enables the user to administer the dashboard.                                                                                                  You can use the <code>tw_config_dashboards</code> utility to configure and customize dashboards in BMC Atrium Discovery. For more information, see <code>tw_config_dashboards</code>.</td>
</tr>
<tr>
<td>ui/datastore/admin</td>
<td>Enables the user to administer the datastore.</td>
</tr>
<tr>
<td>ui/taxonomy/admin</td>
<td>Enables the user to administer the taxonomy.</td>
</tr>
<tr>
<td>ui/report/admin</td>
<td>Enables the user to access the Generic Search Query page and enter search queries. To navigate to the Generic Search Query page:</td>
</tr>
<tr>
<td></td>
<td>1. Click the <strong>Search</strong> icon to the left of the Search box at the top right of the User Interface. The Search Options in the drop down panel is displayed.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <strong>Generic Search Query</strong> link. For more information, see <strong>Using the Search service</strong>. Note that, by default, all admin users get this permission.</td>
</tr>
</tbody>
</table>

Appliance administration permissions

The following table shows the current group permissions relating to the appliance administration operations.
<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
</table>
| admin/category/createmodify | Enables the user to create and modify categories from the Custom Categories page:  
To navigate to the Custom Categories page:  
1. Click Administration.  
2. From the Model section, click Custom categories.  
For more information, see Setting up standard data categories. |
| Appliance admin operations | |
| appliance/info/read | Enables the user to view appliance information (identity, support information, read-only information about the appliance software and hardware configuration, and so on) from the Appliance Configuration page.  
To navigate to the Appliance Configuration page:  
1. Click Administration.  
2. From the Appliance section, click Configuration.  
For more information, see Configuring appliance settings. |
| appliance/info/write | Enables the user to configure appliance information from the Appliance Configuration page.  
To navigate to the Appliance Configuration page:  
1. Click Administration.  
2. From the Appliance section, click Configuration.  
For more information, see Configuring appliance settings. |
| appliance/maintenance | Enables the user to put the appliance into maintenance mode from the Appliance Control page. To navigate to the Appliance Control page:  
1. Click Administration.  
2. From the Appliance section, click Control.  
For more information, see Using maintenance mode. |
| appliance/reboot | Enables the user to reboot the appliance from the Appliance Control page. To navigate to the Appliance Control page:  
1. Click Administration.  
2. From the Appliance section, click Control.  
For more information, see Rebooting or shutting down the appliance. |
| appliance/reportsusage/reset | Enables the user to reset the report usage statistics. |
| appliance/restart | Enables the user to restart the appliance from the Appliance Control page. To navigate to the Appliance Control page:  
1. Click Administration.  
2. From the Appliance section, click Control.  
For more information, see Rebooting or shutting down the appliance. |
| appliance/shutdown | Enables the user to shut down the appliance from the Appliance Control page. To navigate to the Appliance Control page:  
1. Click Administration. |
<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **2.** From the Appliance section, click **Control.**  
For more information, see **Rebooting or shutting down the appliance.** | **Baseline** |
| baseline/admin | Enables the user to change the baseline configuration (such as the recipients of automatic emails, and the messages to be included) from the Appliance Baseline page. To navigate to the Appliance Baseline page:  
1. Click **Administration.**  
2. From the Appliance section, click **Baseline Status.**  
For more information, see **Baseline configuration.** |
| baseline/read | Enables the user to view the baseline configuration from the Appliance Baseline page. To navigate to the Appliance Baseline page:  
1. Click **Administration.**  
2. From the Appliance section, click **Baseline Status.**  
For more information, see **Baseline configuration.** |
| baseline/update | Enables the user to update the baseline configuration after changes have been seen from the Appliance Baseline page. To navigate to the Appliance Baseline page:  
1. Click **Administration.**  
2. From the Appliance section, click **Baseline Status.**  
For more information, see **Baseline configuration.** |
| **Logging** | |
| admin/log/info | Enables the user to view log information.  
As each BMC Atrium Discovery component and script runs, it outputs logging information. Logs are all stored in `/usr/tideway/log`.  
You can access the files directly from the appliance command line or in the log viewer in the UI. |
| admin/log/read | Enables the user to read log files.  
Logs are all stored in `/usr/tideway/log`.  
You can access the files directly from the appliance command line or in the log viewer in the UI. |
| admin/log/delete | Enables the user to delete log files.  
You can delete the log files from the Logs page. To navigate to the Logs page:  
1. Click **Administration.**  
2. From the Appliance section, click **Logs.**  
For more information, see **view and delete logs.** |
| admin/loglevel/read | Enables the user to read the appliance log level from the Logs page. To navigate to the Logs page:  
1. Click **Administration.**  
2. From the Appliance section, click **Logs.**  
For more information, see **view log levels.** |
| admin/loglevel/write | Enables the user to change the service log levels at runtime from the Logs page. To navigate to the Logs page:  
1. Click **Administration.** |
<table>
<thead>
<tr>
<th>Permission</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import</strong></td>
<td>2. From the Appliance section, click <strong>Logs</strong>. For more information, see Changing log levels at runtime.</td>
</tr>
<tr>
<td>admin/import/ciscoworks</td>
<td>Enables the user to import data using the CiscoWorks importer. You can use the <code>tw_imp_ciscoworks</code> utility to import CiscoWorks network device data from the command line. For more information, see <code>tw_imp_ciscoworks</code>.</td>
</tr>
<tr>
<td>admin/import/csv</td>
<td>Enables the user to import CSV data from the Import CSV Data page and also enables the user to import application mapping definitions from the Import Application Mapping Definitions page. To navigate to these pages: 1. Click <strong>Administration</strong>. 2. From the Model section, click <strong>CSV Import</strong>. For more information, see Importing CSV data. 3. From the Model section, click <strong>Application Mapping Import</strong>. For more information, see Importing application mapping definitions.</td>
</tr>
<tr>
<td>admin/import/hrd</td>
<td>Enables the user to import Hardware Reference data (HRD) from the Import Hardware Reference Data page. To navigate to the Hardware Reference Data page: 1. Click <strong>Administration</strong>. 2. From the Model section, click <strong>HRD Import</strong>. For more information, see Importing Hardware Reference Data.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td></td>
</tr>
<tr>
<td>admin/interface/read</td>
<td>Enables the user to view interface information from the Appliance Configuration page for network interfaces. To navigate to the Appliance Configuration page for network interfaces: 1. Click <strong>Administration</strong>. 2. From the Appliance section, click <strong>Configuration</strong>. 3. Click <strong>Network Interfaces</strong>. For more information, see Viewing network interface and routing settings.</td>
</tr>
<tr>
<td>admin/interface/write</td>
<td>This permission is not used.</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td></td>
</tr>
<tr>
<td>admin/routing/read</td>
<td>Obsolete permission.</td>
</tr>
<tr>
<td>admin/routing/write</td>
<td>Obsolete permission.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td></td>
</tr>
<tr>
<td>admin/dns/read</td>
<td>Enables the user to read DNS information. You can view the DNS (Name Resolution) information from the Appliance Configuration page for name resolution. To navigate to the page: 1. Click <strong>Administration</strong>. 2. From the Appliance section, click <strong>Configuration</strong>. 3. Click <strong>Name Resolution</strong>. For more information, see Configuring name resolution settings.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| admin/dns/write               | The user is allowed to write DNS information. You can configure the DNS (Name Resolution) information from the Appliance Configuration page for name resolution. To navigate to the page:  
  1. Click **Administration**.  
  2. From the Appliance section, click **Configuration**.  
  3. Click **Name Resolution**.  
    For more information, see Configuring name resolution settings. |
| admin/mail/read                | Enables the user to view email configuration information from the Appliance Configuration page for mail settings. To navigate to the page:  
  1. Click **Administration**.  
  2. From the Appliance section, click **Configuration**.  
  3. Click **Mail Settings**.  
    For more information, see Configuring mail settings. |
| admin/mail/write              | Enables the user to configure the mail settings from the Appliance Configuration page for mail settings. To navigate to the page:  
  1. Click **Administration**.  
  2. From the Appliance section, click **Configuration**.  
  3. Click **Mail Settings**.  
    For more information, see Configuring mail settings. |
| system/settings/read           | Enables the user to read system settings from the command line utilities and from the UI.                                                   |
| system/settings/write          | Enables the user to write system settings from the command line utilities and from the UI.                                                   |
| Windows proxy Installation    | Enables the user to download and install Windows proxies onto the local Windows host.  
  You can download the Windows proxies as installation files from Discovery Tools page. To navigate to the Discovery Tools page:  
  1. Click **Discovery**.  
  2. Click **Tools**.  
    For more information, see Installing Windows proxies. |

⚠️ The 'all' permission (*) allows the user to perform any tasks in BMC Atrium Discovery.  
Each user has a token which is assigned by the security system and whenever a privilege is requested by a user, the security service checks the database to see if that particular user has permission to carry out that particular task.
However, the first check that BMC Atrium Discovery carries out is to see if the user has the * permission. If the answer is yes, no further privilege checks will be carried out.

Managing security policies

Many organizations enforce security policies on user access to their systems. BMC Atrium Discovery supports this by providing configurable security options and multiple authentication mechanisms. You can configure the following:

- **Accounts and Passwords**
  - Password strength and expiry
  - Forced password change
  - Account blocking after authentication failures
  - Deactivation of unused accounts
- **Login Page**
  - Appearance of the login page
  - Legal banner messages
  - Allow browser autocomplete
- **UI Security page**
  - Prevent Cross Site Framing

Configuring these settings is described in the following sections.

Accounts and passwords

To configure the security options:

1. Click **Administration**.
2. From the Security section, click **Security Policy**.

The options on the Security Policy page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Blocking</td>
<td>User accounts can be blocked after a number of unsuccessful login attempts. Select the number of attempts from the drop-down list. Choose from the following 1, 2, 3, 4, or 5 attempts. If you do not want accounts to be blocked, select Never. The default is 3.</td>
</tr>
<tr>
<td>Automatically Unblock</td>
<td>After a user account is blocked, it can be automatically unblocked after a specified period. Select the period from the drop-down list. Choose from the following 1, 2, 3, 4, 5, 10, 15, 20, 30, or 60 minutes. If you do not want accounts to be automatically unblocked, select Never. The default is 10 minutes. If you select Never, there is a chance that you could lock out the system account. See #Blocking of the System Account for more information.</td>
</tr>
<tr>
<td>Account Deactivation</td>
<td>Unused user accounts can be deactivated after a specified period of time. Select the period from the drop-down list. Choose from the following 15, 30, 45, 60, 75, 90, 105, and 120 days. If you do not want accounts to be deactivated, select Never. The default is that disabled accounts cannot be reactivated. Select Yes or No to allow user accounts to be reactivated. You will need an administrator to reactivate the account.</td>
</tr>
</tbody>
</table>
### Blocking of the system account

In the following scenario, the system user account may be locked.

- Account blocking is enabled (the default).
- Automatic account unblocking is disabled (not the default).
- A user repeatedly attempts to login unsuccessfully to the UI as the system user.

An administrator will be required to login to the system and unblock the account.

### Login page

You can configure the appearance of the login page and add a legal notice to the login page.

To configure the login page:

1. From the Security section of the Administration tab, select Login Page Options.
   
   The options on the The Security Options: Login page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain login page</td>
<td>Where security is a concern, you can choose to remove all banners and logos from the login page. Doing so reduces the risk of attack by hiding the nature of system from a would be attacker. Select Yes to do this. This option is not available in the BMC Atrium Discovery Community Edition.</td>
</tr>
</tbody>
</table>
1. Field Name: Details
   - Field Name: Prevent Cross Site Framing
     - Details: You can specify whether to allow the BMC Atrium Discovery UI to be incorporated as part of an umbrella UI. Select Yes or No.

UI security page – new in 8.3 SP2

You can prevent cross site framing to defend against possible "clickjacking" attacks.

To configure the UI security page:

1. From the Security section of the Administration tab, select UI Security.

HTTPS configuration

The HTTPS Configuration page enables you to configure the HTTPS settings for the appliance. This includes:

- Generating server keys and certificate signing requests
- Uploading and signing server certificates
- Upload a CA certificate bundle to the appliance, or download them from the appliance
- Enable and disable HTTP or HTTPS web access to the appliance

To access the HTTPS Configuration page, select HTTPS from the Security section of the Administration tab. The server key displays the private key for the appliance.

Generating a server key

1. To generate a server key, enter relevant information in the editable fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>A read-only description of the current server key status. For example, this may contain information on the length and modification date of the key in use.</td>
</tr>
<tr>
<td>Hostname</td>
<td>A read-only field containing the hostname of the appliance. If the hostname has not already been configured on the appliance (for example, the hostname is displayed as 'localhost'), you must login as the netadmin user and change the hostname. For more information, see netadmin user.</td>
</tr>
</tbody>
</table>
1. Enter the required information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country Code</td>
<td>The two character country code for the country in which the appliance is located, for example GB.</td>
</tr>
<tr>
<td>State or Province</td>
<td>The state or province in which the appliance is located, for example Yorkshire.</td>
</tr>
<tr>
<td>Locality</td>
<td>The locality in which the appliance is located, for example York.</td>
</tr>
<tr>
<td>Company Name</td>
<td>The company name, for example, BMC Software.</td>
</tr>
<tr>
<td>Department</td>
<td>The department using the appliance. This field is optional.</td>
</tr>
<tr>
<td>Email Address</td>
<td>The email contact for users of this appliance. This field is optional.</td>
</tr>
</tbody>
</table>

⚠️ The values in the **Server Key** tab must match those used by the certificate authority.

2. When you have entered the required information, click **Generate New Server Key**. The new server key is saved as $TIDEWAY/etc/https/server.key onto the appliance's file system. A certificate signing request is also generated, it is called server.csr and is saved in the same location.

When you have a key and a signing request, it must be signed before it can be used. You can do this using one of the following methods:

- Use a certificate authority: continue with this procedure.
- Sign the certificate yourself: see **Self Signing a Server Certificate**.

3. To download the certificate signing request, click **Download CSR**. Use the download dialog to choose the location on your local filesystem in which to save the file.

4. Send the certificate signing request file to your certificate signing authority for signing. When the certificate signing authority has approved the request, they will generate the corresponding certificate and return it as a .crt file.

### Uploading a server certificate

1. When your certificate signing authority has approved the request, they will return a certificate. Save this file on your local filesystem.
2. On the HTTPS Configuration page, click the **Server Certificate** tab.
3. Click **Browse** next to **Certificate File**: and select the server certificate you saved in Step 1 of this procedure.
4. Click **Upload New Certificate**. The new certificate is uploaded onto the appliance.
Self signing a server certificate

If you do not use a certificate authority, but still require https access to the appliance, you can use the self-signing feature.

To self sign a certificate:

1. Ensure that you have created a server key and certificate signing request on the appliance using the procedure described in Generating a Server Key.
2. In the HTTPS Configuration page, click Server Certificate => Self Sign.
   The server key that you created is signed and saved as a new certificate called server.crt.
3. Enable HTTPS access. See Enabling or Disabling HTTP and HTTPS Access to the Appliance for more information.
   When you access BMC Atrium Discovery using HTTPS, you will be prompted to accept the certificate once per each session.

Uploading or downloading a CA certificate bundle

The CA certificate bundle that is included by default contains a number of certificates from public certificate authorities. These are usually known as Trusted root certificates, or Trusted Intermediate Certificates. You can continue to use these or replace them with a certificate bundle from a certificate authority used by your organization. Your system administrator should tell you whether to use the supplied bundle or will provide you with one supported by your organization.

⚠️ If you do not have a CA bundle, either the default supplied with the appliance, or one supplied by your organization, you will be unable to use HTTPS.

The default CA bundle is stored on the appliance in the following directory:
/etc/pki/tls/certs/ca-bundle.crt
When the certificate signing authority has approved the request, they will generate the corresponding certificate bundle and return it as a .crt file.
To replace the certificate bundle with one from a certificate authority used by your organization:

1. On the HTTPS Configuration page, click CA Certificates.
2. Click Browse next to CA Certificate Bundle File and select the server certificate you saved in Step 1 of this procedure.
3. Click Upload New CA Certificate Bundle.
   The new certificate bundle is uploaded.

To download the existing CA certificate bundle:

1. Click Download CA Certificate Bundle.
2. Use the download dialog to choose the location on your local filesystem in which to save the file.
Enabling or disabling HTTP and HTTPS access to the appliance

⚠️ Use a two stage approach to enabling redirect to HTTPS. Configure the HTTPS and test that it is configured correctly and permits access to authenticated users. Only then should you enable redirect to HTTPS.

If HTTPS is not configured correctly, and you enable redirect to HTTPS, you could be locked out of the appliance.
By default users can access the BMC Atrium Discovery over HTTP. You can enable HTTPS connections on this page and specify that attempts to connect over HTTP should be redirected to HTTPS.
By default HTTP access is enabled and HTTPS access is disabled.

1. On the HTTPS Configuration page, click HTTPS tab.
The following screen illustrates an example of HTTPS enabled and HTTP redirected to HTTPS:

![HTTPS Configuration](image)

This screen illustrates an HTTPS enabled and HTTP redirected to HTTPS.
- To enable HTTPS access, from the HTTPS list, select Enabled.
- To disable HTTPS access, from the HTTPS list, select Disabled.
- To enable HTTP access, from the HTTPS list, select Enabled.
- To redirect HTTP access attempts to HTTPS, from the HTTP list, select Redirect to HTTPS.

Managing LDAP

Lightweight Directory Access Protocol (LDAP) is commonly used to access user or group information in a corporate directory. Using your corporate LDAP infrastructure to authenticate users can reduce the number of administrative tasks that you need to perform in BMC Atrium Discovery. LDAP groups can be mapped to BMC Atrium Discovery groups and hence assigned permissions on the system. The way in which BMC Atrium Discovery integrates with your LDAP infrastructure depends on the schema that is implemented in your organization.

ℹ️ If you are using LDAP authentication there is no need to set up local user accounts for LDAP users on BMC Atrium Discovery.
LDAP Terms

The following terms are used in the sections describing BMC Atrium Discovery LDAP configuration:

- **Directory Information Tree (DIT):** The overall tree structure of the data directory queried using the LDAP protocol. The structure is defined by the schema. Each entry in a directory is an object; one of two types:
  - **Containers:** A container is like a folder: it contains other containers or leaves.
  - **Leaves:** A leaf is an object at the end of a tree. Leaves cannot contain other objects.
- **Domain Component (dc):** Each element of the Internet domain name of the company is given individually.
- **Organizational Unit (ou):** Organizations in the company.
- **Common Name (cn):** The name of a person.
- **Distinguished Name (dn):** The complete name for a person, including the domain components, organisational unit, and common name.

An example Directory Information Tree is shown below.

```
dc=tideway,dc=com
    ou=engineering
        cn=Timothy Taylor
            telephoneNumber=1234
            email=t.taylor@bmc.com
    ou=test
        cn=Sam Smith
            telephoneNumber=2345
            email=s.smith@bmc.com
    ou=product management
        cn=John Smith
            telephoneNumber=3456
            email=j.smith@bmc.com
```

The login procedure

When a user attempts to log in through the user interface, BMC Atrium Discovery first checks to see whether the username represents a local account. If no local account exists, and LDAP has been configured correctly, BMC Atrium Discovery attempts to authenticate against the directory and then performs an account lookup to return the group memberships of that account. If the group mappings have been enabled, and configured correctly, then authentication takes place and the user is logged in with the local BMC Atrium Discovery rights as defined in the group mapping.
The Global Catalog

The Global Catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory Domain Services (AD DS) forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

Configuring LDAP

To configure the LDAP settings:

1. From the Security section of the Administration tab, select LDAP.

The LDAP page is displayed showing the LDAP tab.

![Graphic showing the main LDAP configuration screen.]

This graphic shows the main LDAP configuration screen.

The options on this page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Support</td>
<td>Select Enabled or Disabled to enable or disable LDAP support for this appliance.</td>
</tr>
<tr>
<td>Connection Status</td>
<td>Displays a message regarding the status of the connection to the LDAP server. For example:</td>
</tr>
<tr>
<td></td>
<td>• No LDAP operations performed (last update: timestamp)</td>
</tr>
<tr>
<td></td>
<td>• Invalid credentials (last update: timestamp)</td>
</tr>
<tr>
<td></td>
<td>• Connection established (last update: timestamp)</td>
</tr>
<tr>
<td></td>
<td>• Can't contact LDAP server (last update: timestamp)</td>
</tr>
<tr>
<td>Server URI</td>
<td>The address of the LDAP server to connect to. For example:</td>
</tr>
<tr>
<td></td>
<td>ldap://engineering.bmc.com:3268 or</td>
</tr>
<tr>
<td></td>
<td>ldaps://engineering.bmc.com</td>
</tr>
<tr>
<td></td>
<td>The default LDAP port is 389 and the default LDAPS port is 636.</td>
</tr>
<tr>
<td></td>
<td>For multiple (failover) LDAP servers, enter a space separated list of LDAP server URIs.</td>
</tr>
<tr>
<td></td>
<td>When using the Microsoft Active Directory group mode for LDAP, you can also use port 3268 to reference the Global Catalog. Check with your LDAP administrator to ensure that you use the correct port.</td>
</tr>
<tr>
<td>LDAPS</td>
<td>Displays a message regarding the CA certificate and provides controls enabling you to upload, remove or replace a certificate. Many large enterprises have their own CAs that will provide a root CA certificate which will allow the appliance to trust the LDAP server's certificate it receives over the network.</td>
</tr>
</tbody>
</table>
### Field Name | Details
--- | ---
To upload a certificate, click the Browse button, select the new certificate using the file upload dialog, then click Apply. To replace an existing CA Certificate, select the Remove CA Certificate check box and click Apply. When the page is refreshed, add the new certificate as above. You should contact your organization's LDAP administrator to obtain a CA certificate. Multiple CA certificates can be uploaded by concatenating into a single file prior to upload. Note that you cannot delete a CA certificate when LDAPS is enabled. Likewise, you cannot enable LDAPS without a CA Certificate loaded. In both these cases you will encounter a Cannot use LDAPS without a CA Certificate warning.

| Bind Username | The user name with which to connect to the LDAP server. For example, user01@bmc.com. |
| Bind Password | The password that corresponds to the user name entered in the **Bind Username** field. Check the box to modify the password. |
| Bind Timeout | The length of time that the appliance will wait before the login is assumed to have failed. |
| Search Base | The location in the directory from which the LDAP search begins. For example: dc=tideway,dc=com. This restricts the search to the tideway container in the directory information tree. |
| Search Template | Specifies the template to use to search for the user name in the LDAP database. For example: (userPrincipalName=%(username)s) This queries the LDAP database for the userPrincipalName attribute which is equal to %(username)s, which is the user name string entered at the login prompt. |
| Search Timeout | If no response is received from the server in this length of time, the query times out. Select a timeout value from the drop-down list. |
| Search Scope | Defines how deep to search within the search base. "Base", or zero level, indicates a search of the base object only. "One level" indicates a search of objects immediately subordinate to the base object, but does not include the base object itself. This is typically used to search for objects immediately contained in the search base level. "Sub Tree" indicates a search of the base object and the entire subtree of which the base object distinguished name is the topmost object. Select the required scope from the drop-down list. |
| User Cache Timeout | The appliance queries the LDAP server for user information and caches the results to avoid overloading the LDAP server. Select a timeout value from the drop-down list. Note that values less than 10 minutes are not recommended. You can also clear the cache manually using the Flush Cache button. |
| Group Cache Timeout | The appliance queries the LDAP server for group information and caches the results to avoid overloading the LDAP server. Select a timeout value from the drop-down list. Values less than 1 hour are not recommended. You can also clear the user and group cache manually using the Flush Cache button. |
| Group Mode | The group mode determines the way that the LDAP server is queried for group information, it should match the LDAP server used by your organization. Select one of the following LDAP server types from the drop-down list:  
- Microsoft Active Directory  
- SunONE Directory Server  
- Other |
### Group Attribute on User node
The LDAP attribute name to search for when running a group query. The attribute is on the User node, and provides a list of distinguished names of groups that the user belongs to. For example, the attribute might be called "memberOf" and contain data such as "cn=sales,ou=groups,dc=bmc,dc=com". This field is user editable when the Other Group Mode is selected from the Group Mode drop-down (if the User node does not contain such an attribute, this field should be empty so the Membership Attribute on Group node will be used instead). When any other mode is selected the field is automatically populated.

### Group Query
The LDAP query that is used to find Group objects. It is usual to match the nodes’ Object Class, for example: (objectclass=group). This field is user editable when the Other Group Mode is selected from the Group Mode drop-down. When any other mode is selected the field is automatically populated.

### Membership Attribute on Group node
The LDAP attribute name to search for to determine whether an individual is a member of a group. The attribute is on the Group nodes, and provides a list of names of users. For example, the attribute might be called "member". This field is user editable when the Other Group Mode is selected from the Group Mode drop-down. When any other mode is selected the field is automatically populated.

 halls: To save the LDAP settings, click **Apply**.

### Changing from LDAPS to LDAP
When you reconfigure BMC Atrium Discovery to use LDAP when it was previously configured to use LDAPS, you must remove the CA Certificate, and change the URI in a single step otherwise you will encounter a Cannot use LDAPS without a CA Certificate warning. To do this:

1. Edit the URI to point to the LDAP server’s ldap:// URI. *Do not click Apply button yet.*
2. Select **Remove CA Certificate**.
3. Click **Apply**.

### Changing from LDAP to LDAPS
When you reconfigure BMC Atrium Discovery to use LDAPS when it was previously configured to use LDAP, you must add a CA certificate before you attempt to enter an ldaps:// URI.

### LDAP group mapping
The LDAP group mapping enables you to assign membership of BMC Atrium Discovery groups to LDAP groups. If you do not use group mapping, users will be only be assigned to groups in BMC Atrium Discovery which are exactly the same as the LDAP groups that they are members of, that is, in LDAP form `dc=tideway,dc=com,ou=engineering`....

To configure the LDAP group mapping settings:

1. From the LDAP page, select the **Group Mapping** tab.

   ![Group Mapping Tab](image)

   This graphic shows the LDAP Groups tab.
The LDAP Group Mapping page lists the LDAP groups that are assigned to BMC Atrium Discovery security groups. For each LDAP group, the appliance security groups to which it is assigned are listed. Links for each action that you can perform are provided for each group.

2. Select **Enabled** or **Disabled** from the drop-down list to enable or disable LDAP group mapping.

   For each LDAP group listed, an edit link and a delete link are provided.
   - To remove the LDAP group mapping, click **Delete**.
   - To edit the security groups mapped to an LDAP group, click **Edit**.
     
     **Add** enables you to add a new group mapping. To do this:

3. Click **Add**.

4. On the Add LDAP Group Mapping page, enter a search term for the common name into the LDAP Group field and click the **Search** button. A list of matches is displayed. If more than ten entries match, the first ten are shown and a label is displayed at the bottom of the list showing how many additional matches there are.

   Select the matching LDAP group from the list. The LDAP groups field is not case sensitive. If you use any upper case characters, their case is ignored. All LDAP groups returned from the LDAP server are displayed in lower case.

5. Select the appliance security groups to which you want to assign the LDAP group.

6. To save the mapping, click **Apply**.

**Troubleshooting**

If you receive a Can't Contact LDAP Server error in the Connection Status field, this may be caused by certificate problems rather than simple connectivity (wrong URI, port and so forth). Check that the certificate you are using is the one you received from your LDAP administrator.

If the login fails when attempting LDAP authentication, set the security log `/usr/tideway/log/tw_svc_security.log` level to debug.

Where the account used to bind to the directory fails to authenticate look for messages similar to the following:

```
-1285350512: 2010-08-13 10:00:46,843: security.authenticator.ldap: DEBUG: Attempt to auth
-1285350512: 2010-08-13 10:00:47,117: security.authenticator.ldap: DEBUG: LDAP passwd for "CN=Administrator,CN=Users,DC=generic,DC=com" not valid
```

If you are using group mapping and are experiencing login failures, check that the groups have been correctly defined. The security log shows the list of groups that the user is assigned to, if the list is empty, no groups have been mapped and no login is possible.

```
-1306330224: 2010-08-13 10:01:54,253: security.validator.ldap: DEBUG: LDAP.permitted(): Final mapped group list for user Administrator is 
```

Web authentication

BMC Atrium Discovery supports a number of web authentication plugins. You can view and configure these on the Web Authentication Methods Page. The following web authentication methods are supported:

- **SSL Client Certificate Verification**: The client's SSL Certificate is verified by the web server. The user name is extracted from the certificate and used for authorization via LDAP. Requires HTTPS and LDAP support.
- **SSL Certificate Lookup**: The user is authenticated by looking up custom parts of the client's SSL Certificate via LDAP. The certificate is not verified, but it must be valid. Requires HTTPS and LDAP support.
- **RSA SecurID Authentication**: Authentication is performed by the RSA Authentication Agent. The username is used for authorization via LDAP. Requires HTTPS and LDAP support.
- **Standard Atrium Discovery Web Authentication**: The user is authenticated by entering a user name and password via the Login page. Supports authentication via LDAP, if LDAP support is enabled.

To configure the web authentication settings

1. From the Security section of the Administration tab, select Web Authentication.
2. In the Web Authentication Methods page, you can choose the order in which the methods will be attempted, and you can enable, disable, and configure each one. The Standard Atrium Discovery Web Authentication module is a special case, it cannot be disabled and acts as the fail safe login.
3. For each authentication module, except for the Standard Atrium Discovery Web Authentication module, the following controls are provided:
   - Disable link: click this link to disable the module. When a module is disabled, the link is replaced with an Enable link.
   - Configure link: click this link to open a dialog box to configure the module. These dialogs are described in the following sections.
   - Ordering controls: click the up or down arrow to move the module up or down. Click the barred up or down arrow to move the module to the top or bottom.

The page also provide links to the configuration pages for HTTPS and LDAP.

To configure SSL client certificate verification

This module verifies the client SSL certificate with the web server. If the certificate is valid, the user name is extracted and used for LDAP authorization.

Click Configure in the SSL Client Certificate Verification row.

There is a single editable field in the configure page, this is the Extract Key which is used to extract the user name. The default is emailAddress which is used when the email address is the user name.
If the user name is not the email address, enter a new extract key to get the user name. This must match the search template used in the LDAP settings.

**SSL certificate lookup**

This module extracts information from the client SSL certificate and verifies it against the LDAP server.

Click **Configure** in the SSL Certificate Lookup row.

There are two editable fields:

- **Lookup Expression**: an LDAP search expression. The variables you can use are:
  
<table>
<thead>
<tr>
<th>HTTPS</th>
<th>SSL_PROTOCOL</th>
<th>SSL_SESSION_ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_CIPHER</td>
<td>SSL_CIPHER_EXPORT</td>
<td>SSL_CIPHER_USEKEYSIZE</td>
</tr>
<tr>
<td>SSL_CIPHER_ALGKEYSIZE</td>
<td>SSL_VERSION_INTERFACE</td>
<td>SSL_VERSION_LIBRARY</td>
</tr>
<tr>
<td>SSL_CLIENT_M_VERSION</td>
<td>SSL_CLIENT_M_SERIAL</td>
<td>SSL_CLIENT_S_DN</td>
</tr>
<tr>
<td>SSL_CLIENT_S_DN_x509</td>
<td>SSL_CLIENT_I_DN</td>
<td>SSL_CLIENT_I_DN_x509</td>
</tr>
<tr>
<td>SSL_CLIENT_V_START</td>
<td>SSL_CLIENT_V_END</td>
<td>SSL_CLIENT_A_SIG</td>
</tr>
<tr>
<td>SSL_CLIENT_A_KEY</td>
<td>SSL_CLIENT_CERT</td>
<td>SSL_CLIENT_CERT_CHAINn</td>
</tr>
<tr>
<td>SSL_CLIENT_VERIFY</td>
<td>SSL_SERVER_M_VERSION</td>
<td>SSL_SERVER_M_SERIAL</td>
</tr>
<tr>
<td>SSL_SERVER_S_DN</td>
<td>SSL_SERVER_S_DN_x509</td>
<td>SSL_SERVER_I_DN</td>
</tr>
<tr>
<td>SSL_SERVER_I_DN_x509</td>
<td>SSL_SERVER_V_START</td>
<td>SSL_SERVER_V_END</td>
</tr>
<tr>
<td>SSL_SERVER_A_SIG</td>
<td>SSL_SERVER_A_KEY</td>
<td>SSL_SERVER_CERT</td>
</tr>
</tbody>
</table>

  These are the Apache mod_ssl variables. See the Apache website for more information.

- **LDAP Attribute**: the LDAP attribute against which to check the user name.

**To configure RSA SecurID authentication (8.3 SP3 only)**

BMC Atrium Discovery can use an RSA SecurID server to perform authentication. To do this you must first install the **RSA Authentication Agent 7.1 for Web for Apache Web Server** on the appliance, configure it to access your RSA Authentication Manager, and test to ensure that it is working. See the RSA documentation for instructions on how to do this.

**Cannot use system and other standard users**

You cannot access the system user and the other standard users unless they have an exactly corresponding RSA/LDAP user. You must create an RSA/LDAP user with permissions exactly corresponding to any default users that you use.

To configure RSA SecurID authentication:
1. Log in to the BMC Atrium Discovery UI using an LDAP account with permissions equivalent to the system user. Ensure you can access the Administration -> Web authentication page while logged in as this user.

2. Click **Configure** in the RSA SecurID Authentication row.
   There is a single editable field in the configure page, this is the Logout URL which is required to logout via the web authentication framework. The default is `/webauthentication?logoff?referrer=/ui`.

3. Log out of the BMC Atrium Discovery UI.

4. Install and configure the RSA Authentication Manager according to the instructions in the download.
   - During the configuration of RSA SecurID, "Use RSA Token for Cross-Site Request Forgery Protection" must be set to disabled otherwise logging out from the BMC Atrium discovery UI will fail.
   - The installation requires that some environment variables are configured. These variables should be appended to `/etc/sysconfig/httpd`. A typical entry looks like this:

```
# RSA enablement
export VAR_ACE=/var/ace
export LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/etc/httpd/rsawebagent
```

   - If the appliance is a virtual machine and you use VMware snapshots, you should ensure that you update the snapshot after configuring the RSA Authentication Manager. Rolling back to an earlier snapshot removes the shared secret and prevents subsequent log ins. See the RSA Authentication Manager documentation for more information.

5. Navigate to the BMC Atrium Discovery URL. You are presented with the RSA SecurID login page.

6. Log in using the same LDAP account with permissions equivalent to the system user. You are now presented with the standard BMC Atrium Discovery login page.

7. Log in to BMC Atrium Discovery with the same LDAP account as you used in the previous step.

8. Navigate to the Administration -> Web authentication page and enable the RSA SecurID integration.
   If you cannot access the Administration -> Web authentication page, you must log out of BMC Atrium Discovery, log back in as the system user, and grant sufficient permissions to the RSA/LDAP user to access that page.
Once RSA SecurID Authentication is enabled in BMC Atrium Discovery, the BMC Atrium Discovery login screen is no longer displayed. To login, enter your username, password, and code from the SecurID token in the RSA SecurID login screens. You are authenticated against the RSA Authentication Manager, and once authenticated you are logged into BMC Atrium Discovery using the same username.

If RSA SecurID Authentication is not enabled, the normal BMC Atrium Discovery login page is displayed, even after successfully logging in using the RSA Authentication Agent. If RSA SecurID Authentication is enabled in ADDM, but the RSA Authentication Agent is not installed or is installed incorrectly, the normal BMC Atrium Discovery login page is also displayed.

**Standard Atrium Discovery web authentication**

No configuration is required for the Standard Atrium Discovery Web Authentication section, it is the fail-safe method of logging in to the system. This authentication method uses local users created on the appliance.

**Viewing active sessions**

Multiple users may be logged into the BMC Atrium Discovery user interface (UI) concurrently. You can check who is logged on and see details of their session using the Active Sessions page.

To view the Active Sessions page:

1. From the Security section of the Administration tab, select **Active Sessions**.

   The Active Sessions page contains the following information on each user logged in to the UI:

   - **User**: the user name of the user logged in.
   - **IP Address**: the IP address that the browser is reporting.
   - **Browser**: information on the browser, such as: type, major version, platform, language, version and so on.
   - **Login Time**: the time that the user logged in to the UI.
   - **Last URL Accessed**: the last URL that the user accessed.
   - **Last Access Time**: the time that the user last performed an action in the UI.

**Appliance audit**

Users with sufficient privileges can modify an appliance configuration in ways which could affect the appliance or the customer environment. The appliance audit feature enables you to track changes to the appliance's configuration. All user-initiated events that modify the state or the behavior of the appliance are logged.

To use the appliance audit feature, you must be logged in as a system user. If you are not a member of this group you are shown the message, You do not have permission to run audit reports.
Reporting on audit events

You can configure the actions that will occur when the appliance status changes. To do this:

From the Security section of the Administration tab, select Audit.

To Search for events, enter search criteria in all or some of the following fields:

- **From**: the start date and time of the search. The default for this field is 24 hours before the page was loaded.
- **To**: the end time and date of the search. The default for this is to display the following text in the To fields: Day Month Year hh mm. This means that the logs will be searched up to the current time.
- **User ID**: a filter to search only for events logged to a particular user, for example, the reporter user.
- **Event group**: a drop-down filter to search only for events belonging to a particular event group or category. The event group provides a means for viewing related event types. See Event Groups for a list of event groups.
- **Events**: a drop-down filter to search only for events of a specified type.

When you have entered the search criteria, click Run to start the search. The page is refreshed to show a results table below the search panel.

You can only search the logs through the user interface (UI) using the fields in the Search audit records page. However, if you export the Results List by clicking Export as CSV, you can use a spreadsheet or text editor to perform detailed searches on the data. For example, you can search for events on a specific host.

Click Export as CSV and choose a location to save the file.

Each item in the result row is a hyperlink to the detailed record of the event.

The record data is divided into two sections:

- Standard Details
- Additional Details

**Standard details**

The standard details that are recorded for every event are described in the table below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event</td>
<td>The type of event.</td>
</tr>
<tr>
<td>Event Group</td>
<td>The event group to which this event belongs. The purpose of the event group is to provide a filter for viewing related event types.</td>
</tr>
<tr>
<td>User</td>
<td>The user ID who initiated the event.</td>
</tr>
<tr>
<td>Full Name</td>
<td>The full name of the user who initiated the event.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Groups</td>
<td>The name of the groups the user who initiated the event belongs.</td>
</tr>
<tr>
<td>When</td>
<td>When the event was logged.</td>
</tr>
<tr>
<td>Summary</td>
<td>Summary description of the event.</td>
</tr>
</tbody>
</table>

### Additional details

The details shown in the Additional Details section varies from event to event. For example, the following information is provided for a Windows proxy that has been pinged:

- IP Address
- Port
- Windows proxy Name
- Windows proxy Type

### Event groups

Audited events are collected into the following groups:

- Appliance Config
- Audit Log
- Consolidation
- DIP
- Datastore Edit
- Discovery Config
- Discovery Ruleset
- ECA Reasoning
- Search
- Security
- Windows proxy
- UI Access
- cmdb-export

The events that belong to these groups are described in Audit Categories and Events.

### Purging the audit Log

You can purge the audit log of all events that are over one month old. Events less than one month old cannot be deleted. You can purge events using the Audit Purge page. To access the Audit Purge page, from the Audit section of the Administration tab, select Purge.

In the Audit Purge page, the log name, number of events, and the date and time of the oldest record is displayed. A selection drop-down list is displayed which enables you to select the purge until date. The following options are available:
- 1 month ago
- 3 months ago
- 6 months ago
- 12 months ago
- 24 months ago

This ensures that there is a minimum retention period of one month. Click **Purge** to purge the archive up to the Purge until date selected. When you click **Purge**, the operation commences immediately. You can navigate away from the page and continue with other tasks. Purging archive information is also an auditable event. Therefore, after a purge, the newest event is a record of that purge.

⚠️ There is no automatic purge of the audit information. When the audit information on the appliance becomes very large, you can use the appliance snapshot feature to create an archive.

A typical number of auditable events is approximately 1000 per day. This equates to approximately 90 000 events in three months. When deleting events, you can typically remove 500 events per second. Deleting 60 000 or more events will result in the browser timing out, however, the process continues.

### Audit categories and events

The following sections list the events that are in each event category:

#### Appliance Config Events

- change_password
- administration_move_up
- administration_move_down
- appliance_config_modify
- appliance_reboot_request
- appliance_restart_request
- appliance_shutdown_request
- appliance_mail_settings_modify
- appliance_name_resolution_modify
- baseline_actions_change
- baseline_change
- baseline_config_change
- baseline_options_change
- gather_create
- gather_delete
- loglevel_change
- maintenance_mode_enable
- maintenance_mode_disable
- mass_delete
- partition_create
- partition_destroy
- partition_purge
- partition_rename
- portal_add
- portal_delete
- portal_rename
- portal_section_add
- portal_section_del
- portal_section_move
- snapshot_component_migrate
- snapshot_create
- snapshot_delete
- snapshot_download
- snapshot_import
- snapshot_migrate
- snapshot_restore_accept
- snapshot_restore_request
- snapshot_upload
- system_settings_change

**Audit Log Event**

- purge_audit_log

**Consolidation Events**

- consolidation_approved_da
- consolidation_autoapproved_da
- consolidation_registered_da
- consolidation_registered_to_ca
- consolidation_released_da
- consolidation_removed_da
- consolidation_set_as_consolidation
- consolidation_set_as_discovery
- consolidation_unregistered_from_ca
DIP Event

- test_static_connection

Datastore Edit Events

- datastore_add_node
- datastore_add_relationship
- datastore_modify_node
- datastore_remove_node
- datastore_remove_relationship

Discovery Config Events

- commands_modify_command_modify
- commands_modify_path_modify
- commands_reset_command_reset
- commands_reset_path_reset
- credentials_add
- credentials_delete
- credentials_expire
- credentials_modify
- credentials_move_down
- credentials_move_first
- credentials_move_last
- credentials_move_up
- credentials_password
- credentials_test
- discovery_config_option_modify
- external_windows_proxy_add
- external_windows_proxy_modify
- external_windows_proxy_move_down
- external_windows_proxy_move_first
- external_windows_proxy_move_last
- external_windows_proxy_move_up
- external_windows_proxy_ping
- external_windows_proxy_remove
- filters_add
- filters_modify
- filters_delete
- filters_ordering
modify_command
modify_discovery_config_option
modify_path
ports_add
ports_modify
ports_delete
protocol_probing_add
protocol_probing_modify
protocol_probing_delete
protocol_probing_reordering
range_exclusion_add
range_exclusion_del
exclude_ranges_modify
reset_command
scan_level_modify
scanning_emergency_stop_request
scanning_start_request
scanning_stop_request
scheduled_scan_add
scheduled_scan_remove
snapshot_scan_add
snapshot_scan_remove
test_snmp_login_cred

Discovery Ruleset

ruleset_add
ruleset_delete_request
ruleset_modify
rulesets_run_request

ECA Reasoning

ECA_activate_pattern_package
ECA_add_event
ECA_add_pattern_package
ECA_commit_pattern_state
ECA_deactivate_pattern_package
ECA_delete_pattern_package
ECA_disabled_pattern_module
ECA_enabled_pattern_module
ECA_execute_pattern
• ECA_modify_pattern_config
• ECA_remove_event
• ECA_reset_engine
• ECA_scan_levels
• ECA_start_engine
• ECA_stop_engine
• ECA_test_pattern_state

Search

• search_query

Security Events

• security_add_group
• security_add_ldap_group
• security_add_user
• security_delete_group
• security_delete_ldap_group
• security_delete_user
• security_edit_ldap_group
• security_group_permissions_modify
• security_modify_user
• security_options_modify
• security_user_change_password
• security_user_state_modify
• https_config_change
• password_management_policy_add
• password_management_policy_delete
• password_management_policy_expired
• password_management_policy_modify

Windows proxy events

• external_windows_proxy_add
• external_windows_proxy_modify
• external_windows_proxy_move_down
• external_windows_proxy_move_first
• external_windows_proxy_move_last
• external_windows_proxy_move_up
• external_windows_proxy_ping
• external_windows_proxy_remove
• windows_proxy_conf_reload
• windows_proxy_conf_reload_failure
• windows_proxy_conf_upload
• windows_proxy_conf_upload_failure
• windows_proxy_loglevel_change
• windows_proxy_modify_no_permission
• windows_proxy_process_terminate
• windows_proxy_read_no_permission
• windows_proxy_setting_update
• windows_proxy_sign_conf_modify

UI Access Events

• logoff
• logon
• logon_failure

cmdb-export Events

• export_starting
• export_add_to_mapping_set
• export_create_exporter
• export_create_mapping_set
• export_delete_adapter_config
• export_delete_exporter
• export_delete_mapping_set
• export_save_exporter_config
• export_update_adapter_config
• export_update_mapping_set
Maintaining the appliance

The BMC Atrium Discovery appliance requires little daily maintenance; however, a maintenance mode is provided that only system users can access to perform tasks such as rebooting or shutting down the appliance. In this mode, you can also take appliance snapshots, and configure the way the system is monitored and audited.

- Maintenance mode
- Rebooting or shutting down the appliance
- Using appliance snapshot
- Baseline configuration
- Configuring dependency visualizations
- Configuring model maintenance settings
- Configuring audit, snapshot and application options
- Configuring the NTP client
- Using command line utilities

Maintenance mode

Maintenance mode is a user mode in which the only users permitted are users who are members of the system group. All users who are not members of this group are logged off the appliance and an explanatory message is displayed.

Putting the appliance into maintenance mode

You must be logged in as a user who is a member of the system group to see the Set Maintenance Mode button.

To put the appliance into Maintenance Mode:

1. From the Appliance section of the Administration tab, select Control. The Appliance Control page is displayed.
2. Click Set Maintenance Mode.
3. The appliance is placed into maintenance mode. All users who are not members of this group are logged off. System group users' screens are refreshed and a button, Quit Maintenance Mode, is displayed.

Maintenance Mode is not a single user mode. If you are performing any tasks which could affect other users, such as appliance snapshots, you should ensure that you are the only logged in user. Use the Administration => Security => Active Sessions window to verify this.
In maintenance mode, a flashing banner is displayed at the top of all pages. The flashing banner is a link to the Appliance Control page.

To leave maintenance mode, click **Quit Maintenance Mode**.

![Warning]

When non-system users are logged out, the login banner is displayed with an "under maintenance" message. When logging into an appliance that is in maintenance mode, you should ensure that your work does not interfere with that of other logged in users. For example, the appliance may be in maintenance mode so that an appliance snapshot can be taken.

**Controlling the appliance**

**Rebooting the appliance**

You must be logged in as a user who is a member of the system group to reboot the appliance.

1. From the Appliance section of the **Administration** tab, select **Control**.
   
   The Appliance Control page is displayed.

2. Click **Reboot**.

3. You are asked to confirm the reboot action.

   If you choose to reboot the appliance, a reboot countdown page is displayed and after 600 seconds, you will be returned to the login page.

**Shutting down the appliance**

You must be logged in as a user who is a member of the system group to shut down the appliance.

1. From the Appliance section of the **Administration** tab, select **Control**.

   The Appliance Control page is displayed.

2. Click **Shutdown**.

3. You are asked to confirm the shutdown action.

   If you choose to shut down the appliance, you will require full security access rights to restart the appliance.
Rebooting or shutting down the appliance

Controlling the appliance

The Appliance Control page enables you to restart the tideway services (required for changing certain discovery settings), reboot or shutdown the appliance, and put the appliance into Maintenance mode.

For all of these operations you must be logged in as a user who is a member of the system group.

Restarting the services

Restarting the services is required when changing certain settings on the appliance, for example, many discovery settings.
You must be logged in as a user who is a member of the system group to restart the services.

1. From the Appliance section of the Administration tab, select Control.
   The Appliance Control page is displayed.
2. Click Restart Services.
3. You are asked to confirm the restart services action.

Rebooting the appliance

You must be logged in as a user who is a member of the system group to reboot the appliance.

1. From the Appliance section of the Administration tab, select Control.
   The Appliance Control page is displayed.
2. Click Reboot.
3. You are asked to confirm the reboot action.
   If you choose to reboot the appliance, a reboot countdown page is displayed and after 600 seconds, you will be returned to the login page.

Shutting down the appliance

You must be logged in as a user who is a member of the system group to shut down the appliance.

1. From the Appliance section of the Administration tab, select Information.
   The Appliance Information page is displayed.
2. Click Shutdown.
3. You are asked to confirm the shutdown action.

⚠️ If you choose to shut down the appliance, you will require full security access rights to restart the appliance.
Putting the appliance into maintenance mode

You must be logged in as a user who is a member of the system group to see the Set Maintenance Mode button.

To put the appliance into Maintenance Mode:

1. From the Appliance section of the Administration tab, select Control. The Appliance Control page is displayed.
2. Click Set Maintenance Mode.
3. The appliance is placed into maintenance mode. All users who are not members of this group are logged off. System group users' screens are refreshed and a button, Quit Maintenance Mode, is displayed.

- Maintenance Mode is not a single user mode. If you are performing any tasks which could affect other users, such as appliance snapshots, you should ensure that you are the only logged in user.
  Use the Administration => Security => Active Sessions window to verify this.

In maintenance mode, a flashing banner is displayed at the top of all pages. The flashing banner is a link to the Appliance Control page.

To leave maintenance mode, click Quit Maintenance Mode.

- When non-system users are logged out, the login banner is displayed with an "under maintenance" message. When logging into an appliance that is in maintenance mode, you should ensure that your work does not interfere with that of other logged in users. For example, the appliance may be in maintenance mode so that an appliance snapshot can be taken.

Disk space monitor

To prevent problems that may occur if the disk containing the datastore or the datastore logs runs out of space, a disk space monitor is used. If there is less than a predefined amount of space on either of the disks, the monitor shuts down BMC Atrium Discovery gracefully, or prevents it starting. If this occurs you must create more space before you can use BMC Atrium Discovery again.

By default the minimum amount of space permitted on either disk is 1024MB.

If the disk space monitor shuts down BMC Atrium Discovery because the datastore disk has less than 1024MB free space, you should run the datastore compaction tool.

If the disk space monitor shuts down BMC Atrium Discovery, you should log into the appliance and free up some disk space. Possible areas are:
• Log files: see Log files for a description and the location of the main log files. BMC Atrium Discovery is not reliant on these log files and they may be safely deleted. The other log files must not be deleted, modified or moved.
• Cores: check that there are no old cores in $TIDEWAY/cores
• Snapshots: old snapshots in $TIDEWAY/var/snapshot/snapshots
• Workspaces: any areas that you have used as workspaces or staging areas for exports.

Using appliance snapshot

Appliance snapshot enables you to:

• take a snapshot of the datastore
• capture critical configuration files
• support disaster recovery between appliances
• archive snapshots off the appliance

⚠️ Warning

Appliance snapshot and restore functionality can be used only with the same versions of BMC Atrium Discovery. The feature is not designed to backup and restore a complete appliance including the operating system and the BMC Atrium Discovery application. You should use the VMware features to backup or restore the entire appliance.

The following items are included by default in a snapshot:

• From $TIDEWAY/var/tideway.db/data, the critical files of the datastore:
  • the data files
  • the log files (These are non-optional log files. Never delete or modify these files.)
• From $TIDEWAY/etc
  • All configuration files (*.conf)
  • User information (users.db)
  • Group information (groups.db)
  • Security information (security.db)
  • Port information (portdb.xml)
  • Credentials vault (tideway.vault)
• From $TIDEWAY/bin
  • All tideway binaries (tw_*)
  • All shell scripts (*.sh)
• Customer data: $TIDEWAY/data/customer
• Taxonomy extensions: $TIDEWAY/data/custom/taxonomy/extensions.xml
Any items that you want to ensure are archived as part of a snapshot that are particular to your installation of BMC Atrium Discovery should be stored in the directory provided for customer data – $TIDEWAY/data/customer.

The items included in a snapshot are configured using the $TIDEWAY/etc/archive_conf.xml file. You do not need to edit this file. However, if you make changes in this file, make sure that you add new repository sections rather than edit existing ones.

⚠️ **Appliance email settings**

Appliance snapshot does not preserve the BMC Atrium Discovery email settings. Before making a snapshot, make a note of the settings so that you can reconfigure the email settings after restoring the snapshot.

### Archive disk space limit

There is a limit to the amount of disk space that the archive can use. When this limit is passed the archive memory information is highlighted and **Create** on the user interface (UI) is dimmed. If this happens, you must delete some or all of the archived data in order to continue using the appliance database snapshot.

The actual amount of disk space required is at least twice the size of the database being archived. This is because a copy of the datastore is made and that copy is compressed. If insufficient diskspace is available, the error message reports the amount of space available and the amount of space required.

### Creating a new appliance snapshot

To create an appliance snapshot you must place the appliance into maintenance mode and stop discovery. For more details, see [Putting the Appliance into Maintenance Mode](#) and [Controlling discovery](#).

⚠️ **Warning**

Maintenance Mode is not a single user mode. If you are performing any tasks which could affect other users, such as appliance snapshots, you should ensure that you are the only logged in user.

Before you create the new snapshot, view the currently active sessions to ensure that you are the only user that is logged in.
To create a new snapshot

1. From the Appliance section of the Administration tab, click Control.
2. On the Appliance Control page, click Set Maintenance Mode to place the appliance into the maintenance mode.
3. Select Snapshot & Restore from the Appliance menu to display the Appliance Snapshot page. If discovery is still running or the appliance is not in maintenance mode at this stage, a pop-up warning is displayed. When you dismiss this warning, the Appliance Snapshot window is displayed, though all buttons are inoperative. Depending on the warning, see Putting the Appliance into Maintenance Mode or Stopping the Discovery Process for more information.
4. In the Create New section, specify the name of the snapshot to be saved in the field for Name, and record any notes applicable to the snapshot to be saved in the field for Notes. Each snapshot also records the date and the time it was taken. The size of the snapshot is displayed to enable you to make informed decisions about managing the archive.
5. Click Create.

A confirmation screen displays.

Warning

This process can take a few minutes. Do not refresh or navigate away from this page during this process.

When the snapshot is completed, the Appliance Snapshot page is redisplayed showing the newly created snapshot.

Migrating your appliance snapshot to another appliance

You can move your snapshot between appliances of the same version.

Moving a snapshot to another appliance

The label Download refers to copying the snapshot to a destination appliance. This may be counter intuitive.

1. From the Utilities section, click Download.
2. Enter the following details in the Download Snapshot pop-up window:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Target IP</td>
<td>The IP address of the destination appliance.</td>
</tr>
<tr>
<td>Target User</td>
<td>The user account to access the destination appliance.</td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
Target Password | The corresponding password.
Target Archive Root | The directory into which to copy the snapshot. For migration this is $TIDEWAY/var/snapshot/snapshots/

3. Click **Download** on the pop-up window.
   An operation log window is displayed indicating whether the operation was successful or not, and providing information about any errors that may have occurred.
   If successful, your appliance snapshot has now been copied to your destination appliance and can be seen in the Appliance Snapshots section of the main page.

4. On the destination appliance, click **Restore** next to your selected snapshot to restore to the migrated snapshot.

5. On the WARNING pop-up screen, select the check box for one or all of the following:
   - Create Rollback Snapshot: to create a snapshot that you can roll back to before attempting to restore a snapshot.
   - Preserve Current Config Files: to prevent the new snapshot overwriting the current configuration files.

   **Note**
   If you do not select the Preserve Current Config Files option, the current configuration of the target appliance will be replaced with those from the snapshot; including such items as the appliance name, SMTP settings and so forth.

   - Restore discovery run state from snapshot: to restore the state of the discovery run that was preserved in the appliance snapshot.
   
   The Automatic Rollback Timer option enables you to set the time that you have in minutes before the snapshot is automatically rolled back to its previous state. There is a list on the UI where you can select 3, 5, 10, 15, and 60 minutes, where 5 minutes is the default setting.

6. After you select your options, click **Restore** on the pop-up window.

   **Warning**
   This process can take a few minutes. Do not refresh or navigate away from this page during this process.

   The Confirm Restore screen is displayed.
   The restore commences and the BMC Atrium Discovery software restarts. When you login again you are returned to the Home Page.
7. From the Appliance section of the **Administration** tab, select **Snapshot & Restore**.
8. Click either **Confirm Restore** in the pre-set time period to prevent Automatic Rollback, or **Cancel** to rollback the restore.

### Warning

You must click **Confirm Restore** to keep the restored snapshot.

If you click **Cancel**, it causes the snapshot to rollback. The snapshot is marked as invalid and **Restore** is dimmed. An Alert icon is displayed which, when clicked, shows the name and the states the reason why it has cancelled Restore. If you want to override a cancel, click **Mark Valid**.

9. In the Utilities section, click **Restore Log** to view details of the restore operation. If a problem occurs during snapshot processing, an alert icon will appear next to that particular log. An alert log icon will also appear if an invalid IP Address is entered for the migration.

### Uploading and downloading snapshots

In the Utilities section, **Upload** (copy from an SSH server) and **Download** (copy to an SSH server) enable you to take snapshots on or off the appliance.

### Note

To use the upload and download features, your target must be an SSH server.

#### Downloading a snapshot from the appliance to an SSH server

The label **Download** refers to copying the snapshot to a destination SSH server. This may be counter intuitive.

1. From the Utilities section, click **Download**.
2. Enter the following details in the Download Snapshot pop-up window:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download Target IP</td>
<td>The IP address of the destination SSH server.</td>
</tr>
<tr>
<td>Target User</td>
<td>The user account to access the destination SSH server.</td>
</tr>
<tr>
<td>Target Password</td>
<td>The corresponding password.</td>
</tr>
<tr>
<td>Target Archive Root</td>
<td>The directory into which to copy the snapshot.</td>
</tr>
</tbody>
</table>

3. Click **Download** on the pop-up window.
On completion, an operation log window is displayed indicating whether the operation was successful or not, and providing information about any errors that may have occurred.

Uploading a snapshot to the appliance from an SSH server

The label Upload refers to copying the snapshot from an SSH server. This may be counter intuitive.

1. From the Utilities section, click Upload.
2. On the Upload Snapshot pop-up window, next to Upload Target IP, enter the IP address for the SSH server.
3. Enter the Target User (the user account name) and the user account password next to Target Password.
   The Target Archive Root is the directory under which snapshots are saved.
   The Snapshot ID is a unique identifier created using the date and time of the snapshot creation in the form: YYYY-DD-MM_hhmmss. Snapshots are saved in a directory of this name under the target archive root directory.
4. Click Upload on the pop-up window.

On completion, an operation log window is displayed indicating whether the operation was successful or not, and providing information about any errors that may have occurred.

Scheduled appliance snapshot

The scheduled appliance snapshot feature enables you to use the cron feature to schedule appliance snapshots. The script should be scheduled using the cron feature ($TIDEWAY/etc/cron) as the tideway user.

Appliance snapshot requires Discovery to be stopped and the appliance put into maintenance mode. For more information see Putting the Appliance into Maintenance Mode. If the script is configured and scheduled, you can prevent it running by putting a file called .nosnap in the $TIDEWAY/var/ directory. If this file is present, the script will not perform any operations. You can also create and delete this file through the user interface. Enter the following URL:

http://appliance/ui/SetupSnapshotSchedule

where appliance is the name or IP address of the appliance. The Appliance Scheduled Snapshot page is displayed which contains an Enable or Disable Scheduled Snapshot toggle button. Click the button to enable or disable the scheduled appliance snapshot feature.

Using the snapshot utility

The snapshot utility $TIDEWAY/bin/tw_scheduled_snapshot is used to create and transfer appliance snapshots. With the utility, you can:

- Create named snapshots and include notes
- Transfer the snapshot to another appliance or to a remote host running SSH
Delete the local copy of the snapshot after it has been transferred to a remote host or another appliance.

BMC Software recommends that you enable the migrate user when you transfer snapshots onto an appliance using the command line. This user has a home directory that is the default location for uploading snapshots, and it has limited access to the appliance. See The migrate user for information.

For more information about the utility and the available options, see tw_scheduled_snapshot.

### Baseline configuration

The appliance status is displayed in the Appliance Status icon in the dynamic toolbox. It is displayed as a Status link next to a traffic light symbol which shows the overall status of the appliance. See Appliance status for more information.

#### Appliance Status Drop-down

A drop-down dialog is displayed when you click **Appliance Status** in the dynamic toolbox. It shows the following information:

- **Appliance Name**: the name of the appliance
- **Appliance Time**: the time read from the appliance’s internal clock
- **ECA Engines**: the number of ECA engines running. You cannot change the number of ECA engines, but it affects the maximum number of concurrent discovery requests. For more information, see Discovery.

The link description is one of the following:

- **No Problems Detected**: The status is green. No problems have been detected.
- **Status Information Available**: The status is green, but at least one potential problem has been detected which has an information level message.
- **Minor Problems Detected**: At least one minor problem has been detected with your appliance.
- **Major Problems Detected**: At least one major problem has been detected with your appliance.
- **Critical Problems Detected**: At least one critical problem has been detected with your appliance.

One or more of the following actions can be configured to occur if the appliance status is reported as critical, major, or minor.

- Send Email
- Restrict Network Access
- Stop Discovery
You can configure the precise levels at which states change. This is described in the following section.

**Configuring appliance status options**

You can configure the appliance baseline options such as the recipients of automatic emails, and the messages to be included. You must have setup email on the appliance before using this feature. See Setting Up Appliance Mail Settings for more information.

To do this:

1. From the Appliance section of the **Administration** tab, select **Baseline Status**. The Appliance Baseline page is displayed.
   The Appliance Baseline page can also be reached by clicking on **Appliance Status** in the dynamic toolbox, and then clicking the link in the drop-down list.
2. Click **Configure Options**.
3. The Appliance Baseline Options page is displayed.

The options on this page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Recipients</td>
<td>The email address or addresses which will be sent an email. This is entered as a single email address or a comma separated list of addresses.</td>
</tr>
<tr>
<td>Email Subject Template</td>
<td>The template used to create the email subject. By default this is: \texttt{ADDM Baseline: %(appliance_name)s: %(message)s (%(severity)s)} \newline \texttt{Where:} \newline \quad \texttt{• %(appliance_name) – replaced with the name of the appliance.} \newline \quad \texttt{• %(message) – replaced with the passed message or failed message appropriately.} \newline \quad \texttt{• %(severity) – replaced with the severity of the highest severity check that failed, or ok if the checks all passed.}</td>
</tr>
<tr>
<td>Passed Message</td>
<td>The message to include in the email when the test is passed.</td>
</tr>
<tr>
<td>Failed Message</td>
<td>The message to include in the email when the test is failed.</td>
</tr>
<tr>
<td>Services To Allow</td>
<td>Select one or more of the following services to remain open if network access is restricted according to the actions configured: \newline \quad \texttt{• HTTP} \newline \quad \texttt{• HTTPS} \newline \quad \texttt{• SMTP} \newline \quad \texttt{• SSH} \newline \quad \texttt{• DNS} \newline \quad \texttt{• LDAP} \newline For example, where a critical problem is detected, you may choose to limit network access to and from the appliance to HTTP or HTTPS only. To do this, select HTTP and HTTPS, ensure the other services are deselected.</td>
</tr>
</tbody>
</table>
**Note:** If the appliance mail server settings are set to an invalid mail server, configuring baseline to send email introduces a delay of approximately three minutes while the appliance attempts to contact the SMTP server, each time baseline is run. Baseline is run hourly by cron, and may be run manually by a user.

### Configuring actions on changing appliance status

You can configure the actions that will occur when the appliance status changes. To do this:

1. From the Appliance section of the **Administration** tab, select **Baseline Status**.
   The Appliance Baseline page is displayed.
   The Appliance Baseline page can also be reached by clicking **Appliance Status** in the dynamic toolbox, and then clicking the link in the drop-down list.
2. Click **Configure Actions**.
3. The Appliance Baseline Actions page is displayed.
   The options on this page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
   | Actions to take on CRITICAL failure | Select the actions to take when a CRITICAL failure occurs. The following options are available:  
                                            • Send Email  
                                            • Restrict Network Access  
                                            • Stop Discovery |
   | Actions to take on MAJOR failure | Select the actions to take when a MAJOR failure occurs. The following options are available:  
                                            • Send Email  
                                            • Restrict Network Access  
                                            • Stop Discovery |
   | Actions to take on MINOR failure | Select the actions to take when a MINOR failure occurs. The following options are available:  
                                            • Send Email  
                                            • Restrict Network Access  
                                            • Stop Discovery |
   | Actions to take on INFO only | Select the actions to take when an INFO failure occurs. The following options are available:  
                                            • Send Email  
                                            • Restrict Network Access  
                                            • Stop Discovery |
   | Actions to take on SUCCESS | Select the action to take when there are no failures. The following option is available:  
                                            • Send Email |

### Checks performed

The checks that are performed for each item in the Appliance Baseline Page are described in the following table:

<table>
<thead>
<tr>
<th>Name</th>
<th>Check Performed</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks to ensure that the Apache configuration has not been changed since the last baseline.</td>
<td></td>
<td>Major</td>
</tr>
<tr>
<td>Name</td>
<td>Check Performed</td>
<td>Severity</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Apache Configuration</td>
<td>Checks that the HTTPS configuration which allows secure web access (enabled/disabled) on the appliance is the same as that configured in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Apache HTTPS</td>
<td>Checks that the HTTPS configuration which allows secure web access (enabled/disabled) on the appliance is the same as that configured in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Appliance Configuration Files Tripwire</td>
<td>Checks the tripwire logs to ensure that no appliance configuration files have been added, deleted, or edited since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Appliance eth0</td>
<td>Checks that the eth0 configuration on the appliance is the same as that configured in the baseline. The following items are checked: • Speed • Duplex • Autonegotiation</td>
<td>Minor</td>
</tr>
<tr>
<td>Appliance Firewall</td>
<td>Checks that the firewall (iptables) configuration matches that recorded in the baseline.</td>
<td>Critical</td>
</tr>
<tr>
<td>Appliance HTML Files Tripwire</td>
<td>Checks the tripwire logs to ensure that no HTML files have been added, deleted, or edited since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Appliance System Files Tripwire</td>
<td>Checks the tripwire logs to ensure that no system files have been added, deleted, or edited since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Application Configuration</td>
<td>Checks to ensure that the application configuration has not been changed since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Application Server</td>
<td>Checks that the UI service is alive.</td>
<td>Critical</td>
</tr>
<tr>
<td>AppServer Configuration</td>
<td>Checks to ensure that the application server configuration has not been changed since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>AppServer Start Script</td>
<td>Checks to ensure that the application server start script has not been edited since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Atrium Discovery RPM</td>
<td>Checks that the BMC Atrium Discovery RPM version number matches that in the baseline.</td>
<td>Critical</td>
</tr>
<tr>
<td>Atrium Export Credentials</td>
<td>Checks to ensure that the Atrium credentials have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Audit Settings</td>
<td>Checks to ensure that the audit settings have not been changed since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Basket Service</td>
<td>Checks to ensure that the basket service settings have not been changed since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Consolidation</td>
<td>Checks to ensure that the consolidation settings (scanning or consolidation appliance and configured connections including status) have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Crontab</td>
<td>Checks that the cron tab setting on the appliance is the same as that configured in the baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Custom rules and actions</td>
<td>Checks that the custom rules and actions that are used by BMC staff have not been changed since the last check.</td>
<td>Major</td>
</tr>
<tr>
<td>DataStore SoftLimit</td>
<td>Checks that the datastore soft limit matches that in the baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Name</td>
<td>Check Performed</td>
<td>Severity</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Default Scan Level</td>
<td>Checks that the default scan level matches that in the baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Discovery Configuration</td>
<td>Checks that the Discovery configuration matches that in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Discovery Filters</td>
<td>Checks that the sensitive data filters configured on the appliance match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Discovery Mode</td>
<td>Checks that the Discovery mode (Record/Playback/Normal) matches that in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Discovery Scripts</td>
<td>Checks that the Discovery commands match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Discovery Service</td>
<td>Checks that the Discovery service is alive.</td>
<td>Critical</td>
</tr>
<tr>
<td>Discovery Start Script</td>
<td>Checks that the following settings in the Discovery start script match those in the baseline:</td>
<td>Minor</td>
</tr>
<tr>
<td></td>
<td>• Mode - record or playback</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Log level</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pool data expiry time</td>
<td></td>
</tr>
<tr>
<td>DNS Configuration</td>
<td>Checks that the following DNS settings match those in the baseline:</td>
<td>Minor</td>
</tr>
<tr>
<td></td>
<td>• Name servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
<td></td>
</tr>
<tr>
<td>Exclusion Ranges</td>
<td>Checks to ensure that the exclude ranges have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>File Export Credentials</td>
<td>Checks to ensure that the file export credentials have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Integrations Configuration</td>
<td>Checks to ensure that integration points and software credential groups, and their constituent queries and connections/credentials have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>JDBC Export Credentials</td>
<td>Checks to ensure that the JDBC export credentials have not been changed since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Login Credentials</td>
<td>Checks that the Discovery login credentials match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Model Service</td>
<td>Checks that the model service is alive.</td>
<td>Critical</td>
</tr>
<tr>
<td>Model Start Script</td>
<td>Checks to ensure that the model start script has not been edited since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>NTP Configuration</td>
<td>Checks whether the NTP configuration matches that recorded in the baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>NTP Running</td>
<td>Checks whether the NTP status (enabled/disabled) matches that in the baseline. When ntpd is running, the message ntpd is not configured to run at run level 5 is displayed this is incorrect and can be ignored.</td>
<td>Minor</td>
</tr>
<tr>
<td>Operating System</td>
<td>Checks whether the operating system version matches that in the baseline.</td>
<td>Critical</td>
</tr>
<tr>
<td>Options Service</td>
<td>Checks to ensure that the options service settings have not been changed since the last baseline.</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Checks that the pattern configuration matches that in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Name</td>
<td>Check Performed</td>
<td>Severity</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Pattern Configuration Modification</td>
<td>Checks that pattern definitions match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Pattern Definition Modification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pattern Modification</td>
<td>Checks that the patterns match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Port Scan Settings</td>
<td>Checks that the port scan settings match those in the baseline. The check is performed for each port that is enabled for TCP, UDP, or both.</td>
<td>Major</td>
</tr>
<tr>
<td>Reasoning Service</td>
<td>Checks that the Reasoning service is alive.</td>
<td>Critical</td>
</tr>
<tr>
<td>Reasoning Start Script</td>
<td>Checks that the log level for Reasoning matches that in the baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Security Options</td>
<td>Checks that the security service options match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Security Service</td>
<td>Checks that the security service match those in the baseline.</td>
<td>Critical</td>
</tr>
<tr>
<td>Security Start Script</td>
<td>Checks to ensure that the security start script has not been edited since the last baseline.</td>
<td>Minor</td>
</tr>
<tr>
<td>Windows Proxy Availability</td>
<td>Checks that all of the Windows proxies respond when pinged.</td>
<td>Info</td>
</tr>
<tr>
<td>Windows Proxy Configuration</td>
<td>Checks that the Windows proxy configuration on the appliance (not the external Windows proxies) matches that recorded in the baseline. This includes checking the type, version, and position in the Windows proxy order.</td>
<td>Major</td>
</tr>
<tr>
<td>Windows Proxy Configuration File</td>
<td>Checks to ensure that the winproxy.conf file on each connected Windows proxy has not been edited since the last baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>Windows Proxy Pool Configuration</td>
<td>Checks that the Windows proxy pool configuration on the appliance (not the Windows proxies) matches that recorded in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>SNMP Credentials</td>
<td>Checks that the Discovery SNMP credentials match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>SSL Appliance Key</td>
<td>Checks that the appliance SSL key file MD5 checksums that match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>SSL CA Key</td>
<td>Checks that the appliance certificate authority file MD5 checksums that match those in the baseline.</td>
<td>Major</td>
</tr>
<tr>
<td>System Settings</td>
<td>Checks that the system settings match those in the baseline.</td>
<td>Major</td>
</tr>
</tbody>
</table>
Tripwire commissioning and configuration

Tripwire is a third-party software tool that monitors a given set of configuration, system, and source files on an appliance. For further information about Tripwire, see: http://sourceforge.net/projects/tripwire/. Tripwire is installed by the kickstart process but is not commissioned. When Tripwire has been commissioned, it is run hourly. You can also run it manually, see #Running Tripwire Checks Manually for more information.

Tripwire reports

The Tripwire reports are stored in the following directory: /usr/tideway/var/tripwire/report
You must create this directory if it does not exist. As the tideway user, enter the following command:

```
mkdir -p /usr/tideway/var/tripwire/report
```

Commissioning tripwire passkeys

Commissioning Tripwire passkeys is a one-off procedure. You must be able to log in as the root user to complete Tripwire passkeys commissioning.

1. Log in as the root user.
   The default Tripwire policy file is /usr/tideway/etc/twpol.txt.
2. Edit the file and enter the hostname of the appliance (as returned by the hostname command), replacing localhost.
   An excerpt of the file is shown below:

```
@@section GLOBAL
TWROOT="/usr/tideway/tripwire/sbin";
TWBIN="/usr/tideway/tripwire/sbin";
TWPOL="/usr/tideway/tripwire/etc";
TWDB="/usr/tideway/tripwire/var/lib";
TWSKEY="/usr/tideway/tripwire/etc";
TMLKEY="/usr/tideway/tripwire/etc";
TWREPORT="/usr/tideway/var/tripwire/report";
ARCH="x86_64";
HOSTNAME="localhost";
```
If you want to monitor any additional files, add the full path to that file to the policy file.

If you want to monitor any additional directories, add the full path to that directory to the policy file.

Copy the /usr/tideway/etc/twpol.txt file to /usr/tideway/tripwire/etc/twpol.txt, overwriting the existing file.

Run the following command which will set up the initial database and passwords allowing changes to the Tripwire configuration:

```
/usr/tideway/tripwire/sbin/tripwire-setup-keyfiles
```

You are prompted to create a site and a local password. Record these passwords or you will need to reinstall the Tripwire database.

The local password is required to remove Tripwire violations.
The site password is required to update the Tripwire policy file.

You are prompted to sign the configuration file twcfg.txt and the policy file twpol.txt.

Change the ownership and permissions of the /usr/tideway/tripwire/etc/twpol.txt and the /usr/tideway/tripwire/etc/twcfg.txt files to the tideway user. Enter the following commands:

```
cd /usr/tideway/tripwire/
chown tideway:tideway etc
chmod 750 etc
cd etc
chown tideway:tideway twcfg.txt twpol.txt
chmod 640 twcfg.txt twpol.txt
```

**Initializing the tripwire database**

Initializing the Tripwire database is a one-off procedure. This procedure should be performed as the tideway user.

1. The Tripwire database must be initialised with the contents of the Tripwire policy file.
2. Run the following command to initialize the Tripwire database:

```
sudo /usr/tideway/tripwire/sbin/tripwire --init
```

3. Run the following command to rebaseline the Tripwire database:

```
/usr/tideway/bin/tw_tripwire_rebaseline
```

An error is reported as a database backup file is created.

4. Run the following command again to rebaseline the Tripwire database:
This time, no errors are reported as no files have been added. The tripwire database is now initialised and baselined.

**Initial appliance baseline configuration**

When you have freshly configured the tripwire database, the appliance baseline must be updated to ensure that the correct status is shown in the user interface.

**Warning**

This will cause all of the appliance baseline checks to be reset. Make sure that all existing baseline failures are addressed.

1. Run `/usr/tideway/bin/tw_baseline` or click Check Baseline Now in the user interface to execute all the baseline tests.
2. Verify that only tripwire related tests are failing. Trip wire test names end with "tripwire".
3. Update the tripwire report and then update the appliance baseline as follows:

   ```bash
   sudo /usr/tideway/tripwire/sbin/tripwire --check > /usr/tideway/var/tw_tripwire.txt
   /usr/tideway/bin/tw_baseline --rebaseline
   ```

The appliance status is updated, and tripwire commissioning is now complete.

**Tripwire maintenance**

**Updating after a violation**

When you use the `tw_tripwire_rebaseline` utility to rebaseline the Tripwire database, you accept that all files that are being monitored are correct. This procedure should be performed as the `tideway` user. To update the Tripwire database after an error:

1. Check the items that are reported in the violation report and ensure that the reported changes are what you expected.
2. Run the following command:

   ```bash
   /usr/tideway/bin/tw_tripwire_rebaseline
   ```
Updating the tripwire policy file

Sometimes you will need to update the Tripwire policy file. This may be due to:

- An EFix being applied
- A full system upgrade
- Appliance relocation or change of IP Address
- Files changing too frequently and creating false positive alerts

Edit /usr/tideway/tripwire/etc/twpol.txt and make the necessary changes. Save the file using the same name.

Clear all violations before updating the Tripwire policy file by rebaselining the Tripwire database. The system must be in a known good state to update the policy database. This procedure should be performed as the tideway user.

1. Run the following command to rebaseline the Tripwire database:

```
/usr/tideway/bin/tw_tripwire_rebaseline
```

2. Run the following command (on one line) to update the Tripwire policy file:

```
cd /usr/tideway/tripwire/etc/
sudo /usr/tideway/tripwire/sbin/tripwire --update-policy twpol.txt
```

You will need both the local and site password for this operation.

3. Check that the update has been performed correctly. Enter:

```
sudo /usr/tideway/tripwire/sbin/tripwire --check
```

4. Run the following command to rebaseline the Tripwire database:

```
/usr/tideway/bin/tw_tripwire_rebaseline
```

For more information about the `tw_tripwire_rebaseline` utility, see `tw_tripwire_rebaseline`.
Running tripwire checks manually

By default, Tripwire is run hourly and the output is written to the tw_tripwire.txt file. If a deviation from the baseline has been detected, the tw_tripwire.txt file is updated with the details. The monitor which sets the appliance status in the user interface checks the tw_tripwire.txt file hourly and sets certain restrictions if configured.
If you have rebaselined the Tripwire database, you should run the following commands to ensure that the correct status is shown in the user interface.

```
sudo /usr/tideway/tripwire/sbin/tripwire --check > /usr/tideway/var/tw_tripwire.txt
/usr/tideway/bin/tw_baseline --rebaseline
```

The appliance status is updated.

For more information about the `tw_baseline` utility, see `tw_baseline`.

Configuring dependency visualizations

The Dependency Visualization links displayed in the Visualization list in the user interface (UI) are generated from a visualization configuration file. For more information, see the Viewing dependency visualizations section. You can now add new visualizations to this configuration file, edit existing ones or remove them from the visualization list.

Notes:

1. Configuration File Location - The default configuration file can be found in the following location:
   `/usr/tideway/data/default/graph-definition.txt`
   This default configuration file must not be changed.
2. Configuration File Customisation - To customize a configuration file, create the following:
   `/usr/tideway/data/customer/graph-definition.txt`
   This overlays the default configuration file.

Structure of the file

The file is divided into three sections by rows of equals signs. The first section defines visualization definitions, the second dependency definitions, and the third tooltip definitions. For an explanation of each of these, see the following sections:

Visualization definitions

The visualization definition section contains a number of definitions for visualizations. Each definition takes the form:
visualization_name {tab=tab_name}
  viewed_node_type
    type_of_dependency dependency_target_node_type
    type_of_dependency dependency_target_node_type
    ...
    type_of_dependency dependency_target_node_type

- **visualization_name** – the name of the visualization. This is displayed in the visualizations list when viewing a node of the type defined in `viewed_node_type`.
- **tab_name** – the tab under which to display the visualization. Valid values are:
  - Home
  - Application
  - Infrastructure
  - Discovery
  - Reports
  - Setup
  - If no tab is specified, no tab is selected when the visualization is displayed.
- **viewed_node_type** – the type of node for which this visualization is available.
- **type_of_dependency** - the type of dependency, for example, depended_upon, or dependant.
- **dependency_target_node_type** - the node type that is the target for the dependency.
  For example, in a dependency visualization describing the relationship between a business application running on a host and the host itself, the target is `Host`.

For example:

```
Dependency (tab=Infrastructure)
  SoftwareInstance
    depended_upon SoftwareInstance
    dependant SoftwareInstance
    running_on Host

BusinessApplicationInstance
    depended_upon BusinessApplicationInstance
    dependant BusinessApplicationInstance
    running_on Host
```

This defines a visualization called `Dependency` which will be available on the visualizations list when viewing a `SoftwareInstance` or a `BusinessApplicationInstance`. When displayed, the Infrastructure tab will be selected.
When you pick the SoftwareInstance visualisation, you see the SoftwareInstance node as the starting point of the visualisation, and then all SoftwareInstance and Host nodes related to that SoftwareInstance. Exactly which SoftwareInstance and Host nodes are shown depends on the definition of the depended_upon, dependant, and running_on dependency definitions, which are defined in the dependency definitions part of this file.

The indentation is important and defines the structure of the visualization. An indentation must be composed of spaces, not tabs, and be a multiple of two spaces.

### Dependency definitions

The dependency definition (type_of_dependency) defines the route from the viewed_node_type to the dependency_target_node_type.

For example, the following visualization definition, from the first section of the file, shows all Hosts that a SoftwareInstance is running on:

```plaintext
Dependency
    SoftwareInstance
        running_on Host
```

The **running_on** Host relationship defines the route from the SoftwareInstance to the Host. One of these definitions must exist in the dependency definitions. For example:

```plaintext
SoftwareInstance
    running_on Host
        RunningSoftware:HostedSoftware:Host:Host
```

Here, SoftwareInstance is defined as the source node kind and Host is defined as the destination node kind, and the system will use the traversal RunningSoftware:HostedSoftware:Host:Host to get from any SoftwareInstance nodes currently in the visualization to any related Host nodes.

A dependency definition can have multiple traversals chained one after the other in order to get to a node kind that is distantly related:

```plaintext
Host
    connected_to Subnet
        DeviceWithInterface:DeviceInterface:InterfaceOfDevice:NetworkInterface DeviceOnSubnet:
```

The visualization will show only Host and Subnet nodes, but in order to get to Subnet nodes from Host nodes, it will traverse through NetworkInterface nodes.
You can also define a number of alternative paths by listing them on separate lines:

```
SoftwareInstance
communication SoftwareInstance
  Server:Communication:Client:SoftwareInstance
  Client:Communication:Server:SoftwareInstance
```

Each path will be tried in turn, and all resulting nodes connected to the source node will be returned.

Relationships can be wildcarded in the same way as in a generic search using `::`

```
SoftwareInstance
composed_of DiscoveredProcess
  InferredElement:Inference::DiscoveredProcess
```

Traversal steps can have an optional `+' after them, for example:

```
SoftwareContainer:SoftwareContainment:ContainedSoftware:SoftwareInstance+
```

This causes the step to be followed repeatedly, adding nodes to the set of nodes found so far, until further traversals add no further nodes. The step is always evaluated at least once. A good use of this function is to follow a relationship that forms an arbitrarily deep hierarchy: for example, the SoftwareInstances making up a BAI. Here it is possible to have a first-order SoftwareInstance with a second-order SoftwareInstance as the container, before reaching the BAI. Although not recommended and not often seen, a third-order SoftwareInstance can be inserted between the second order SoftwareInstance and the BAI, and so on. This function will navigate this structure.

**Attributes**

Attributes can be set on a dependency definition that affect how it is rendered. For example:

```
SoftwareInstance
communication.server SoftwareInstance (color=0f0,left_arrow)
  Server:Communication:Client:SoftwareInstance
communication.client SoftwareInstance (color=0f0,right_arrow)
  Client:Communication:Server:SoftwareInstance
```

This displays lines between SoftwareInstance nodes representing client/server communications in green, and draws an arrow pointing at the server.
Attributes appear in brackets after the definition of the dependency type and destination node kind. No spaces are allowed between the brackets, and the attributes are a comma separated list of either flags, or key and value.

Defined attributes are:

- **color**: sets the color of the line in the graph. It takes a three character argument that is the color as an RGB tuple. Each character is the color of that component as a hexadecimal digit (0-f).
- **left_arrow**: sets arrow heads on the line, pointing to the source node.
- **right_arrow**: sets arrow heads on the line, pointing to the target node.
  Both attributes can be set, in which case both ends of the line have an arrow, and neither attribute can be set, in which case the line is plain.
- **left_box**
  - traverse to the destination nodes using the given traversal
  - represent the source node as a box
  - add the destination nodes in the box
- **right_box**
  - traverse to the destination node using the given traversal
  - represent the destination node as a box
  - add the source node in that box

Note that there must only be a single destination node when using right_box, because it is impossible to turn several destination nodes into separate boxes and put the source node inside each of them. It should be used when it is known there will always be at most one destination node, for example, the HostContainer for a Host.

Boxes only appear at the top level; they cannot be nested. If a later definition conflicts with an earlier, for example, attempting to nest boxes or put a node inside two different boxes, the later definition overrides the earlier. The order depends on how the graph is constructed and is not predictable.

The left_box and right_box attributes override the color, left_arrow, and right_arrow attributes.
Special traversals

The :NetworkConnections:: traversal which can be used with Hosts and DiscoveredProcesses, connects nodes based on observed communication information. Observed communication information is directly discovered, rather than specific communication relationships built by patterns.

DiscoveredNetworkConnections and ListeningPorts are used to find this information. These types of traversal are quite slow.

Notes for defining traversals

It is recommended that arrows on edges point towards the depended upon node. For example, the Switch on an edge between Host and Switch, or the SoftwareInstance on an edge between BAI and SoftwareInstance. This will ensure the layout algorithm lays the graph out properly when in hierarchical layout mode.

It makes sense to name traversals as a verb phrase that can be read in the middle of the start and end node kinds (where end is defined as the node with the arrow head and start is the other one). For example, SoftwareInstance running_on Host. This makes it easy to read off what any given edge in the visualization means.

It is also recommended that when defining a pair of traversals for moving between nodes in either direction (eg. from Host to SoftwareInstance and from SoftwareInstance to Host, both using the "RunningSoftware" relationship), that the traversal is named the same thing. In other words, instead of defining the two traversals like this:

```
Host
   has_running_on_it SoftwareInstance (right_arrow)
   Host:HostedSoftware:RunningSoftware:SoftwareInstance
SoftwareInstance
   is_running_on Host (right_arrow)
   RunningSoftware:HostedSoftware:Host:Host
```

...define it like this:

```
Host
   running_on SoftwareInstance (left_arrow)
   Host:HostedSoftware:RunningSoftware:SoftwareInstance
SoftwareInstance
   running_on Host (right_arrow)
   RunningSoftware:HostedSoftware:Host:Host
```
The latter form ensures that the edges all point towards the depended upon node (the Host), and also keeps the name the same. If the name, attributes (color and dashed), and source and destination nodes are the same, but the arrow and source and destination nodes are opposites, the two edges will be merged. Without this, the visualization can become ugly as lots of edges will be double edges.

There is one case where a pair of opposite traversals cannot have the same name: when the source and destination nodes are the same node kind. For example:

```
SoftwareInstance
depended_upon SoftwareInstance (color=00f,right_arrow)
Dependant:Dependency:DependedUpon:SoftwareInstance
dependant SoftwareInstance (color=00f,right_arrow)
DependedUpon:Dependency:Dependant:SoftwareInstance
```

Ideally the traversals should be called the same thing, as they are opposites of each other. But because the source and destination nodes are the same, there is no way to distinguish them other than to use a different traversal name. In this case, the visualization might end up with two edges between a pair of SoftwareInstances, one pointing one way and labelled "depended_upon" and the other pointing the other way and labelled "dependant".

It is a convention to use the name "xxxxx.box" for "box" traversals, ie. those that put the source or destination nodes in a box by using left_box or right_box. This is because often the non-box case is also required in some visualizations. With this naming scheme, it is clear which form is being used.

### Tooltip definitions

By default, the attributes shown as a tooltip when a user hovers over a node are read from the summary list defined in the taxonomy. The tooltip section allows that to be overridden. For example:

```
Host
name
os_class
```

### Configuring model maintenance settings

You can modify settings for maintaining your data model, including aging limits, in the Model Maintenance settings of the user interface.

To configure model maintenance settings:

1. From the Model section of the **Administration** tab, select **Model Maintenance**.
This screen illustrates the configuration settings you can modify for maintaining the model.

The options on the page are described in the following table.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
| DDD removal                       | Specify the age past which Discovery Accesses and all the related DDD nodes are removed (the default is 28 days). 
• Quarterly (90 days) 
• Monthly (28 days) 
• Fortnightly 
• Weekly 
If the setting does not match one of these options the value will be shown as "--custom settings--". 
In a demonstration appliance only, the default setting for aging is Never, meaning that demonstration data never ages out of the system. This setting is not available for any other type of appliance, and demonstration appliances should never be used for anything other than demonstrations. 
For guidelines, see Modifying DDD, host, and software instance aging limits. |
| Scan optimization timeout         | When an IP address is designated the preferred IP address for a host, Discovery does not perform scans on other known IP addresses for that host. This is referred to as scan optimization. After a specified Scan optimization timeout period, Discovery will scan other known IP addresses for that host to ensure that they are still non-preferred and on the same host. Specify one of the following timeout periods from the drop-down list. 
• 1 - 10 days 
• 14 days 
• 21 days |
| Host/Network Device/Mainframe aging time limit | Specify the host/network device/mainframe aging time limit (the default is 10 days). 
• 2 - 10 days 
• 14 days 
• 21 days 
• 28 days 
For guidelines, see Modifying DDD, host, and software instance aging limits |
| Host/Network Device/Mainframe aging access failures | Specify the number of host/network device/mainframe aging access failures. 
• 1 - 10 failures |
| Time to elapse before a software instance/runtime environment can be aged | Specify the time to elapse before a software instance/runtime environment can be aged. (the default is 10 days). 
• 1 - 20 days 
• Steps of 5 to 100 days 
For guidelines, see Modifying DDD, host, and software instance/runtime environment aging limits |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of failed accesses before a</td>
<td>Failed accesses before a software instance/runtime environment is aged.</td>
</tr>
<tr>
<td>software instance/runtime environment is aged</td>
<td>• 1 - 20 failures</td>
</tr>
<tr>
<td></td>
<td>• Steps of 5 to 45 failures</td>
</tr>
<tr>
<td>Dark space suppression scheme</td>
<td>The scheme to use for dark space suppression. Select either Keep Most Recent or Remove All from the list. See #Dark space DiscoveryAccess nodes for a description of this setting.</td>
</tr>
<tr>
<td>Cache Size</td>
<td>The size of the disk cache. The default is 1GB. Do not change the value of this setting unless you are advised to by Customer Support.</td>
</tr>
<tr>
<td>Size Warning</td>
<td>The maximum size of the datastore. When this limit is reached, a warning is displayed in the Appliance Status page. This is a soft limit and does not prevent the datastore growing beyond the specified limit. You can select any value from 10 to 100 GB in steps of 5 GB from the list. The default is 30 GB.</td>
</tr>
<tr>
<td>Checkpoint Interval</td>
<td>The interval between datastore checkpoints. The larger the interval, the more data has to be written to the checkpoint files. The smaller the interval, less data needs to be written to the checkpoint files, though the writing takes place more often. The default is 15 minutes. You must contact Customer Support before you make any changes to this setting.</td>
</tr>
</tbody>
</table>

Modifying DDD, host, and software instance aging limits

In general, the expectation that BMC Atrium Discovery uses for deriving the default model maintenance settings is based on performing one scan of the estate every 24 hours with a DDD depth of one month. This expectation is also used to derive the sizing data. The default setting for data aging for both hosts and software instances is 10 days, because for most deployments this limit provides the best balance of responsiveness without data thrashing. Putting this in a business example, this gives two weekends plus additional time to detect that a host is aging, investigate why it is doing so, and make changes before the host is destroyed. It gives the software teams the same length of time to sort out any failures in the estate.

👍 Best Practice
BMC recommends that you do not attempt to fine-tune model maintenance parameters. Doing so can make BMC Atrium Discovery highly reactive and have negative consequences, such as causing a dramatic increase in the size of the datastore and putting more load on your target estate. If you do alter the model maintenance parameters, BMC recommends that you do not vary more than half or twice the standard settings detailed in the preceding table.

However, there might be occasions when modifying the defaults are necessary, particularly if you scan your estate at different intervals and need to keep close control on disk consumption. The following table show recommended settings based on your scanning frequency.

<table>
<thead>
<tr>
<th>Scanning Frequency</th>
<th>Recommended Aging Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every 2 days</td>
<td>Maintain DDD at 28 days, and decrease the Host and Software Instance access failures to 4 (to account for half as many expected scans).</td>
</tr>
<tr>
<td>2 times per day</td>
<td>Decrease DDD to 14 days (to cap how much space it consumes, unless you increase the disk space to more than the sizing guidelines); increase the Host and Software Instance access failures to 12-14 (to account for scanning at twice the expected rate).</td>
</tr>
</tbody>
</table>

For more information about aging and how it fits in the node removal process, see How nodes are removed.

**Scheduled DDD aging – new in 8.3 SP2**

In BMC Atrium Discovery systems where discovery (or consolidation) is in progress for most of the available time, contention between the removal (aging out) of DDD nodes (in this case DiscoveryAccess nodes and their children) and the creation of new nodes, may affect the performance of in-progress discovery runs. From BMC Atrium Discovery 8.3 SP2 you can avoid this performance impact by scheduling DDD removal blackout windows during which no DDD removal is undertaken.

**When should DDD removal blackout windows be used?**

DDD removal blackout windows should typically only be used on consolidation appliances when you need to achieve maximum discovery throughput. This is only likely to be needed at the Consolidated Enterprise scale, or possibly in the very largest scanning appliances. In virtually every discovery schedule used, the continual aging scheme used by BMC Atrium Discovery can remove "old" DDD at a similar rate as they are created.

You can determine whether scheduling DDD removal blackout windows may be beneficial using the DDD removal statistics page. The DDD removal statistics page shows the total number of DiscoveryAccesses in the datastore and those eligible for removal. If DiscoveryAccess removal is
keeping up with DiscoveryAccess creation, then the number of eligible DiscoveryAccess nodes is zero, or near zero, DDD removal blackout windows are not required. If the trend of eligible DiscoveryAccess is rising over a two week period, then DDD removal blackout windows may be a solution. See DDD removal statistics page for more information.

Viewing existing DDD aging blackout windows

To view existing DDD aging blackout windows:

1. From the Model section of the Administration tab, select Model Maintenance.
2. Select the DDD Removal Blackout Windows tab.

This screen shows existing DDD removal blackout windows and provides links to edit or delete existing windows and a button to add a new one.

When you view the DDD Removal Blackout Windows tab, the active blackout window is highlighted. If multiple blackout windows are active, the one with the longest time remaining before it ends is highlighted. This is not automatically refreshed.

DDD nodes are removed in batches which are not interrupted. Once removal starts, it continues to completion. Therefore, if a batch removal is in progress at the beginning of a DDD removal blackout window, it will continue into the blackout until completion. In normal operation this should take no more than a few minutes.

Adding a new DDD aging blackout window

You can schedule a new DDD aging blackout window to occur daily, weekly, or monthly and can specify a start time and duration. To schedule a new DDD aging blackout window:

1. Click the Add button.
   The Add a New DDD Removal Blackout Window dialog box is displayed.
2. Enter the information for the blackout window in the fields described below.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comment</td>
<td>Enter a descriptive comment for the blackout window.</td>
</tr>
<tr>
<td>Frequency</td>
<td>Select a frequency for the window to operate. For example, this can be Daily, Weekly, or Monthly. For a weekly blackout window, you are provided with buttons for each day. Select the day or days that you want the window to operate. For a monthly blackout window, you are provided with buttons for each day in the month. Select the day or days that you want the window to operate. Alternatively, select the No Removal On The radio button and choose one of: • First • Second • Third • Fourth</td>
</tr>
</tbody>
</table>
2. Select the following fields in the table:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Last and the day that you want the window to operate. In this way you can select the Second Tuesday of the month and so forth.</td>
<td></td>
</tr>
<tr>
<td>Start Time</td>
<td>Select a time for the window to start.</td>
</tr>
<tr>
<td>Duration</td>
<td>Select a duration in hours. This is the length of time that the blackout window operates and can be from 1 to 24 hours. For a daily blackout window the maximum number of hours you can select is 23. This prevents you from inadvertently scheduling a 24/7 blackout.</td>
</tr>
</tbody>
</table>

3. Click OK.

**Dark space DiscoveryAccess nodes**

DiscoveryAccess nodes are created in the datastore for any discovery access attempt, whether or not the attempt was successful. A DiscoveryAccess node is created when an endpoint is scanned, if there is no response, the state is set to **NoResponse**. On some estates where IP address space is sparsely populated, a very large number of DiscoveryAccess nodes are created, these predominantly being in the **NoResponse** state. On a large estate, the number of these nodes may be large enough to affect the performance of the appliance.

A dark space suppression scheme is provided. You can choose to either keep the most recent, or to remove all DiscoveryAccess nodes in the **NoResponse** state.

To identify a DiscoveryRun which has been performed with the remove all option set and to indicate to the user why the state counts shown could look misleading, a `remove_first_no_response` attribute is set on the DiscoveryRun and displayed as Dark Space Suppression.

**Configuring audit, snapshot and application options**

Certain advanced audit, snapshot and application options can be configured using the Miscellaneous Settings page.

**To set audit, snapshot and application options**

1. From the Appliance section of the **Administration** tab, select **Miscellaneous**.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Audit logs to be fully purged</td>
<td>Users can purge the audit log of all events up to one month before the current date. This ensures that there is a minimum retention period of one month. You can configure the appliance to permit purging up to the current date. You can enable or disable full purging with this option. The default is No.</td>
</tr>
<tr>
<td>Snapshot Disk Threshold</td>
<td>The amount of disk space to reserve for the appliance snapshot. When the available disk space falls below this value, this is flagged on the Appliance Snapshot page. Select the one of the following values to use as the disk threshold:</td>
</tr>
<tr>
<td>Field Name</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>• 10%</td>
</tr>
<tr>
<td></td>
<td>• 25%</td>
</tr>
<tr>
<td></td>
<td>• 33% (default)</td>
</tr>
<tr>
<td></td>
<td>• 50%</td>
</tr>
<tr>
<td></td>
<td>• 66%</td>
</tr>
<tr>
<td></td>
<td>• 75%</td>
</tr>
<tr>
<td>Snapshot Migration Timeout</td>
<td>You can set a maximum time for a snapshot migration to take. This is the migration timeout. If a snapshot migration takes in excess of migration timeout, it is considered to have failed and the migration aborts. Select the migration timeout from the following values in the list:</td>
</tr>
<tr>
<td></td>
<td>• 5 minutes</td>
</tr>
<tr>
<td></td>
<td>• 10 minutes (default)</td>
</tr>
<tr>
<td></td>
<td>• 15 minutes</td>
</tr>
<tr>
<td></td>
<td>• 30 minutes</td>
</tr>
<tr>
<td></td>
<td>• 45 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1 hour</td>
</tr>
<tr>
<td>History Compression Threshold</td>
<td>The historical comparison pages ‘compress’ the raw history into changes. Entries are grouped by user and a sliding time threshold. This time threshold is necessary to enable you to view a number of separate changes made by Reasoning as a single change. Select from the following values in the list:</td>
</tr>
<tr>
<td></td>
<td>• 15 seconds</td>
</tr>
<tr>
<td></td>
<td>• 30 seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 minute (default)</td>
</tr>
<tr>
<td></td>
<td>• 5 minutes</td>
</tr>
<tr>
<td></td>
<td>• 10 minutes</td>
</tr>
<tr>
<td></td>
<td>• 30 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1 hour</td>
</tr>
<tr>
<td></td>
<td>• 8 hours</td>
</tr>
<tr>
<td></td>
<td>• 24 hours</td>
</tr>
<tr>
<td></td>
<td>The History Compression Threshold can be thought of as a sample rate. Select a value providing sufficient granularity to capture the change that you are looking for. For example, if a node is changing state every 20 minutes, a sample rate below this would be required to capture the changes, in this case, choose 10 minutes.</td>
</tr>
<tr>
<td>Max number of visualizations to cache</td>
<td>The maximum number of visualizations to cache. Select from the following values in the list:</td>
</tr>
<tr>
<td></td>
<td>• 0 (default)</td>
</tr>
<tr>
<td></td>
<td>• 10</td>
</tr>
<tr>
<td></td>
<td>• 100</td>
</tr>
<tr>
<td></td>
<td>Changing this setting requires a restart of the tideway service to take effect. Restarting the tideway service clears the visualizations from the cache.</td>
</tr>
<tr>
<td>Time to cache visualizations for</td>
<td>The time to cache visualizations for. This is the length of time from creation of the visualization rather than the last view. Select from the following values in the drop-down list:</td>
</tr>
<tr>
<td></td>
<td>• 1 hour</td>
</tr>
<tr>
<td></td>
<td>• 1 day</td>
</tr>
<tr>
<td></td>
<td>• Forever (default)</td>
</tr>
</tbody>
</table>

**Visualization cache**

Complex visualizations which need to traverse over many relationships to build the data, such as the Application Dependencies - Software View, can be slow to load. Caching of generated visualizations has been introduced to ensure that this can be minimized.
You should note that cached data is not live, so using this feature will result in visualizations which may not be consistent with the current state of the datastore. This is particularly important when using the forever setting.

Changing either visualization cache settings requires a restart of the tideway service to take effect. Restarting the tideway service clears the visualizations from the cache.

**Configuring the NTP client**

The NTP client enables the appliance or virtual machine to synchronize its internal clock with an NTP server on your network or on the internet.

⚠️ **NTP and VMware Tools**

If you are using NTP on a BMC Atrium Discovery Virtual Appliance, you should disable the VMware tools time syncing. This is explained in VMware's timekeeping best practices for Linux based Virtual Machines which can be found [here](#) under the heading *VMware Tools time synchronization configuration*.

To configure the NTP client you must be logged in to the command line as the root user.

1. Edit the `/etc/ntp.conf` file.
2. Search for the lines beginning `server`.

   ```
   server 0.rhel.pool.ntp.org
   server 1.rhel.pool.ntp.org
   server 2.rhel.pool.ntp.org
   ```

3. Replace the server entries with the IP address or hostname of the NTP server or servers with which you want to synchronize. For example:

   ```
   server ntp.tideway.com
   server 172.17.1.24
   ```

4. Save the file.
5. Configure the NTP client service to start at run level 3 when the appliance boots. Enter:

   ```
   [root@localhost ] # /sbin/chkconfig --levels 3 ntpd on
   [root@localhost ] #
   ```
6. Check to ensure that this change has been made correctly. Enter the following command and ensure that the output is the same as that shown:

```
[root@localhost] # /sbin/chkconfig --list ntpd
ntpd            0:off   1:off   2:off   3:on    4:off   5:off   6:off
[root@localhost] #
```

7. Start the service. Enter:

```
[root@localhost] # /sbin/service ntpd start
Starting ntpd:                                             [ OK ]
[root@localhost] #
```

The NTP client is now running and needs no further attention.

**Rebaseline the appliance after configuring the NTP client**

If you use appliance baseline, you must rebaseline the appliance after making this change. To rebaseline the appliance, as the `tideway` user, enter the following command:

```
/usr/tideway/bin/tw_tripwire_rebaseline
```

For more information about tripwire and baselining the appliance, see [Baseline configuration](#).

⚠️ **Message - ntpd is not configured to run at run level 5**

The message `ntpd is not configured to run at run level 5` which is displayed in the appliance baseline window is erroneous. It is displayed when `ntpd` is running.

**Using command line utilities**

BMC Atrium Discovery provides utilities that you can run on a command line interface to configure Discovery by obtaining information from specific systems. All the utilities are located in the `/usr/tideway/bin` directory and are named `tw_utilityname`. Documentation for each utility in this section includes a link to the corresponding location in the user interface where you can perform the intended function.
**Supported utilities**

All command line utilities that are supported in BMC Atrium Discovery are documented in this section. Any utility that is not documented in this section is an explicitly unsupported tool.

- `tw_adduser`
- `tw_baseline`
- `tw_config_dashboards`
- `tw_convert_reports`
- `tw_cron_update`
- `tw_deluser`
- `tw_disco_control`
- `tw_disco_export_platforms`
- `tw_disco_import_platforms`
- `tw_ds_compact`
- `tw_excluderanges`
- `tw_imp_ciscoworks`
- `tw_imp_csv`
- `tw_injectip`
- `tw_listusers`
- `tw_model_init`
- `tw_passwd`
- `tw_pattern_management`
- `tw_query`
- `tw_reasoningstatus`
- `tw_remove_darkspace`
- `tw_scan_control`
- `tw_scheduled_snapshot`
- `tw_sign_winproxy_config`
- `tw_tax_export`
- `tw_tax_import`
- `tw_terminate_winproxy`
- `tw_tripwire_rebaseline`
- `tw_upduser`
Duplicate or enhanced functionality in user interface

Many of the utilities perform functions that are already part the BMC Atrium Discovery user interface, and might duplicate what you might be able to accomplish more easily in the best-practice use of the product. Most of the configuration you perform will be done using the Discovery Configuration page accessed from the Administration tab; however, the functionality might be located in other areas of the product.

⚠️ Note

Although command line utilities offer a potentially faster or more convenient way to perform a specific function, they may also cause unintended consequences that might compromise your environment if not used carefully.

Common options in the utilities

In each utility, you can specify options, or arguments, that enable you to specify what action you want the utility to perform. For many of the utilities, several options are inherited and their basic purpose does not change. In this section, common options are not described for each utility because they are not typically used.

The following table lists the common options that are inherited by many of the command line utilities available with BMC Atrium Discovery.

<table>
<thead>
<tr>
<th>Common Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Displays the required use of the utility and describes the available options</td>
</tr>
<tr>
<td>--logbackupcount NUM</td>
<td>Specifies the number of backup logs files that are preserved</td>
</tr>
<tr>
<td>--logfile=FILE</td>
<td>Specifies the log file that log messages are written to</td>
</tr>
<tr>
<td>--loglevel=LEVEL</td>
<td>Specifies the logging level as one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• debug: logs all messages</td>
</tr>
<tr>
<td></td>
<td>• info: logs critical, error, warning, and information messages</td>
</tr>
<tr>
<td></td>
<td>• warn: logs critical, error, and warning messages</td>
</tr>
<tr>
<td></td>
<td>• error: logs critical and error messages</td>
</tr>
<tr>
<td></td>
<td>• crit: logs only critical messages</td>
</tr>
<tr>
<td>--passwordfile=FILE</td>
<td></td>
</tr>
</tbody>
</table>
### Common Command Line Option

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a file from which the password is to be read. This is only relevant for utilities that have the --username option. Note that this file is not encrypted, though you can set the file permissions to owner-only (chmod 600 passwordfile.txt) to restrict access to the file. For more information about password policies, see Managing Security Policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-p, --password=PASSWD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the password of the BMC Atrium Discovery user. If no password is specified, you are prompted for one. This is only relevant for utilities that have the --username option. For more information about password policies, see Managing Security Policies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-u, --username</th>
</tr>
</thead>
<tbody>
<tr>
<td>The username to run the utility as. This has to be a valid BMC Atrium Discovery UI user such as the system user, not a username used to access the command line via ssh.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-v, --version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the BMC Atrium Discovery version number, copyright information, and the name of the utility</td>
</tr>
</tbody>
</table>

---

**Warning**

You should not use any service utilities (those named `tw_svc_name`), because the improper use of a service-based command could have potentially adverse results on your system.

---

**tw_adduser**

The `tw_adduser` utility enables you to add a new user to the system, and assign a user to a new group.

---

**Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_adduser` command line utility (see Enabling other users). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_adduser [options] username
```

where:

- `username` is the name of the new user.

If you do not specify a user name, BMC Atrium Discovery will use the default, `system`. 
• *options* are any of the options described in the following table and the common command line options described in *Using command line utilities*.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f, --fullname=ARG</td>
<td><em>(Optional)</em> Specifies the full name of the user</td>
</tr>
<tr>
<td>-g, --groups=ARG</td>
<td><em>(Optional)</em> Specifies additional groups to add a user to (the default value is <em>public</em>). The value <em>public</em> is also the default when you select the Groups option from the Add User page on the Administration tab.</td>
</tr>
</tbody>
</table>

**User example**

In the following example, you can add a new adminstrative user to a multiple groups by using the utility, the *-g* option, and a comma-separated list.

**Adding a new user to multiple groups**

```bash
$TIDEWAY/bin/tw_adduser -g discovery,admin newuser
```

**tw_baseline**

The *tw_baseline* utility enables you to audit your appliance for existing state, inventory, and relationships between configuration items.

**Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the *tw_baseline* command line utility (see *Baseline configuration*). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

Options in the utility specify how the baseline properties can be performed or displayed, or determine what action to take. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```bash
tw_baseline [options]
```
where *options* are any of the options described in the following table and the common command line options described in *Using command line utilities*.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--conditional</td>
<td>Specifies to check for missing data and baselines only that data</td>
</tr>
<tr>
<td>--config=FILE</td>
<td>Specifies to baseline a configuration file, where <em>FILE</em> is the name of the file</td>
</tr>
<tr>
<td>--csvfile=FILE</td>
<td>Specifies to baseline a CSV output file, where <em>FILE</em> is the name of the file</td>
</tr>
<tr>
<td>--interactive</td>
<td>Specifies to run a baseline check in interactive mode, whereby you are prompted to respond Yes (Y) or No (N) to run specific checks until there are no further checks available. For checks that you request to run, results are displayed after you have responded to all checks. Checks that you have declined to run are skipped, and no further actions are run.</td>
</tr>
<tr>
<td>--no-actions</td>
<td>Specifies to run all baseline checks and perform no subsequent action after the checks are complete</td>
</tr>
<tr>
<td>--no-checks</td>
<td>Specifies to run the baseline and performs no subsequent checks</td>
</tr>
<tr>
<td>--no-display</td>
<td>Specifies to run the baseline with no terminal highlighting</td>
</tr>
<tr>
<td>--rebaseline</td>
<td>Specifies to rebaseline the check data</td>
</tr>
<tr>
<td>--statusfile=FILE</td>
<td>Specifies to rebaseline a status output file, where <em>FILE</em> is the name of the file</td>
</tr>
<tr>
<td>--verbose</td>
<td>Specifies to run the baseline and display information messages for checked data</td>
</tr>
</tbody>
</table>

User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

**Running a manual tripwire check**

By default, Tripwire is run hourly and the output is written to the `tw_tripwire.txt` file. If a deviation from the baseline has been detected, the `tw_tripwire.txt` file is updated with the details. The monitor which sets the appliance status in the user interface checks the `tw_tripwire.txt` file hourly and sets certain restrictions if configured.

If you have rebaselined the Tripwire database, you should run the following commands (as the tideway user) to ensure that the correct status is shown in the user interface.

```
sudo /usr/tideway/tripwire/sbin/tripwire --check > /usr/tideway/var/tw_tripwire.txt
/usr/tideway/bin/tw_baseline
```
The appliance status is updated.

For more information about using Tripwire and baseline configuration, see Baseline configuration.

**tw_config_dashboards**

The `tw_config_dashboards` utility enables you to configure and customize dashboards in BMC Atrium Discovery.

✅ **Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_config_dashboards` command line utility (see Using and customizing dashboards). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_config_dashboards [options] title
```

where:

- `title` is the title of the dashboard. If a title is not specified, an error is displayed.
- `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--lock</code></td>
<td>Specifies to lock the dashboard so that it is read-only (the default)</td>
</tr>
<tr>
<td><code>--ls</code></td>
<td>Specifies to display a list of the current dashboards and whether they are locked or unlocked. For this option only, a title does not need to be specified.</td>
</tr>
<tr>
<td><code>--unlock</code></td>
<td>Specifies to unlock the dashboard so that it can be edited</td>
</tr>
</tbody>
</table>

**User example**

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.
Changing a dashboard

By default, dashboards are configured to be read-only. If you want to customize a dashboard, you first need to make it accessible using the `--unlock` option:

```
$TIDEWAY/bin/tw_config_dashboards --unlock Default
```

tw_convert_reports

The `tw_convert_reports` utility enables you to manually customize reports and channels on the appliance. This utility can serve as a standalone tool to manually convert reports from the old format to the new format (introduced in Tideway Foundation 7.3) after you have upgraded BMC Atrium Discovery and started the system.

⚠️ Note

The new report format was introduced in Tideway Foundation 7.3. Therefore, the utility is required only for report files that have been manually copied from an appliance version earlier than 7.3 to an appliance version later than 7.3. If you upgrade to a BMC Atrium Discovery version later than 7.3, the utility runs automatically.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
$TIDEWAY/bin/tw_convert_reports options reports_file
```

where:

- `reports_file` is the name of the xml reports file to be converted. If a file name is not specified, an error is displayed.

- `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d</code>, <code>--debug</code></td>
<td>Specifies to display debug messages</td>
</tr>
</tbody>
</table>
### Command Line Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-r, --rename</code></td>
<td>Specifies to rename the input file <code>reports_file.old</code> and save the converted file as <code>reports_file</code>. If there are errors, they are written to the terminal and the file is not converted.</td>
</tr>
<tr>
<td><code>-v, --verbose</code></td>
<td>Specifies to display errors and warning messages. If no errors are reported, the reports and charts work the same way they did in the previous version. These messages are also written in the comments section of the converted file.</td>
</tr>
</tbody>
</table>

### User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

#### Converting a reports file

To convert a consolidated report file named `30ListenerReports.xml`, type the following command:

```
$ cd /usr/tideway/data/custom/reports
$ ls
30ListenerReports.xml
$ TIDEWAY/bin/tw_convert_reports 30ListenerReports.xml

Generated converted_30ListenerReports.xml (0 errors, 2 warnings)
$ ls
30ListenerReports.xml
converted_30ListenerReports.xml
$ 
```

The file is converted and saved as a new file prepended with `converted_`. The original file is not changed.

**tw_cron_update**

The `tw_cron_update` utility is used to manage tideway user cron.

⚠️ **Warning**

Do not use `crontab -e` to edit the tideway user cron directly on the appliance.

To use the utility, type the following command at the `$TIDEWAY/bin` directory:

```
tw_cron_update
```
Cron overview

BMC Atrium Discovery makes use of cron on the appliance to run various housekeeping tasks. This means that crontab must not be directly edited on the appliance, but must instead be managed using `tw_cron_update`. This way, BMC Atrium Discovery can manage cron entries across upgrades without affecting, or being affected by, any local customizations.

Cron entries are stored in `$TIDEWAY/etc/cron`. Each cron entry has its own file, using the file extension `.cron` to identify that file. A cron entry is created by adding a new file ending with `.cron` containing standard cron formatted commands. Similarly entries can be edited or removed by editing or removing `.cron` files.

`$TIDEWAY/bin/tw_cron_update` checks, every time it is run, that the file has not been edited since `tw_cron_update` was last run.

A note on the format of a cron entry is provided in the `tw_cron.header` file. For full details, see the Red Hat Enterprise Linux 5 cron documentation.

⚠️ Note

If crontab has been directly edited, `tw_cron_update` can no longer manage cron. You will have to manually resolve any differences before continuing. A copy of the expected cron configuration is stored as `$TIDEWAY/etc/cron/tw_cron.previous` whenever `tw_cron_update` is run. This can be compared to the live configuration. If this file does not exist, then the utility has never been used and crontab should be used as the default.

Managing cron entries

Cron entry files in `$TIDEWAY/etc/cron` are applied to the live cron configuration by running `$TIDEWAY/bin/tw_cron_update` as the tideway user.

- Run `$TIDEWAY/bin/tw_cron_update` as the tideway user. Every time the script is run it confirms that the current live cron configuration matches what BMC Atrium Discovery expects it to be. If the configuration is as expected, there will be no output. If there is a discrepancy, an appropriate message will be displayed, and the discrepancy must be resolved before continuing.
- To add a new cron entry, add a new `.cron` file.
- To remove a cron entry, remove its `.cron` file, or modify the file extension to something other than `.cron`, (for example, `.disabled`.
- To modify a cron entry, edit its `.cron` file.
- Run `$TIDEWAY/bin/tw_cron_update` as the tideway user.
User example

One use of the `tw_cron_update` utility is to schedule an appliance snapshot using the `tw_scheduled_snapshot` utility. The following example schedules a snapshot at 1 a.m. on the first day of every month.

- Create a new file named `$TIDEWAY/etc/cron/scheduled_snapshot.cron`
- Add the cron entry to it as follows:

```
# Snapshot once a month at 1am
0 1 1 * * tw_scheduled_snapshot
```

- Run `tw_cron_update`.

It is safe to use `crontab -l` to see the current cron content.

**tw_deluser**

The `tw_deluser` utility enables you to delete a BMC Atrium Discovery user. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_deluser [options] username
```

where:

- `username` is the name of the user to delete
- `options` are any of the common arguments described in Using command line utilities.

**User example**

In the following example, a user deletes another user named `Joe` with a specific logging level of `info`.

**Deleting a user with a specific logging level**

```
$TIDEWAY/bin/tw_deluser --loglevel=info Joe
```
tw_disco_control

The `tw_disco_control` utility enables you to manually control specific functions of the BMC Atrium Discovery process. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
 tw_disco_control [options] [opt=val ...]
```

where:

- `opt=val ...` is a list of options to be set.
- `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

⚠️ **Warning**

`tw_disco_control` controls the Discovery process. It does not control the discovery status (Reasoning process). If you want to change the discovery status, use `tw_scan_control`. When the Discovery process is stopped, discovery runs can start but they will fail. Use caution when using the `--emergency`, `--start`, and `--stop` options.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--devices</code></td>
<td>Specifies to display current devices</td>
</tr>
<tr>
<td><code>--emergency</code></td>
<td>Specifies to stop BMC Atrium Discovery immediately. All scheduled discovery scans are stopped.</td>
</tr>
<tr>
<td><code>--passphrase=ARG</code></td>
<td>Specifies the passphrase of the vault</td>
</tr>
<tr>
<td><code>--playback</code></td>
<td>Specifies to set BMC Atrium Discovery into playback mode</td>
</tr>
<tr>
<td><code>--quiet</code></td>
<td>Specifies that the user does not receive any informational messages</td>
</tr>
<tr>
<td><code>--record</code></td>
<td>Specifies to set BMC Atrium Discovery into recording mode</td>
</tr>
<tr>
<td><code>--standard</code></td>
<td>Specifies to set BMC Atrium Discovery into standard operating mode. It cannot be set to playback or record mode.</td>
</tr>
<tr>
<td><code>--start</code></td>
<td>Specifies to start BMC Atrium Discovery. All scheduled discovery scans are started.</td>
</tr>
<tr>
<td><code>--stop</code></td>
<td>Specifies to stop BMC Atrium Discovery. All scheduled discovery scans are stopped.</td>
</tr>
<tr>
<td><code>--test-cancel=ARG</code></td>
<td>Specifies to cancel a specified test</td>
</tr>
<tr>
<td><code>--test-remove=ARG</code></td>
<td>Specifies to remove a specified test</td>
</tr>
<tr>
<td><code>--tests</code></td>
<td>Specifies to display current tests</td>
</tr>
</tbody>
</table>
### Command Line Option

#### Description

- **-u, --username=NAME**
  Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, `system`.

### User example

In the following example, you can stop a discovery scan in progress.

#### Stopping the discovery process

```bash
$TIDEWAY/bin/tw_disco_control
--stop
```

Any regular scans and snapshot scans currently in progress will stop, and no subsequent scans can be started until you restart the discovery process.

### tw_disco_export_platforms

The `tw_disco_export_platforms` utility enables you to export the customizable platform scripts used by BMC Atrium Discovery so that they can be copied to another appliance, where they can subsequently be imported using `tw_disco_import_platforms`. After the scripts are imported, the corresponding platforms are displayed on the Administration => Discovery Platforms page.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```bash
tw_disco_export_platforms [options]
```

where **options** are any of the options described in the following table and the common command line options described in **Using command line utilities**.

#### Note

A password is required to use the commands.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--default</td>
<td>Specifies to only export default platform scripts (not current scripts)</td>
</tr>
<tr>
<td>-o, --output=FILE</td>
<td>Specifies the name of the output file. The default name is <code>platforms.xml</code>.</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium user. If no name is specified, BMC Atrium Discovery uses the default, <code>system</code>.</td>
</tr>
</tbody>
</table>
User example
In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

Transferring custom commands to another appliance
The following example illustrates how to transfer a command to an appliance, or back it up separately to a snapshot (if you had previously customized the command):

```bash
$TIDEWAY/bin/tw_disco_export_platforms --password 'secret'
--output my_scripts_backup.xml
```

Note
Any commands you subsequently import will override existing content in the snapshot. The import process will not affect anything on the appliance that is not in the .xml file. (For example, if you manually deleted a lot of content from the .xml file, and then imported it, nothing would be removed from the appliance.)

tw_disco_import_platforms
The `tw_disco_import_platforms` utility enables you to import the customizable platform scripts used by BMC Atrium Discovery after they have been copied to another appliance, where they have been exported using `tw_disco_export_platforms`. After the scripts are imported, the corresponding platforms are displayed on the Administration => Discovery Platforms page. To use the utility, type the following command at the `TIDEWAY/bin/` directory:

```bash
tw_disco_import_platforms [options] files
```

where:

- **files** is a list of files to be imported (except for when you use the `reset` option).
- **options** are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--reset</td>
<td>Resets all commands to the default value. This is equivalent to clicking <strong>Reset All</strong> on the Administration =&gt; Platforms page (except only commands that have been customized will display).</td>
</tr>
</tbody>
</table>
### Command Line Option

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u, --username=NAME</td>
<td>Specify the name of the BMC Atrium user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

### User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

#### Importing previously exported discovery scripts

The following command imports previously exported scripts to an appliance:

```
$TIDEWAY/bin/tw_disco_import_platforms --password 'secret'
my_scripts_backup.xml
```

**Note**

Any commands that you import will override content in the snapshot. The import process will not affect anything on the appliance that is not in the .xml file. (For example, if you manually deleted a lot of content from the .xml file, and then imported it, nothing would be removed from the appliance.)

#### tw_ds_compact

The `tw_ds_compact` utility enables you to compact the datastore by copying all the data within the datastore and writing a new copy of the database files. Because it creates a new set of files, it compacts any gaps in the files where data has been deleted before, helping to alleviate lost disc space caused by fragmentation.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:

```
tw_ds_compact [options] source_dir destination_dir
```

where:

- `source_dir` is the name of the source directory where database files are being copied from.
- `destination_dir` is the name of the destination directory for the new database files.
• options are any of the options described in the following table and the common command line options described in Using command line utilities.

⚠️ Warning

Because the utility directly accesses database files, you must prepare the database beforehand to avoid damage to crucial data. Before compacting the datastore, back it up by performing an Appliance Snapshot. Failing to do so could result in data loss. For instructions, run the utility using the --docs option and review the instructions. Also see the User Example for an example of how the utility works.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --docs</td>
<td>Displays crucial documentation about the utility, including what tasks to perform before and after you run the utility</td>
</tr>
<tr>
<td>-c, --recode</td>
<td>Specifies to recode old-format data values with a more-efficient 7.3 encoding</td>
</tr>
</tbody>
</table>

⚠️ Warning

The tw_ds_compact utility has a number of additional options that modify the underlying storage parameters. These options will lead to irreversible data loss and should not be used unless you are instructed to do so by BMC Customer Support.

For more information about compacting the datastore offline, see Compacting the datastore.

User example

In the following example, you can use the tw_ds_compact utility to prepare and run a compaction.

Preparing for and running a database compaction

Preparing the database for compaction

The following steps safely prepare the database before you run the compaction.

⚠️ Run as the tideway user

You must to execute this procedure as the tideway user. Executing it as root will prevent the datastore working correctly due to internal permissions problems.

1. Login to the appliance command line as the tideway user.
2. Stop the tideway services.

   [tideway@appliance01 ~]$ sudo /sbin/service tideway stop

3. Make a copy of all data files in the directory /usr/tideway/var/tideway.db/data/datadir.

   [tideway@appliance01 ~]$ mkdir <backup datadir pathname>
   [tideway@appliance01 ~]$ cd /usr/tideway/var/tideway.db/data/datadir
   [tideway@appliance01 datadir]$ cp -pv * <backup datadir pathname>

4. Make a copy of the log files in the directory /usr/tideway/var/tideway.db/logs.

   [tideway@appliance01 datadir]$ mkdir <backup logs pathname>
   [tideway@appliance01 datadir]$ cd /usr/tideway/var/tideway.db/logs
   [tideway@appliance01 logs]$ cp -pv * <backup logs pathname>

5. Type the following command:

   [tideway@appliance01 logs]$ cd /usr/tideway/var/tideway.db/data/datadir

6. Type the following command:

   [tideway@appliance01 datadir]$ /usr/tideway/BerkeleyDB.n.n/bin/db_recover -v

   where \textit{n.n} represents the Berkeley DB version.

7. Type the following command:

   [tideway@appliance01 datadir]$ rm __db.*

Creating new database files to perform data compaction

After you prepare the database, the files are ready to be compacted.
Best Practice

The destination disk must be big enough to store the compacted database. To minimize thrashing between reading the old files and writing new ones, store the new databases on a different physical disk. Generally, the new databases will be smaller than the originals, but you should ensure that there is at least the same amount of space as there is taken by the current databases.

In the following example, new database files are created and subsequently stored on /mnt/mybigdisk.

1. Run the utility:

```
tw_ds_compact /usr/tideway/var/tideway.db/data/datadir /mnt/mybigdisk
```

As it runs, it outputs numbers to show its progress as it copies the databases.

2. If you want to record the information, use `tee` to display the script's output and store it to a file:

```
tw_ds_compact /usr/tideway/var/tideway.db/data/datadir /mnt/mybigdisk | tee compact.log
```

The script outputs numbers to show its progress as it copies the databases.

To recode data values created by earlier versions of Tideway Foundation, run the utility as follows:

```
tw_ds_compact --recode /usr/tideway/var/tideway.db/data/datadir /mnt/mybigdisk
```

When the script finishes, the original database files are not modified, and a new copy is stored in the destination directory.

If the compact finished successfully, then finish the operation by performing the following steps:

3. Remove the log files:

```
rm -f /usr/tideway/var/tideway.db/logs/*
```
4. Remove the old database files:

```bash
rm -f /usr/tideway/var/tideway.db/data/datadir/*
```

5. Move the new files into the `/usr/tideway/var/tideway.db/data/datadir` directory:

```bash
cd /usr/tideway/var/tideway.db/data/datadir
mv /mnt/mybigdisk/* .
```

6. Start the tideway services. Type the following command:

```bash
sudo /sbin/service tideway start
```

The datastore automatically rebuilds the transactional environment so that the `__db.*` files return and a `log.0000000001` file is created in the logs directory.

**tw_excluderanges**

The `tw_excluderanges` utility enables you to exclude IP ranges from discovery. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```bash
tw_excluderanges [options] args
```

where:

- `args` are one of the following arguments:
  - `--add` returns a list of files or IP ranges to exclude
  - `--replace` returns a list of files or IP ranges to replace
  - `--remove` returns a list of range IDs to remove

**Note**

If you do not select an argument in the command, a list of the currently excluded ranges is displayed, which includes the exclude range ID and additional information about that range. You could redirect this output to a file and then clean it up in a text editor to serve as a file which could then be imported.
• options are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add</td>
<td>Specifies to add a new exclude range</td>
</tr>
<tr>
<td>-d, --description= ARG</td>
<td>Specifies a description for the exclude range. Use double quotes around strings with spaces.</td>
</tr>
<tr>
<td>-f, --file</td>
<td>Specifies a file or a list of files to read IP ranges from. This is useful for importing large numbers of exclude ranges.</td>
</tr>
<tr>
<td>-n, --name=ARG</td>
<td>Specifies the name of the exclude range. Use double quotes around strings with spaces.</td>
</tr>
<tr>
<td>-r, --remove</td>
<td>Specifies to remove an exclude range</td>
</tr>
<tr>
<td>-x, --replace</td>
<td>Specifies to add any addresses that have been located, and then clear the current list of exclude ranges</td>
</tr>
<tr>
<td>-s, --silent</td>
<td>Specifies to turn off all informational messages</td>
</tr>
<tr>
<td>-u, --username</td>
<td>Specifies the name of the BMC Atrium Discovery user. If a name is not specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

User example
In the following examples, type the commands on a single line. Line breaks are provided to make the example easier to read.

Excluding an IP range from discovery

```
$TIDEWAY/bin/tw_excluderanges 172.17.1.1-5
--description "Mission critical brewing equipment"
```

Importing IP ranges to use as exclude ranges
You can import multiple IP addresses or ranges if they are contained in text files, one IP address or range per line. Ranges can be specified as usual:
• IP addresses, as a single address or a range, for example 192.168.1.1 or 192.168.1.1-5
• A subnet, for example 192.168.1.0/24
• A * wildcard, for example 192.168.1.*

An example file called excludes1.txt:

```
192.168.1.100
192.168.1.110-120
```

A second example file called excludes2.txt:
Import the exclude ranges from the two files using the following command:

```
[tideway@appliance01 ~]$ tw_excluderanges --username=system --add
   --name="Imported Ranges" --file excludes1.txt excludes2.txt
Password:
Feeding file excludes1.txt
Feeding file excludes2.txt
Add excluded range: 192.168.1.100, 192.168.1.110-120, 192.168.2.100-105,
192.168.2.*, 192.168.3.0/24 Imported Ranges
[tideway@appliance01 ~]$ 
```

tw_imp_ciscoworks

The `tw_imp_ciscoworks` utility enables you to import CiscoWorks network device data from the command line.

✅ Best Practice

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_imp_ciscoworks` command line utility (see Importing network device data). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_imp_ciscoworks [options] --username name
   --file filename
```

where:

- `--username name` is the BMC Atrium Discovery user name to use to import data.
- `--file filename` is the name of the CiscoWorks data file to import.
• *options* are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--delimiter 'delimiter'</td>
<td>Specifies the field delimiter for input files. The default is the tab character.</td>
</tr>
<tr>
<td>--destroy-missing</td>
<td>Removes network devices and associated ports that do not exist in the imported data</td>
</tr>
<tr>
<td>--has-header</td>
<td>Specifies that the CiscoWorks data file to import has a header row</td>
</tr>
<tr>
<td>--no-header</td>
<td>Specifies that the CiscoWorks data file to import has no header row</td>
</tr>
<tr>
<td>--xml</td>
<td>Specifies that the data file being imported is in XML format, not CSV</td>
</tr>
</tbody>
</table>

**User examples**

In the following examples, enter the commands on a single line. Line breaks are provided to make the examples easier to read.

**Generating and importing CSV files**

To generate a CSV file on the CiscoWorks server, type the following:

```
C:\Program Files\CSCOpx\campus\bin\ut -cli -query all
   -layout StandardTideway -export c:\data.csv
   -u user -p password
```

This command produces a Java stack trace. This is a known issue and can be ignored. The file that is produced can be imported by running the following command on the BMC Atrium Discovery appliance:

```
$TIDEWAY/bin/tw_imp_ciscoworks --delimiter=','
   --username name --password password
   --file ~/tmp/data.csv
```

**Generating and importing XML files**

To generate an XML file on the CiscoWorks server, type the following:

```
C:\Program Files\CSCOpx\campus\bin\cmexport ut -u userid
   -p password -host -layout StandardTideway
```
The file is written into the following directory:
C:\PROGRAM FILES\CSCOpx\files\cmexport\ut

The file can be imported onto the BMC Atrium Discovery appliance with the following command:

```
$TIDEWAY/bin/tw_imp_ciscoworks --xml --username name
--password password --file ~/tmp/2006516154526ut.xml
```

tw_imp_csv

The `tw_imp_csv` utility enables you to search the datastore for nodes of a specified kind that have keys matching rows in the supplied csv data. Where the keys match, the node is updated, or deleted and recreated (depending on the options selected).

**Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_imp_csv` command line utility (see Importing CSV data). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

**Incorrect usage may result in data loss**

Before using the `tw_imp_csv` tool you should fully understand the system taxonomy and the changes that you are going to make to your data. Using the `tw_imp_csv` tool incorrectly can cause irreparable damage to your data. The data you submit using this tool is applied directly to the production data without any validation.

Always back up your datastore before using this tool.

**Do not import the following node kinds**

- You *must never* import DDD nodes.
- You should avoid importing Host nodes and other system maintained nodes. If in doubt, contact Customer Support.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:
tw_imp_csv [options] files

where:

- **files** is a list of csv files to import.
- **options** are any of the options described in the following table and the common command line options described in *Using command line utilities*.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--create</td>
<td>Specifies that only new nodes will be created; existing nodes are not updated</td>
</tr>
<tr>
<td>--datastore=</td>
<td><em>(Do Not Use)</em> Specifies the name of the datastore service. The default is tideway.</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
<tr>
<td>--delete</td>
<td>Specifies that matching nodes will be deleted; no other nodes will be affected</td>
</tr>
<tr>
<td>--delimiter=ARG</td>
<td>Specifies a field delimiter character</td>
</tr>
<tr>
<td>--escape-char=ARG</td>
<td>Specifies an escape character</td>
</tr>
<tr>
<td>--force</td>
<td>Disables the validation checks that are performed against the taxonomy to check the specified node-kind and attribute/relationship keys. When you use this option, all keys, attributes and relationship links will be left as strings.</td>
</tr>
<tr>
<td>--keys=keys</td>
<td>Displays a comma-separated list of key columns to use for the data key</td>
</tr>
<tr>
<td>--kind=kind</td>
<td>Displays the kind of node to create, update, or clear</td>
</tr>
<tr>
<td>--line-terminator=ARG</td>
<td>Specifies a line termination string</td>
</tr>
<tr>
<td>--partition=</td>
<td>Specifies the name of the partition to query, where name can be set to All for all partitions (the default).</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
<tr>
<td>--quote-char=ARG</td>
<td>Specifies a quote character</td>
</tr>
<tr>
<td>--search=name</td>
<td><em>(Do Not Use)</em> Specifies the name of the search service</td>
</tr>
<tr>
<td>--taxonomy=name</td>
<td><em>(Do Not Use)</em> Specifies the name of the taxonomy service</td>
</tr>
<tr>
<td>--update</td>
<td>Specifies that only existing nodes will be updated; new nodes will not be created</td>
</tr>
<tr>
<td>--upload=UPLOAD</td>
<td>Specifies to hide the name of the uploaded file</td>
</tr>
<tr>
<td>--username=name-u</td>
<td>Specifies the BMC Atrium Discovery user name to use to import data. If no name is specified, you are prompted for one.</td>
</tr>
<tr>
<td>--verbose</td>
<td>Specifies to display informational messages while processing. This is useful for diagnosing errors</td>
</tr>
</tbody>
</table>
User examples

In the following examples, enter the commands on a single line. Line breaks are provided to make the examples easier to read.

Freeing rack space for applications

To free rack space for other applications, some hosts have been moved from the 'Campus' data centre to the newly acquired 'Firehouse' data centre. Discovery and Reasoning have handled the IP address and subnet changes but the Host nodes are still linked to the wrong location. Here is the CSV file to process, called firehouse_move.csv:

<table>
<thead>
<tr>
<th>name</th>
<th>#HostInLocation:HostLocation:LocationOfHost:Location.name</th>
</tr>
</thead>
<tbody>
<tr>
<td>egon</td>
<td>Firehouse</td>
</tr>
<tr>
<td>ray</td>
<td>Firehouse</td>
</tr>
<tr>
<td>peter</td>
<td>Firehouse</td>
</tr>
</tbody>
</table>

BMC Atrium Discovery processes the CSV file with the following utility at the command line:

```
$ tw_imp_csv --username=system --password=system --kind=Host firehouse_move.csv
```

The utility reads the file called firehouse_move.csv line by line. It uses the first line to name the columns. The first column is called 'name', which doesn't begin with a '#' character so it is treated as an attribute name. The second column does begin with a '#' character so it is treated as a specification for some relationships.

No explicit key has been specified so the first (and in this case, only) attribute name is taken to be the key.

Next, the utility reads the second line. The first field, egon, is in the name column which was selected as the key earlier. So the script uses the search service to find a node of kind Host (from the --kind command line option) that has a name attribute equal to egon. It finds exactly one node matching that search. If it had not found that node, it would have been created. If it had found multiple nodes, an error would have been reported and processing would continue with the next line, NO nodes would have been updated.

Having found the node, it updates it using the other fields on the row. Were there any other attribute columns in the the file, the utility would have used these to update the node before looking at the relationships.

The file has only one relationship column. The name is #HostInLocation:HostLocation:LocationOfHost:Location.name. The utility searches for a Location node with a name attribute equal Firehouse, this row's value
for the column. Having found the Location node, the utility creates a HostLocation relationship to
it with the Host node playing the HostInLocation role and the Location playing the
LocationOfHost role.

Then the utility processes the second and third data rows, updating the ray and peter nodes with
the new location.

Installing a remote Windows proxy

A new host has been installed in the Firehouse data centre. Due to pressure from the organisation's
E-services Protection Adviser, there is now a firewall preventing discovery of hosts on that site.
Until a remote Windows proxy can be installed, the Firehouse system administrators have been
sending us spreadsheets with the changes.

The CSV file new_host.csv looks like the following:

```
name,fqdn,#HostInLocation:HostLocation:LocationOfHost:Location.name,#ITOwnedItem:ITOwner:ITOwner:Person.name,ip_addrs,#HostOnSubnet:HostSubnet:Subnet.name
winston,winston.example.com,Firehouse,"Melnitz,J","[10.3.4.1,'192.168.101.45']","[10.0.
```

BMC Atrium Discovery processes the CSV file with the following utility at the command line:

```
$ tw_imp_csv --username=system --password=system --kind=Host --create new_host.csv
```

The syntax is nearly the same as in the previous example. The differences are that the filename
has changed because we are processing a different file and we are using Create Only mode.

As in the previous example, the utility searches for Host nodes with a name attribute equal to
winston. This time, because it is in create mode, the utility checks that there are no matching
nodes. If there were, the utility would report an error and skip the row.

Next, the utility creates a new node. It populates the attributes of the node from the non-relationship
fields in the data. The ip_addrs field is a list and the value starts with a '[' character so it is
converted into a list. The new node has attributes:

- name = 'winston'
- fqdn = 'winston.example.com'
- ip_addrs = [ '10.3.4.1', '192.168.101.45' ]

Then the utility adds the relationships. The location relationship column is processed in the same
way as in Example 1. The column called #ITOwnedItem:ITOwner:ITOwner:Person.name
creates an ITOwnedItem:ITOwner:ITOwner relationship to a Person node with a name equal to
Melnitz,J. The quotes around that field are needed because the field contains a comma.
After the quote, the #HostOnSubnet:HostSubnet:Subnet.name field begins with a '[' character. This field is converted into a list. Then, for each item in the list, a HostOnSubnet:HostSubnet:Subnet relationship is created to a Subnet node with a name attribute equal to that item. So the new host has one relationship to the 10.0.0.0/8 subnet and one to the 192.168.101.0/24 subnet.

**tw_injectip**

⚠️ **Deprecated utility**

The `tw_injectip` utility is now deprecated and may be removed in future releases. Its functionality is available in the `tw_scan_control` utility which has all of the same options.

The `tw_injectip` utility enables you to scan IP ranges using the command line.

遵守《推荐》

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_injectip` command line utility (see Controlling discovery). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_injectip [options] range
```

where:

- **range** is a single IP address or range (for example, `172.17.1.1` or `172.17.1.1-5`), a space-separated list of IP addresses, a range of IP addresses, or a subnet (for example, `172.17.1.0/24`). If you use the
  --file option, a range refers to a file that contains IP addresses.

- **options** are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--clean</td>
<td>Removes all the recurrent ranges that are not currently being scanned from the Reasoning pipeline.</td>
</tr>
<tr>
<td>Command Line Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--company=companyname</td>
<td>Specify a company name to use for a scan in a multitenant deployment.</td>
</tr>
<tr>
<td>-f, --file</td>
<td>A file or a list of files of IP addresses. They must be plain text files with a new line delimited list of IP addresses.</td>
</tr>
<tr>
<td>--label=label</td>
<td>Specifies a label for the scan.</td>
</tr>
<tr>
<td>--passphrase=passphrase</td>
<td>Specifies a vault passphrase to use</td>
</tr>
<tr>
<td>-r, --random</td>
<td>Specifies to scan the IP addresses (located in a file or listed at the command prompt) in random order</td>
</tr>
<tr>
<td>--recur-daily</td>
<td>Specifies to add a daily recurrent range. This option specifies a recurrent range scan that must be modified with the --recurrence-duration and/or --recurrence-start options.</td>
</tr>
<tr>
<td>--recurrence-duration=int</td>
<td>Specifies the duration that the recurring scan lasts (in hours).</td>
</tr>
<tr>
<td>--recurrence-start=int</td>
<td>Specifies the start time for recurrent ranges (in hours) after midnight</td>
</tr>
<tr>
<td>--replace=ID</td>
<td>Replace (edit) the specified scheduled discovery run. The discovery run is specified using its ID which can be determined using a search query like the following: search IPRange where scan_type='Scheduled' show range_id,label. See below for examples.</td>
</tr>
<tr>
<td>-l, --scanLevel=arg</td>
<td>Specifies the scan level to use. This may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>* Sweep Scan: Performs a sweep scan, trying to determine what is at each endpoint in the scan range. Attempts to login to a device to determine the device type.</td>
</tr>
<tr>
<td></td>
<td>* Full Discovery: Retrieve all the default information for hosts and complete full inference.</td>
</tr>
<tr>
<td></td>
<td>* Default: Use the current default level.</td>
</tr>
<tr>
<td></td>
<td>Scan levels Sweep Scan and Full Discovery should be quoted as they contain spaces.</td>
</tr>
<tr>
<td>-s, --start</td>
<td>Specifies that Reasoning will start. This is equivalent to clicking the START ALL SCANS button.</td>
</tr>
<tr>
<td>-x, --stop</td>
<td>Specifies that Reasoning will stop. This is equivalent to clicking the STOP ALL SCANS button.</td>
</tr>
<tr>
<td>-u, --username=username</td>
<td>Specifies the name of the BMC Atrium Discovery user. If a user is not specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

**User examples**

In the following examples, the user name is system and the password is not specified on the command line. The utility prompts for the password after you enter the command. Type the commands on a single line; line breaks are provided in the examples to make them easier to read.

⚠️ **Note**

The utility is designed to handle only snapshot and daily scans; no weekly or monthly schedules are available within this tool. For this functionality, use the user interface.
Specifying an immediate scan of a single IP address

```
$TIDEWAY/bin/tw_injectip --username system 192.168.0.1
```

Specifying an immediate scan of a single IP address at Sweep Scan level

```
$TIDEWAY/bin/tw_injectip --username system -l 'Sweep Scan' 192.168.0.1
```

Specifying an immediate scan of a range of IP addresses

```
$TIDEWAY/bin/tw_injectip --username system 192.168.0.1-10
```

Specifying an immediate scan of IP addresses listed in a file

```
$TIDEWAY/bin/tw_injectip --username system --file ~/scanlist
```

Specifying a scheduled scan of IP addresses listed in a file at 03.00

```
$TIDEWAY/bin/tw_injectip --username system --recur-daily
   --recurrence-start=3 --file ~/scanlist
```

Specifying a two-hour scheduled scan of IP addresses listed in a file

```
$TIDEWAY/bin/tw_injectip --username system --recur-daily
   --recurrence-duration=2 --file ~/scanlist
```

Specifying a two-hour scheduled scan of IP addresses listed in a file and label it TEST

```
$TIDEWAY/bin/tw_injectip --username system --recur-daily
   --recurrence-duration=2 --scheduled-label=TEST --file ~/scanlist
```
Replacing a discovery run

The following example illustrates how to find the ID of a scheduled discovery run and use it to update the run's label. The way that this option works is to delete and replace the scan, so it is important to specify all essential parameters (recur-daily, recurrence-duration and/or recurrence-start, and a range).

1. In the Enter Generic Query page, enter the following query and click Run Query:

   ```
   search IPRange where scan_type='Scheduled' show range_id, label
   ```

2. Copy the ID from the range that you want to replace and use it to specify the ID of the scan that you want to replace.

3. Enter the command. This example illustrates how a system user replaces a specified scan with a daily six-hour scan of the range 192.168.0.1-10 and a label of UPDATED.

   ```
   tw_injectip -u system -p system --recur-daily --recurrence-duration=6 --label=UPDATED --replace 85be3f2d9ef810d84c1089485c704129 192.168.0.1-10
   ```

**tw_listusers**

The `tw_listusers` utility enables you to display BMC Atrium Discovery user information, and lets you filter our specific names you do not want to display. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
  tw_listusers [options] --filter=ARG
```

where:

- `--filter=ARG` specifies a filter (regular expression) for listing users. Only users whose username match this regular expression are listed.

- `options` are the common, inherited commands described in Using command line utilities.

**User example**

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

Filtering the list of users to just those whose username contains the string "joe"
$TIDEWAY/bin/tw_listusers --filter=joe

tw_model_init

The tw_model_init utility enables you to initialize the model, this consists of deleting any data that you have in the datastore and reapplying the taxonomy. The utility can also install and activate a TKU after deleting the datastore. The TKU package must be stored on the appliance filesystem.

The tw_model_init utility does not delete configuration data held outside the datastore. However, some configuration information is held in the datastore and is lost when running tw_model_init. This is:

- Scan ranges
- Scheduled scan ranges
- Exclude ranges
- Scan levels (default scan level and those which can be selected when adding a new scan)
- CAM (saved queries, groups and subgroups, named values, functional component definitions, and generated patterns)

If you suspect datastore corruption, consult the knowledgebase article KA325751 to determine whether the datastore is corrupted. If you discover that there is corruption then you should contact BMC Customer Support.

Warning

The tw_model_init utility deletes all data in your datastore. Before you use tw_model_init to resolve an issue, it is recommended that you contact BMC Customer Support.

Important

You must stop all tideway services before running the utility. Restart the services after you run the utility.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:

tw_model_init [options]

where options are any of the options described in the following table and the common command line options described in Using command line utilities.
# Command Line Option

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--force</td>
<td>Specifies to remove any existing tideway.db datastore.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning</strong> Use this argument with caution! It deletes all data stored in your datastore!</td>
</tr>
<tr>
<td>--no-tku</td>
<td>Specifies to not automatically install and activate a TKU package. This improves the speed of the utility.</td>
</tr>
<tr>
<td>--tku-dir</td>
<td>Specifies to install a TKU from a location other than $TIDEWAY/data/installed/tpl</td>
</tr>
</tbody>
</table>

## User example

By default, the `tw_model_init` utility activates the TKU package that came with the version of BMC Atrium Discovery appliance that you have installed. If you are not planning to use that TKU, you can set the `--no-tku` option to save you time when running the utility. However, if you use this option and then forget to subsequently load a TKU, your BMC Atrium Discovery instance will collect significantly less data.

### Initializing the model without activating a TKU

The following example illustrates how you can initialize the model without installing and activating a TKU:

```
$TIDEWAY/bin/tw_model_init --no-tku
```

### Effect on CMDB synchronization

When a host has significantly changed so that its key has also changed, problems can be caused if you run `tw_model_init` before the changed host is rediscovered. On the next CMDB synchronization, duplicate hosts are created in the CMDB representing the changed host, and the CIs representing the original hosts are never deleted.

To ensure that no duplicate hosts are created after running `tw_model_init` and then synchronizing the data, perform the following tasks before running the utility:

1. Soft-delete all existing CIs in the BMC.ADDM dataset.
2. Run a reconciliation and a purge so that the deletion is propagated to the BMC.ASSET dataset.

## tw_passwd

The `tw_passwd` utility enables you to change the password of a specified user interface user. To use the utility, type the following command at the $TIDEWAY/bin/ directory:
tw_passwd [options] username

where:

- **username** is the name of the new user to change.
- **options** are the common, inherited commands described in Using command line utilities.

### User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

**Changing a user's password**

```
$TIDEWAY/bin/tw_passwd joe
joeuser
```

⚠️ **Changing passwords for command line users**

The `tw_passwd` utility is for changing UI users’ passwords. To change the passwords for command line users, as the root user, use the Linux command `passwd`. This is described in Changing the root and user passwords

### tw_pattern_management

The `tw_pattern_management` utility enables you to upload patterns to the appliance, activate or deactivate patterns on the appliance, and delete patterns that are no longer required. It does not enable you to manage entire Technology Knowledge Updates (TKUs), because they contain a number of file types. You should always manage TKUs through the user interface (UI).

✅ **Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_pattern_management` command line utility (see Pattern management). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment. Be aware that informational messages for packages may be displayed in the UI but are not available using this tool at the command line.
To use the utility, type the following command at the $TIDEWAY/bin/ directory:

```
$TIDEWAY/bin/tw_pattern_management [options] <package/module file> [package description]
```

where:

- **package/module file** is the name of the package. This argument is also used by the `install-package` and `replace-module` options.

- **package description** is a description of the package. This argument is also used by the `install-package` and `replace-module` options.

- **options** are any of the options described in the following table and the common command line options described in **Using command line utilities**.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--activate-all</code></td>
<td>Specifies to activate all installed packages</td>
</tr>
<tr>
<td><code>-a, --activate-package=PKG_NAME</code></td>
<td>Specifies to activate the pattern package and enable associated patterns</td>
</tr>
<tr>
<td><code>-d, --deactivate-package=PKG_NAME</code></td>
<td>Specifies to deactivate the specified pattern package</td>
</tr>
<tr>
<td><code>-e, --erase-packages</code></td>
<td>Specifies to remove all pattern packages</td>
</tr>
<tr>
<td><code>-f, --force</code></td>
<td>Specifies to deactivate patterns before they are removed</td>
</tr>
<tr>
<td><code>-i, --install-package=PKG_FILE</code></td>
<td>Specifies to upload the specified pattern package</td>
</tr>
<tr>
<td><code>-l, --list-packages</code></td>
<td>Specifies to list uploaded pattern packages</td>
</tr>
<tr>
<td><code>-P, --partition=NAME</code></td>
<td>Specifies the name of the datastore partition</td>
</tr>
<tr>
<td><code>-R, --recompile-active-packages</code></td>
<td>Specifies to recompile all active packages</td>
</tr>
<tr>
<td><code>-r, --remove-package=PKG_NAME</code></td>
<td>Specifies to remove the specified pattern package</td>
</tr>
<tr>
<td><code>--replace-module=MODULE_NAME</code></td>
<td>Specifies to replace specified pattern package with another pattern module</td>
</tr>
<tr>
<td><code>-u, --username=NAME</code></td>
<td>Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
<tr>
<td><code>--verbose</code></td>
<td>Specifies to display informational messages</td>
</tr>
</tbody>
</table>
To understand TPL patterns and how they might function in your environment, reference Configipedia, BMC’s community website that facilitates knowledge sharing around TPL patterns. Configipedia also provides visibility of the Technology Knowledge Update release schedule and contents.

A link to Configipedia is provided for the Pattern Module lists in the Pattern Management section of the Discovery Page. There is also a link to Configipedia provided from the Software Instance nodes and Business Application Instance nodes that are maintained by TPL software patterns.

**User examples**

In the following examples, type the commands on a single line. Line breaks are provided to make the example easier to read.

**Replacing a pattern module**

You can replace a pattern module by specifying the new name and using the `--replace-module=MODULE_NAME` option. To replace a pattern module, type the following command:

```
$TIDEWAY/bin/tw_pattern_management --replace-module=VMware.VM.VMware
VMwareVM.VMwareConsolidateFromSI
```

The changed pattern module is contained in a package with the suffix `editn` applied to the original name. The number `n` is incremented by one after each subsequent edit. The package and pattern module that you edit is noted in the description column of the Pattern Module Source window. The replacement package is made active if the one you edited was active.

**Uploading several TPLs as a package**

In the following example, a shop has six collection servers and one consolidation server, and they want to be able to quickly upload a set of TPL files without having to do so one at a time. Using the `tw_pattern_management` utility, you can package several TPL files in a .zip file and upload the patterns to the appliance.

To upload a set of TPLs:

1. Zip the files from the command line and name the .zip file:

```
[tideway@app01 tpl]$ zip mypackage.zip tpl/*tpl
  adding: tpl/1config.tpl (deflated 46%)
  adding: tpl/6247_IIOPl_only_JMX.tpl (deflated 61%)
  [...]
  adding: tpl/Zilla11939.tpl (deflated 50%)
```
2. Use the utility to upload the zipped package (providing your password to execute the
calendar):

```bash
[tideway@app01 tpl]$ tw_pattern_management -i "my package" mypackage.zip
Password:
[tideway@app01 tpl]$ 
```

**tw_query**

The `tw_query` utility enables you to extract data using a query. The information can be output in
CSV or XML format using one of the available arguments.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_query [options] query
```

where:

- **query** is the data you want to extract from the Search service.
- **options** are any of the options described in the following table and the common command
  line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--csv,</td>
<td>Specifies that the output of the query will be saved in .CSV format</td>
</tr>
<tr>
<td>--delimiter=CHAR</td>
<td>Specifies the delimiter character used in .CSV files</td>
</tr>
<tr>
<td>--file=FILE</td>
<td>Specifies the name of the .CSV output file</td>
</tr>
<tr>
<td>--no-headings</td>
<td>Do not output column headings</td>
</tr>
<tr>
<td>--partition=NAME</td>
<td>Specifies the name of the partition to query</td>
</tr>
<tr>
<td>--search=NAME</td>
<td>Specifies the name of the search service</td>
</tr>
<tr>
<td>--time</td>
<td>Reports the time taken to perform the query</td>
</tr>
<tr>
<td>--xml</td>
<td>Specifies that the output of the query will be saved in .XML format</td>
</tr>
</tbody>
</table>

**tw_reasoningstatus**

The `tw_reasoningstatus` utility enables you to view the status of the Reasoning service.
Typically this utility is used by Customer Support as a troubleshooting tool for investigating possible
problems.
Note

Reasoning runs the same status check automatically every 15 minutes and outputs the results in the `tw_svc_reasoning.log` file.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_reasoningstatus [options]
```

where `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--waiting, -w</td>
<td>Lists information for all endpoints which are on hold waiting for information from the discovery of a different endpoint.</td>
</tr>
<tr>
<td>--waiting-full</td>
<td>Expands the information provided by --waiting to include information on all endpoints being held waiting for discovery. This option is ignored if --waiting is not specified.</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, <code>system</code>.</td>
</tr>
</tbody>
</table>

User example

In the following example, you can view the status of the Reasoning service for user `joe`.

**Viewing the status of the Reasoning service**

To view the status of the Reasoning service, type the following command:

```
$TIDEWAY/bin/tw_reasoningstatus --username joe
```

If you do not provide a password, you are prompted for one.

After providing a password, a status is displayed that includes information about engine status, pool state, queue length, and so forth. The output is saved in the `tw_svc_reasoning.log` file.

**tw_remove_darkspace**

The `tw_remove_darkspace` utility enables you to remove any previously-discovered Dark Space DiscoveryAccess nodes from the datastore.

Important
This utility should only be used when you initially set the Dark Space Suppression scheme from Keep All to Keep Most Recent or Remove ALL. Otherwise, you should rely on the suppression scheme selected and avoid using this utility entirely. Running `tw_remove_darkspace` multiple times serves no useful purpose and will take a long time. The time it takes depends entirely on the amount of dark space in your environment and it is not unknown for it to take more than a day to run.

Background

Originally BMC Atrium Discovery kept all nodes, including dark space nodes. This Dark Space Suppression scheme was called Keep All and is now deprecated. The `tw_remove_darkspace` utility removes these extra nodes immediately; although they would be removed as usual over a period of time during DDD aging.

When an endpoint is discovered and there is no response, it is considered NoResponse. The system traverses back along the complete DiscoveryAccess chain and if it finds any DiscoveryAccess with an associated device then the endpoint is still considered NoResponse. It may be, for example, that the machine is temporarily down. Where no associated device is found, the endpoint is then considered dark space and the subsequent behavior depends on the dark space removal setting. This may be either:

- **Keep Most Recent**: the system removes all but the current DiscoveryAccess.
- **Remove All**: the system removes all DiscoveryAccesses.

An effect of DDD aging is that an endpoint, which at one point in time had an associated device, can become a chain of no response DiscoveryAccesses. So, `tw_remove_darkspace` may find new dark space that it can remove, however, this would have been removed automatically when the endpoint is next scanned.

If an endpoint was associated with an inferred device (Host, MFPart, NetworkDevice, Printer) at any time it remains connected via an AccessFailure until the inferred device is removed, even if that device has changed endpoints.

Usage

Run `tw_remove_darkspace` while the services are running. Existing discoveries can be running while you execute the utility. When run, the utility stops reasoning, removes dark space, and then restarts reasoning. You might notice a pause in any existing discoveries while the utility runs. The utility outputs the results in the `tw_remove_darkspace.log` file.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_remove_darkspace [options]
```
where *options* are any of the options described in the following table and the common command line options described in **Using command line utilities**.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--quiet</td>
<td>Specifies that informational messages will not be printed.</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

**User example**

In the following example, the utility is run with no options to remove dark space DA nodes from the datastore.

```bash
$TIDEWAY/bin/tw_remove_darkspace
Password: system
WARNING: Dark space removal may take considerable time to complete.
WARNING: Please be patient.
Stopping Reasoning processing events
Checking for dark space
Found 113 IPs to check
Checking IPs 0 to 112
113 of which are dark space
Completed removal of dark space DiscoveryAccess nodes
Check for unconnected DiscoveryRuns
No unconnected DiscoveryRuns
Restarting Reasoning processing events
Dark space removal complete.
```

**tw_scan_control**

The *tw_scan_control* utility enables you to scan IP ranges using the command line.

**Recommendation**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the *tw_scan_control* command line utility (see **Controlling discovery**). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:
tw_scan_control [options] range

where:

- **range** is a single IP address or range (for example, 172.17.1.1 or 172.17.1.1-5), a space-separated list of IP addresses, a range of IP addresses, or a subnet (for example, 172.17.1.0/24). If you use the **--file** option, a range refers to a file that contains IP addresses.

- **options** are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--clean</td>
<td>Specifies to remove all the recurrent ranges that are not currently being scanned from the Reasoning pipeline</td>
</tr>
<tr>
<td>--company=companyname</td>
<td>Specify a company name to use for a scan in a multitenant deployment.</td>
</tr>
<tr>
<td>-f, --file</td>
<td>Displays a file or a list of files as arguments. They must be plain text files with a new line delimited list of IP addresses.</td>
</tr>
<tr>
<td>--label=label</td>
<td>Specifies a label for the scan</td>
</tr>
<tr>
<td>--passphrase=passphrase</td>
<td>Specifies a vault passphrase to use</td>
</tr>
<tr>
<td>-r, --random</td>
<td>Specifies to scan the IP addresses (located in a file or listed at the command prompt) in random order</td>
</tr>
<tr>
<td>--recur-daily</td>
<td>Specifies to add a daily recurrent range. This option specifies a recurrent range scan that must be modified with the --recurrence-duration and/or --recurrence-start options.</td>
</tr>
<tr>
<td>--recurrence-duration=int</td>
<td>Specifies the duration that the recurring scan lasts (in hours).</td>
</tr>
<tr>
<td>--recurrence-start=int</td>
<td>Specifies the start time for recurrent ranges (in hours) after midnight</td>
</tr>
<tr>
<td>--replace=ID</td>
<td>Replace (edit) the specified scheduled discovery run. The discovery run is specified using its ID which can be determined using a search query like the following: search IPRange where scan_type='Scheduled' show range_id,label. See below for examples.</td>
</tr>
<tr>
<td>-l, --scanLevel=arg</td>
<td>Specifies the scan level to use. This may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>* Sweep Scan: Performs a sweep scan, trying to determine what is at each endpoint in the scan range. Attempts to login to a device to determine the device type.</td>
</tr>
<tr>
<td></td>
<td>* Full Discovery: Retrieve all the default information for hosts and complete full inference.</td>
</tr>
<tr>
<td></td>
<td>* Default: Use the current default level.</td>
</tr>
<tr>
<td>-s, --start</td>
<td>Specifies that Reasoning will start. This is equivalent to clicking START ALL SCANS.</td>
</tr>
</tbody>
</table>
**Command Line Option** | **Description**
--- | ---
-x, --stop | Specifies that Reasoning will stop. This is equivalent to clicking **STOP ALL SCANS**.
-u, --username= username | Specifies the name of the BMC Atrium Discovery user. If a user is not specified, BMC Atrium Discovery uses the default, **system**.

### User examples

In the following examples, the user name is **system** and the password is not specified on the command line. The utility prompts for the password after you enter the command. Type the commands on a single line; line breaks are provided in the examples to make them easier to read.

- **Note**

  The utility is designed to handle only snapshot and daily scans; no weekly or monthly schedules are available within this tool. For this functionality, use the user interface.

#### Specifying an immediate scan of a single IP address

```
$TIDEWAY/bin/tw_scan_control --username system 192.168.0.1
```

#### Specifying an immediate scan of a single IP address at Sweep Scan level

```
$TIDEWAY/bin/tw_scan_control --username system -l 'Sweep Scan' 192.168.0.1
```

#### Specifying an immediate scan of a range of IP addresses

```
$TIDEWAY/bin/tw_scan_control --username system 192.168.0.1-10
```

#### Specifying an immediate scan of IP addresses listed in a file

```
$TIDEWAY/bin/tw_scan_control --username system --file ~/scanlist
```
Specifying a scheduled scan of IP addresses listed in a file at 03.00

```bash
$TIDEWAY/bin/tw_scan_control --username system --recur-daily --recurrence-start=3 --file ~/scanlist
```

Specifying a two-hour scheduled scan of IP addresses listed in a file

```bash
$TIDEWAY/bin/tw_scan_control --username system --recur-daily --recurrence-duration=2 --file ~/scanlist
```

Specifying a two-hour scheduled scan of IP addresses listed in a file and label it TEST

```bash
$TIDEWAY/bin/tw_scan_control --username system --recur-daily --recurrence-duration=2 --label=TEST --file ~/scanlist
```

Replacing a discovery run

The following example illustrates how to find the ID of a scheduled discovery run and use it to update the label on a run. The way that this option works is to delete and replace the scan, so it is important to specify all essential parameters (recur-daily, recurrence-duration and/or recurrence-start, and a range).

1. In the Enter Generic Query page, enter the following query:

   ```bash
   search IPRange where scan_type='Scheduled' show range_id, label
   ```

2. Click Run Query.

3. Copy the ID from the range that you want to replace and use it to specify the ID of the scan that you want to replace.

4. Enter the command.

   This example illustrates how the system user replaces a specified scan with a daily six-hour scan of the range 192.168.0.1−10 and a label of UPDATED.

   ```bash
tw_scan_control -u system -p system --recur-daily --recurrence-duration=6 --label=UPDATED --replace 85be3f2d9ef810d84c1089485c704129 192.168.0.1-10
   ```
tw_scheduled_snapshot

The **tw_scheduled_snapshot** utility enables you to use the cron feature to schedule and transfer appliance snapshots.

**Best Practice**

You can use the BMC Atrium Discovery user interface to perform appliance snapshots without a schedule. If you do so, see [Using appliance snapshot](#) for important prerequisites for taking the snapshot.

The **tw_scheduled_snapshot** utility should be scheduled using the cron feature ($TIDEWAY/etc/cron) as the tideway user. For more information, see [tw_cron_update](#). However, you can also run a snapshot that creates a current snapshot that you can view in the user interface.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:

```
tw_scheduled_snapshot [options]
```

where *options* are any of the options described in the following table and the common command line options described in [Using command line utilities](#).

**Note**

Although the **--target** options are not required, you must use all four together for a transfer to occur. When transferring a snapshot to a host running SSH, you should do so using an account created specifically for this purpose.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>--child_timeout=</strong></td>
<td></td>
</tr>
<tr>
<td>TIMEOUT</td>
<td>Specifies the timeout period for child processes during the transfer</td>
</tr>
<tr>
<td><strong>--delete_snap</strong></td>
<td>Removes the snapshot as the script exits. This allows the snapshot to be removed after transfer to preserve disk space on the appliance.</td>
</tr>
<tr>
<td><strong>--early_release</strong></td>
<td>Specifies release maintenance mode or reasoning early</td>
</tr>
<tr>
<td><strong>--interactive</strong></td>
<td>Confirms that the user wants to run a snapshot. This argument prompts you to confirm that you want to take the snapshot (Y or N).</td>
</tr>
<tr>
<td>Command Line Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>--pessimistic</td>
<td>Specifies that the creation of the snapshot will continue only if 3 times the size of the datastore is available as free disk space. Otherwise, if pessimistic is not specified, 2 times the size of the datastore will be required for the snapshot to continue. Space is needed for 1) a complete clone of the files, 2) creation of a tarball, and 3) storage of temp files during the snapshot procedure. The worst case is that this would take 3 times the size of the datastore if it is too large to compress. Two times the size of the datastore is the normal space requirement as we are typically able to compress but require a large amount of space for temp files.</td>
</tr>
<tr>
<td>--snapshot_name=string</td>
<td>Specifies a name for the created snapshot. While the allowed characters are unlimited, more than 30 characters is not recommended. The default value is Scheduled Snapshot.</td>
</tr>
<tr>
<td>--snapshot_notes=string</td>
<td>Specifies a notes field for the created snapshot. This is a free text field supporting new line and essentially unlimited. It is advised that this field be used to tag the snapshot with shell variables such as the hostname for tracking purposes. The default value is Scheduled Snapshot.</td>
</tr>
<tr>
<td>--target_host=string</td>
<td>Specifies the target host running SSH. It can be specified as an IP address or a hostname.</td>
</tr>
<tr>
<td>--target_user=string</td>
<td>Specifies the user name of the account on the target host. When transferring a snapshot to another appliance you should always use the migrate user.</td>
</tr>
<tr>
<td>--target_pass=string</td>
<td>Specifies the password of the account on the target host</td>
</tr>
<tr>
<td>--target_root=string</td>
<td>Specifies the relative path to the snapshot archive root on the target host. Snapshots are directories and should be stored under an archive root directory. This directory must be a local one under the user account in use; the name snapshots is recommended. When transferring a snapshot to another appliance you should always specify --snapshot for this option.</td>
</tr>
</tbody>
</table>

**User examples**

In the following examples, type the commands on a single line. Line breaks are provided to make the example easier to read.

**Scheduling a snapshot**

The primary purpose of the `tw_scheduled_snapshot` utility is to schedule a snapshot; however, can do so with no scheduling using no arguments in the script. The following syntax generates a snapshot that can then be viewed on the **Administration => Appliance => Snapshot & Restore** page:

```
[tideway@eu-64 ~]$ tw_scheduled_snapshot

The utility stops scanning before creating the snapshot, and then restarts scanning after the snapshot is created. Optionally, you can name the snapshot and provide a description in the Notes field. The snapshot displays in the Appliance Snapshots section of the Snapshot & Restore page.
Transferring a snapshot

You can use the `tw_scheduled_snapshot` utility to transfer the snapshot to another appliance or to a remote host running SSH. To do so, type the following commands:

```
$TIDEWAY/bin/tw_scheduled_snapshot --snapshot_name="Scheduled Snapshot"
--target_host=172.23.24.16
--target_user=migrate
--target_pass=blueberry38
--target_root=$TIDEWAY/var/snapshot/snapshots/
```

**Best Practice**

When transferring snapshots onto an appliance using the command line you should use the `migrate` user, which has a home directory that is the default location for uploading snapshots, and has limited access to the appliance. See the `migrate` user for information on enabling this user.

Deleting a snapshot

You can make the script delete the local copy of the snapshot after it has been transferred to a remote host or migrated to another appliance. To do so, type the following command:

```
$TIDEWAY/bin/tw_scheduled_snapshot --delete_snap --snapshot_name="Scheduled Snapshot"
```

tw_sign_winproxy_config

The `tw_sign_winproxy_config` utility enables you to add a checksum to a Windows proxy configuration file without uploading the file. When you run this utility, it modifies the specified file but also saves a copy named `<original filename>.orig` before signing the file.

**Best Practice**

Use the BMC Atrium Discovery user interface to perform the functionality provided by the `tw_sign_winproxy_config` command line utility (see the Windows proxy configuration file). If you choose to run the utility, read the documentation in this section to learn its usage and to understand the risks and potential impact on your environment.

To use the utility, type the following command at the `$TIDEWAY/bin/` directory:
tw_sign_winproxy_config [options]

where options are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--config-file=PATHNAME</td>
<td>Specifies the name of the configuration file to sign</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Displays the name of the BMC Atrium Discovery user. If a name is not specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

**Adding a checksum to a Windows proxy configuration file**

In the Checksum section of the Windows proxy configuration file, the checksum ensures that the file has not been tampered with since it has been copied or uploaded from the appliance. Using the `tw_sign_winproxy_config` utility, you can add the checksum without uploading the file to the appliance. To add the checksum to the file, type the following command:

```bash
$TIDEWAY/bin/tw_sign_winproxy_config --config-file=C:\Program Files\BMC Software\ADDM Active Directory Proxy\etc\winproxy.conf
```

You can then copy the signed file to multiple appliances using ftp or similar.

**tw_tax_export**

The `tw_tax_export` utility enables you to export taxonomy files so that they can be stored in another location. This utility can be used as an effective troubleshooting tool to check if all your taxonomy overlays worked as you expected, especially if you left old files in place or ordered them incorrectly.

Taxonomy definitions are configured using .xml files that are stored in the following directories:

```
/usr/tideway/data/installed/taxonomy/
/usr/tideway/data/custom/taxonomy/
```
The directories are parsed in the order shown (installed files take precedence over custom files), and the files contained in these directories are parsed in alphabetical order (numbers before letters). This order is important, because any taxonomy definitions that are subsequently added override any previously loaded definitions. The standard base taxonomy file is contained in /usr/tideway/data/installed/taxonomy/00taxonomy.xml.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:

```bash
$TIDEWAY/bin/tw_tax_export [options]
```

where `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

### Using command line utilities

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-D, --datastore=NAME</td>
<td>(Do Not Use) Specifies the name of the datastore service</td>
</tr>
<tr>
<td>-P, --partition=NAME</td>
<td>Specifies the name of the datastore partition</td>
</tr>
<tr>
<td>-r, --relkinds=REGEXP</td>
<td>Specifies the RelationshipKinds to export</td>
</tr>
<tr>
<td>-l, --rolekinds=REGEXP</td>
<td>Specifies the RoleKinds to export</td>
</tr>
<tr>
<td>--sort</td>
<td>Specifies to sort names</td>
</tr>
<tr>
<td>-t, --taxonomy=LOC</td>
<td>(Do Not Use) Specifies the name of the taxonomy service</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium Discovery user. If no user is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

### User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

#### Exporting a taxonomy file

```
$TIDEWAY/bin/tw_tax_export
/usr/tideway/data/installed/taxonomy/00taxonomy.xml
```

### tw_tax_import

The `tw_tax_import` utility enables you to import custom taxonomy files into the current taxonomy.
**Recommendation**

After you run a taxonomy import using this utility, you must restart the tideway service. Failure to do so will result in a malfunctioning user interface.

Taxonomy definitions are configured using .xml files that are stored in the following directories:

/usr/tideway/data/installed/taxonomy/
/usr/tideway/data/custom/taxonomy/

The directories are parsed in the order shown (installed files take precedence over custom files), and the files contained in these directories are parsed in alphabetical order (numbers before letters). This order is important, because any taxonomy definitions that are subsequently added override any previously loaded definitions. The standard base taxonomy file is contained in /usr/tideway/data/installed/taxonomy/00taxonomy.xml.

To use the utility, type the following command at the $TIDEWAY/bin/ directory:

```
tw_tax_import [options] files
```

where:

- **files** is a list of files to be imported. This command is optional if you use the **--clear** option, but cannot be used with the **--handle-broken-extensions** option.

- **options** are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--clear</td>
<td>Specifies to clear any existing taxonomy before importing</td>
</tr>
<tr>
<td>-h, --handle-broken-extensions</td>
<td>Specifies to ignore any broken extensions. If a taxonomy extension is invalid, the importer ignores it and restarts, attempting to load all other extensions. It repeats this until it has loaded the base taxonomy and has loaded or attempted to load all extensions. In this way you always finish with a valid taxonomy. Where the taxonomy importer fails to load an extension it logs a message to stdout. This option cannot be used with the files command. It is primarily intended for upgrading, but it can be used from the command line.</td>
</tr>
<tr>
<td>-D, --datastore=NAME</td>
<td><em>(Do Not Use)</em> Specifies the name of the datastore service</td>
</tr>
<tr>
<td>--merge</td>
<td>Specifies to merge import data with any existing taxonomy</td>
</tr>
<tr>
<td>-P, --partition=NAME</td>
<td>Specifies the name of the datastore partition</td>
</tr>
<tr>
<td>--replace</td>
<td>Specifies to replace data in any existing taxonomy with imported data</td>
</tr>
<tr>
<td>--strict</td>
<td>Specifies that there is no backwards compatibility for the previous format</td>
</tr>
</tbody>
</table>
### Command Line Option Description

- **-t, --taxonomy=ARG** *(Do Not Use)*
  Specifies the name of the taxonomy service

- **-u, --username=NAME**
  Specifies the name of the BMC Atrium Discovery user. If no user is specified, BMC Atrium Discovery uses the default, *system*.

- **--verbose**
  Specifies to display informational messages

- **--verify**
  Specifies to verify XML data only

### User example

In the following example, type the commands on a single line. Line breaks are provided to make the example easier to read.

#### Importing customized taxonomy definitions

The following example illustrates how to import a custom taxonomy file and merge the imported data into the existing taxonomy.

1. Type the following command:

   ```
   $TIDEWAY/bin/tw_tax_import --merge /usr/tideway/data/custom/taxonomy/MYtaxonomy.xml
   ```

   The standard base taxonomy file named `/usr/tideway/data/installed/taxonomy/00taxonomy.xml` is supplemented with the imported data, and you can view the updated `installed.xml` file on the `Administration > Taxonomy` page.

2. Restart the tideway service.

### tw_terminate_winproxy

The `tw_terminate_winproxy` utility enables you to send a request to the Windows proxy to terminate operation. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
 tw_terminate_winproxy [options]
```

where **options** are any of the options described in the following table and the common command line options described in Using command line utilities.

#### Important

You must have the `discovery/kslave/write` permission to use the utility.
<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--proxy-name proxyname</td>
<td>(Optional) Specifies the name of the Active Directory, Workgroup or Credential Windows proxy that you are logging into</td>
</tr>
<tr>
<td>--username username</td>
<td>(Optional) Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

**User example**

In the following example, you must have the discovery/kslave/write permission to use the utility.

**Stopping a running credential Windows proxy**

```
$TIDEWAY/bin/tw_terminate_winproxy --proxy-name my_proxy
```

When the utility successfully sends a terminate request to a Windows proxy, an audit event is logged. The audit event, named windows_proxy_process_terminate, contains the name of the Windows proxy that the terminate request is sent to.

**Important**

If a Windows proxy is not running as either the Local System account or as a member of the Administrators group, tw_terminate_winproxy will fail to stop the Windows proxy. The following error is logged in the Windows proxy log file:

```
ERROR: Failed to terminate slave service: [(5, 'OpenSCManager', 'Access is denied.')] 
```

**Workaround:** Allow the user that the Windows proxy is running to stop the Windows proxy service. This is documented on the Microsoft Support Site.

For more information about Windows proxy configuration, see Additional Windows proxy configuration.

**tw_tripwire_rebaseline**

The tw_tripwire_rebaseline utility enables you to rebaseline a Tripwire database. Tripwire is a third-party software tool that monitors a specific set of configuration, system, and source files on an appliance. When you use the utility to rebaseline the Tripwire database, you accept that all files that are being monitored are correct. To use the utility, type the following command at the $TIDEWAY/bin/ directory:
tw_tripwire_rebaseline

You might use the script to initialize the Tripwire database, commission and configure Tripwire, or to run a reconfiguration procedure after the rebaseling process returns errors. For more information about rebaselining Tripwire and baseline configuration, see Baseline configuration.

**User example**

In the following example, a user updates the Tripwire database after an error. This procedure should be performed as the tideway user.

**Updating the tripwire database after an error**

1. Check the items that are reported in the violation report and ensure that the reported changes are what you expected.
2. Run the following command:

```
/usr/tideway/bin/tw_tripwire_rebaseline
```

**tw_upduser**

The `tw_upduser` utility enables you to update properties of a specific user, such as the current state, permissions, and passwords. To use the utility, type the following command at the `$TIDEWAY/bin/` directory:

```
tw_upduser [options] username
```

where:

- `username` is the name of the user to update
- `options` are any of the options described in the following table and the common command line options described in Using command line utilities.

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--active</td>
<td>Sets the user to an ACTIVE state</td>
</tr>
<tr>
<td>--blocked</td>
<td>Sets the user to a BLOCKED state</td>
</tr>
<tr>
<td>--disabled</td>
<td>Sets the user to a DISABLED state</td>
</tr>
<tr>
<td>Command Line Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-f, --fullname=ARG</td>
<td>Sets a full name of the user</td>
</tr>
<tr>
<td>-G, --groups=GROUP ,...</td>
<td>Sets the user's group membership</td>
</tr>
<tr>
<td>--locked</td>
<td>Sets the user to a LOCKED state</td>
</tr>
<tr>
<td>--passwd-must-change</td>
<td>Specifies that the password must be changed</td>
</tr>
<tr>
<td>--passwd-ok</td>
<td>Specifies that the password is okay as currently stated</td>
</tr>
<tr>
<td>--passwd-should-change</td>
<td>Specifies that the password should be changed</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

**User example**

In the following example, the *tw_upduser* utility sets the user *Joe* to a locked state to protect from unauthorized changes to that account.

### Locking a user for security purposes

To lock a user, type the following command:

```bash
$TIDEWAY/bin/tw_upduser --locked Joe
```

The following confirmation is displayed:

```
Set User State USER_STATE_LOCKED
```

To unlock the user, run the utility again with the `--active` option.
Discovery

This section describes how BMC Atrium Discovery operates and how to configure and run the product.

The Discovery Engine is designed to locate systems in the network and obtain relevant information from them as quickly as possible, using a variety of different tools and techniques to communicate with devices.

The Reasoning Engine works on the raw data obtained by the Discovery Engine to infer the maximum amount of information about hosts and programs and populate the datastore intelligently. The Reasoning Engine uses patterns that identify running software based on the network ports, processes found, packages installed, protocols used, and so on. It also intelligently searches the discovered data to resolve relationships between items of software.

- Running discovery
- Configuring discovery
- Extending discovery
- Improving discovery
- Credentials
- Consolidation
- Pattern management
- Technology Knowledge Update (TKU)
- Integration points

Running discovery

This section describes how you run and monitor Discovery. It contains the following sections:

- Viewing discovery status: describes how you monitor Discovery using the Discovery Status page.
- Controlling discovery: describes how to start and stop Discovery and create Discovery runs.

Controlling discovery

You can start either an immediate or scheduled scan in BMC Atrium Discovery by clicking the Add New Run link from the Discovery status page.

You can control the discovery process using various options dependent on the type of scan you initiate.

For immediate scans, you can run a snapshot scan of a specified address range right away, whether or not the regular discovery scan is in progress. The specified addresses are scanned automatically and as soon as possible. You can also assign a discovery run to a company name.
For scheduled scans, you can:

- Specify the IP range that is scanned during the normal discovery run.
- Schedule a scan to occur at any time and for a specified amount of time. For example, you might want to schedule a scan during off hours to avoid the risk of touching critical applications.
- Assign a discovery run to a company name.
- Delete a selected range or ranges, or all IP addresses from the regular scan and the snapshot scan lists.

You can stop and restart the discovery process at any time.

⚠️ In order to start the Discovery process, you must click **START ALL SCANS** on the Discovery Status page, as by default Discovery is off.

For general information about the discovery process, see The Discovery Engine.

Scanning IP addresses or ranges immediately

1. Click **Add New Run**.
2. Enter the information for the snapshot discovery run in the fields.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
| Range      | Enter either a single IP address or a range in one of the following formats:  
- IP addresses, as a single address or a range, or a comma separated list, for example, 172.17.1.1 or 172.17.1.1-5 or 172.17.1.1, 172.17.1.2, 172.17.1.3  
- A subnet, for example 172.17.1.0/24  
- A wildcard, for example 172.17.1.* |
| Level      | Select the level for the discovery run. This is one of:  
- **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.  
- **Full Discovery**: This will retrieve all the default info for hosts, and complete full inference. |
| Label      | Enter a label for the discovery run. Where the discovery run is referred to in the UI, it is this label that is shown. |
| Company    | Select the company name to assign to the discovery run. This drop-down list is only displayed if multitenancy has been set up. If (No company) is displayed, or a company names you were expecting is missing, refresh the list by clicking **Lookup Companies** on the CMDB Sync. See multitenancy for a full explanation of this feature. |

⚠️ The default company set by default here will only be used by default in the discovery run. If you set the company to "(no company)" the CIs will be exported with no company and the default value won't be used.
3. Click **OK**.
   The Currently Processing Runs tab is displayed with the new run.

### Scheduling a discovery run

You can schedule a discovery run to occur daily, weekly, or monthly and can specify a start time and duration.

To schedule a scan:

1. Click **Add New Run ...**

   ![Warning: On a consolidation appliance the link name is Add New Local Run ...](image)

2. Select **Scheduled**.
   The dialog displays Frequency, Start Time, and Duration menus.

3. Enter the information for the scheduled scan in the fields.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
   | **Range**  | Enter either a single IP address or a range in one of the following formats:  
   |            | • IP addresses, as a single address or a range, or a comma separated list, for example, 172.17.1.1 or 172.17.1.1-5 or 172.17.1.1, 172.17.1.2, 172.17.1.3  
   |            | • A subnet, for example 172.17.1.0/24  
   |            | • A wildcard, for example 172.17.1.* |
   | **Level**  | Select the level for the discovery run. This is one of:  
   |            | • **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.  
   |            | • **Full Discovery**: This will retrieve all the default info for hosts, and complete full inference. |
   | **Label**  | Enter a label for the discovery run. Where the discovery run is referred to in the UI, it is this label that is shown. |
   | **Company**| Select the company name to assign to the discovery run. This drop-down list is only displayed if multitenancy has been set up. If (No company) is displayed, or a company names you were expecting is missing, refresh the list by clicking **Lookup Companies** on the CMDB Sync. See multitenancy for a full explanation of this feature. |
   | **Frequency** | Select a frequency for the discovery run to be performed. For example, this can be Daily, Weekly, or Monthly.  
   |            | For a weekly discovery run, you are provided with buttons for each day. Select the day or days that you want the run to take place.  
   |            | For a monthly discovery run, you are provided with buttons for each day in the month. Select the day or days that you want the run to take place. Alternatively, select the Scan on the radio button and choose one of:  
   |            | • First  
   |            | • Second  
   |            | • Third |
### Field Name Details

- Fourth
- Last
and the day that you want the scan to take place. In this way you can select the Second Tuesday of the month and so forth.

<table>
<thead>
<tr>
<th>Start Time</th>
<th>Select a time for the scan to start. Discovery will need to be running at this time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Select a duration in hours. This is the length of the scan window and can be from 1 to 23 hours. If this duration expires before the scan has completed, then the scan will be suspended until the next scheduled time for this scan occurs. At that point, the scan will resume from the point where it was previously suspended.</td>
</tr>
</tbody>
</table>

4. Click OK. The Scheduled Runs tab is displayed with the new run.

To add another scan to the page, click **Add New Run**. To delete any existing scheduled scans, select the entry and click **Delete**.

#### Editing an existing scheduled run

You can edit an existing scheduled run. If the run is currently in progress it is automatically cancelled when you edit it. To do this, from the Scheduled Runs tab of the Discovery Status page:

1. Click on the Scheduled Run that you want to edit.

   ![Edit an Existing Run](image)

   **This screen illustrates where to edit an existing run.**

   All of the fields described in the previous table can be edited.

2. Make the required changes and click **OK**.

#### Excluding IP addresses and ranges from scanning

There may be some IP devices in your network that you never want to be scanned. For example, you may have some legacy applications which will only run on old hardware which may be regarded as *fragile*. You can add this device as a single IP exclude, or as an Exclude Range.

To add an Exclude Range:

1. On the **Exclude Ranges** tab on the Discovery Status page, click **Add New Exclude**.
2. Enter the information for the exclude range in the fields.
### Field Name | Details
--- | ---
**Range** | Enter either a single IP address or a range in one of the following formats:
• IP addresses, as a single address or a range, or a comma separated list, for example, 172.17.1.1 or 172.17.1.1-5 or 172.17.1.1, 172.17.1.2, 172.17.1.3
• A subnet, for example 172.17.1.0/24
• A * wildcard, for example 172.17.1.*

**Label** | Enter a label for the discovery run. Where the discovery run is referred to in the UI, it is this label that is shown.

**Description** | A free text description of the exclude range.

3. Click **OK**.
   The Excluded Ranges tab is displayed with the new exclusion.

#### Editing an existing exclude range

You can edit an existing exclude range. To do this:

1. From the **Exclude Ranges** tab of the Discovery Status page:
2. Click on the exclude range that you want to edit.
   All of the fields are editable.
3. Make the required changes and click **OK**.

#### Starting the discovery process

The status of the discovery process is shown at the top of the page. You can click **START ALL SCANS** to start the scan, any scans that are on hold or waiting to start will transition into "In progress". If a run is on hold but outside its scheduled window it will not start.

1. Click **START ALL SCANS**.
   The screen is automatically refreshed to show the progress of the discovery process.

#### Stopping the discovery process

The status of the discovery process is shown at the top of the page. If a scan is in progress, that is "Discovery is running", you can click **STOP ALL SCANS** to stop the scan. Any regular scans and snapshot scans currently in progress will stop. The status changes to "Discovery is stopping" while the process closes.

1. Click **STOP ALL SCANS**.
   No more scans will be started and discovery will attempt to stop all in progress commands.
   After the scan has stopped, no more scans will be performed until you restart the scan.
2. To restart the discovery process, click **START ALL SCANS**.
Viewing discovery status

The status of the discovery process is shown on the Home tab in the Discovery Status summary. This shows the current status of the discovery and reasoning process.

Click **Discovery is currently** by the green **RUNNING** or red **STOPPED** button to display the Discovery Status page.

⚠️ In order to start the discovery process, you must click **START ALL SCANS**, as by default discovery is off.

The Discovery Status page

The Discovery Status page is the central point for running discovery. It contains the following tabs:

- **Currently Processing Runs**: shows the first 10 runs that are currently in progress.
- **Recent Runs**: shows the 10 most recently completed runs.
- **Scheduled Runs**: list the scheduled runs.
- **Exclude Ranges**: shows the first 10 excluded ranges and enables you to add new exclude ranges.
- **Topology Runs**: shows the 10 most recently completed topology runs.

The Discovery Status page also provides a **START ALL SCANS** button or a **STOP ALL SCANS** button depending whether discovery is running or not. The default view of the Discovery Status page, with a snapshot scan in progress, is shown in the following screen.

This screen illustrates the default view of the Discovery Status page.

Consolidation

An appliance may be configured to be either a Consolidation appliance or a Scanning appliance. Consolidation refers to the centralization of discovery data from scheduled or snapshot scans on multiple Scanning appliances to one or more Consolidation appliances. For a detailed description about consolidation and how to configure it, see Consolidation.

Currently Processing Runs

The Currently Processing Runs tab shows the first 10 Discovery runs that are in progress. The Currently Processing Runs tab contains the following fields:
Field Name | Details
---|---
Label | The descriptive label that is applied to the run. This is the label applied by the user who created the run.
Started | The scan start time. This is the time that the Discovery Run was requested rather than the actual start time. In practice these are almost identical, the only time that a large discrepancy is seen is when the Discovery Run is requested at the end of, or outside a scan window.
Range | The IP range that is being scanned in this discovery run. For a large list of IP addresses this shows the first two IP addresses and the number of other IP addresses in the queue.
# of IPs | The total number of IP addresses being scanned in this discovery run.
Type | The type of scan. This is one of:
• Snapshot
• Scheduled
Level | The level for the discovery run. This is one of:
• **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.
• **Full Discovery**: Retrieve all the default info for hosts, and complete full inference.
Percent Complete | A progress indicator showing how much of the scan has been completed and how many are in progress.
User | The user name of the user who created the scan.

If a discovery run is in progress but has been stopped because the scan window in which it can take place has ended, it is **On Hold**. On hold scans are shown in the Currently Processing Runs tab and marked as such.

You can select a discovery run and cancel it using **Cancel**. The discovery run will stop though individual commands in progress will run to completion.

Adding new discovery runs is described in **Controlling discovery**.

**Recent Runs**

The Recent Runs tab shows the 10 most recently completed Discovery Runs, and contains the following fields:

Field Name | Details
---|---
Label | The descriptive label that is applied to the run. This is the label applied by the user who created the run.
Range | The IP range that was scanned in this discovery run.
# of IPs | The total number of IP addresses scanned in this discovery run.
Timing | The scan start time, finish time, and elapsed time. This is the time that the Discovery Run was requested rather than the actual start time. In practice these are almost identical, the only time that a large discrepancy is seen is when the Discovery Run is requested at the end of, or outside a scan window.
Complete | States whether the scan was completed or cancelled by the user.
Type |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Name</td>
<td>Details</td>
</tr>
</tbody>
</table>
| The type of scan. This is one of:  
- Snapshot  
- Scheduled |
| Level | The level for the discovery run. This is one of:  
- **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.  
- **Full Discovery**: Retrieve all the default info for hosts, and complete full inference. |
| User | The name of the user who created the scan. |
| Actions | A **Rescan Now** button is provided in this column which enables you to rescan the discovery run. If you rescan a scheduled scan, it is scanned immediately as a snapshot scan with the same label. |

### Scheduled Runs

The Scheduled Runs tab shows up to 10 scheduled Discovery Runs, and contains the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The descriptive label that is applied to the run. This is the label applied by the user who created the run.</td>
</tr>
<tr>
<td>IP Range</td>
<td>The IP range to be scanned in this discovery run.</td>
</tr>
</tbody>
</table>
| Level | The level for the discovery run. This is one of:  
- **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.  
- **Full Discovery**: Retrieve all the default info for hosts, and complete full inference. |
| Date Rules | Describes the schedule for this discovery run. The days on which the discovery run takes place, the time it starts, and the period in which the scan is permitted to run. |
| State | The scan start time. |
| User | The name of the user who created the run. |
| Created | The date that the scheduled run was created. |

Adding scheduled discovery runs is described in **Scheduled Discovery Run**.

### Exclude Ranges

The Exclude Ranges tab shows the ranges which have been specified as not to be scanned, and contains the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The descriptive label that was applied to the exclude range.</td>
</tr>
<tr>
<td>Range</td>
<td>The IP range that is not to be scanned in any discovery run.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the exclude range.</td>
</tr>
<tr>
<td>User</td>
<td>The user who created the exclude range.</td>
</tr>
</tbody>
</table>
Adding new exclude ranges is described in Exclude Ranges.

**Topology Runs**

The Topology Runs tab shows the 10 most recently completed topology runs, and contains the following fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>The descriptive label that was applied to the topology run.</td>
</tr>
<tr>
<td>Completed/LANs</td>
<td>The number of LANs which have been processed and the total number to be processed.</td>
</tr>
<tr>
<td>Timing</td>
<td>A description for the exclude range.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the run. This may be Processing, Complete, or Canceled.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user who created the run.</td>
</tr>
</tbody>
</table>

Adding a new topology run is described in Adding a topology run.

**Stalled discovery runs**

When a discovery run is scheduled for a particular scan range, the time in which it is scheduled is called its scan window. Scheduled discovery of the scan range can only take place in that open scan window.

**Stalled discovery runs**

Some discovery runs can appear to be stalled. This occurs in one of two situations:

- a discovery run has not completed within its scheduled scan window. This scan is termed *on hold*. The run continues or restarts at the next scan window.
- discovering an endpoint requires additional discovery on another endpoint which is not currently in an open scan window. This scan is termed *blocked*.

When the scan window for the other endpoint opens, the endpoint is scanned irrespective of whether the first endpoint is in an open scan window or not.

In previous releases, there was no way of determining that these situations were causing a run to stall.

**Restart or continue**

At the next scheduled scan window, any on hold or blocked runs will continue or restart, depending on whether all endpoints have been started or not. The behavior change introduced in BMC Atrium Discovery 8.2.1 is described below:

- Scan fails to complete in scan window and all endpoints have *not* been started
  - Pre-8.2.1: scan continues at next window.
  - 8.2.1 and later: scan continues at next window.
- Scan fails to complete in scan window and *all* endpoints have been started
1. Pre-8.2.1: scan continues at next window.
2. 8.2.1 and later: scan restarts at next window.

Blocked and on hold runs in the UI

The Currently Processing Runs tab of the Discovery Status window now displays a red (on hold) notice if a run is on hold and a red (blocked) notice if a run is blocked.

Blocked runs
Click the (blocked) notice. A dialog box is displayed showing why the discovery run is blocked.

The blocked endpoint is shown and the reason for it being blocked is given. In the preceding example, the blocked endpoint is 137.72.94.27 and it is blocked because the \texttt{DiscoveryRuncommand.Disc}overy\texttt{Runcommand} pattern is attempting to access another endpoint (137.72.94.219) which is currently outside a scan window.

On hold runs
Click anywhere in the row of the on hold run to display the Discovery Run page for that run. To check the scanning window:

1. From the Discovery Status page click the Scheduled Runs tab.
2. The timing information for each scheduled run is shown in a table.

If you want to edit the discovery run, click its entry in the table and the Edit an Existing Run dialog box is displayed.

The \texttt{tw_reasoning\_status} command line utility

The \texttt{tw_reasoning\_status} utility enables you to view the status of the Reasoning service. Typically this utility is used by Customer Support as a troubleshooting tool for investigating possible problems.

\begin{boxed_notes}
\textbf{Note}
Reasoning runs the same status check automatically every 15 minutes and outputs the results in the \texttt{tw\_svc\_reasoning.log} file.
\end{boxed_notes}

To use the utility, type the following command at the $\text{TIDEWAY}/bin/ directory:

\begin{verbatim}
tw_reasoningstatus [options]
\end{verbatim}

where \texttt{options} are either the command described in the following table or the standard, inherited options detailed in Using command line utilities.
### Command Line Option

<table>
<thead>
<tr>
<th>Command Line Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--waiting, -w</td>
<td>Lists information for all endpoints which are on hold waiting for information from the discovery of a different endpoint.</td>
</tr>
<tr>
<td>--waiting-full</td>
<td>Expands the information provided by --waiting to include information on all endpoints being held waiting for discovery. This option is ignored if --waiting is not specified.</td>
</tr>
<tr>
<td>-u, --username=NAME</td>
<td>Specifies the name of the BMC Atrium Discovery user. If no name is specified, BMC Atrium Discovery uses the default, system.</td>
</tr>
</tbody>
</table>

### User example

In the following example, you can view the status of the reasoning service.

#### Viewing the status of the Reasoning service

To view the status of the Reasoning service, type the following command:

```bash
$TIDEWAY/bin/tw_reasoningstatus --username joe
```

If you do not provide a password, you are prompted for one. After providing a password, a status is displayed that includes information about engine status, pool state, queue length, and so forth. The output is saved in the `tw_svc_reasoning.log` file.

### Edge connectivity

Edge connectivity refers to the manner in which hosts are connected to edge switches. BMC Atrium Discovery version 8.3 introduces *Edge Connectivity discovery* as a replacement for the network topology feature that was introduced in BMC Atrium Discovery 8.2. It is not a like-for-like replacement, Edge Connectivity does not attempt to calculate overall network topology, rather, it determines which hosts are connected to which edge switches.

Network topology mapping in BMC Atrium Discovery 8.2 required an additional topology run to calculate the topology of a LAN by processing existing Network Devices and calculating switch-to-switch and switch-to-host relationships. Edge connectivity is calculated in the course of a normal discovery run. The separate topology run no longer exists. For information on the previous version of network topology, see the BMC Atrium Discovery version 8.2 documentation.

Edge connectivity discovery occurs when a discovery run takes place. When a switch is discovered, it is queried for port information. The SNMP request *(getPortInfo)* method gathers information on all ports found on the switch, as well as a list of neighbor MAC addresses found for each port.

When a host is discovered, its MAC address or addresses are determined. Reasoning uses the MAC addresses to determine whether there is a connection between that host and any previously scanned switches, and if so, will create a new one. If a connection already exists, then it is confirmed. If no connection is found, any existing connection is deleted.
- When a host is discovered, an old connection may be deleted, and a connection to a switch may be made or confirmed.
- When a switch is discovered, an old connection may be deleted. No new connections are made.

⚠️ Connections are only made when a host is discovered

Connections are only made when a host is discovered, and when the switch that it is connected to has already been scanned. Both ends of the connection are required before the connection can be confirmed. Consequently, connection information may not be complete until two scans have taken place.

The provenance of a connection is the provenance of the host or the switch, whichever was discovered last.

**Enabling or disabling edge connectivity**

Edge connectivity is enabled by default in a fresh install of BMC Atrium Discovery version 8.3. See [upgrades](#) for information on the behavior of upgraded appliances.

If you do not intend to use the connection information obtained by edge connectivity, you can disable it on the [Discovery Configuration](#) page. Disabling edge connectivity will avoid any additional load being put onto switches in your infrastructure. To do this, an additional option [Discover neighbor information when scanning network devices](#) is provided in [Discovery Configuration](#). This option controls whether the information on neighboring ports is obtained.

- Select **Yes** to retrieve neighbor MAC addresses (enable edge connectivity)
- Select **No** if you do not want to retrieve neighbor MAC addresses (disable edge connectivity)

If you do disable edge connectivity, all existing connections are deleted at the time of the next scan.

**Edge connectivity in upgraded appliances**

In a fresh install of BMC Atrium Discovery version 8.3, Edge Connectivity discovery is enabled by default. In an upgraded appliance the behavior is as follows:

**Where network topology has not been used**

Where network topology has not been used, Edge Connectivity discovery is enabled on upgrade. The Topology tab on the Discovery page is removed.

**Where network topology has been used**

Where network topology has been used, it is retained on upgrade. The Topology tab on the Discovery tab is retained and topology runs can be performed in the same way as BMC Atrium Discovery version 8.2. An information banner is displayed describing the new edge connectivity feature. This is shown in the screen below:
This screen shows the topology tab on an appliance upgraded from version 8.2 where the network topology feature has been used.

To enable edge connectivity in the upgraded appliance, click the **Enable Edge Connectivity** button. The screen is refreshed to show that the network topology has been replaced by edge connectivity. When you do enable edge connectivity on an upgraded appliance you must check to ensure that you have removed any cron jobs that performed scheduled topology runs. See [tw_cron_update](#) for details of managing cron jobs.

This screen shows the topology tab on an appliance where network topology has been replaced by edge connectivity.

**Configuring discovery**

Discovery settings can be configured using the Discovery Settings page.

**To set Discovery Settings**

1. From the Discovery section of the **Administration** tab, select **Discovery Configuration**.
   Any non default settings are highlighted by a red change bar.
   The page is grouped into the following sections according to the type of settings:
   - Port Settings
   - Device identification settings
   - Session settings
   - Scanning settings
   - SQL integration settings
   - Other discovery settings
2. Make any required changes to the settings on this page and click **Apply**.

You can also click **Reset To Defaults** to remove any user-defined changes.
Port settings
This section contains settings related to the ports that discovery uses.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP ports to use for initial scan</td>
<td>Enter the TCP ports that will be scanned on a first scan. Use this setting to prevent scanning of any ports that you want to avoid. The default is to use ports: 21, 22, 23, 80, 135, 443, 513, 902 and 3940. Older versions included port 514, which can now be removed from upgraded systems. See notes on #Order of Operations and #TCP and UDP ports to use for initial scan below.</td>
</tr>
<tr>
<td>UDP ports to use for initial scan</td>
<td>Enter the UDP ports that will be scanned on a first scan. Use this setting to prevent scanning of any ports that you want to avoid. The default is port 161. See notes on #Order of Operations and #TCP and UDP ports to use for initial scan below.</td>
</tr>
<tr>
<td>SSH Ports</td>
<td>The default is port 22. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>RLogin Ports</td>
<td>The default is port 513. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>Windows Ports</td>
<td>The default is port 135. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>Telnet Ports</td>
<td>The default is port 23. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>FTP Ports</td>
<td>The default is port 21. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>SNMP Ports</td>
<td>The default is port 161. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>HTTP Ports</td>
<td>The default is port 80. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>HTTPS Ports</td>
<td>The default is port 443. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>VMware Authentication Daemon Ports</td>
<td>The only supported port is 902. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>Mainframe Host Server Ports</td>
<td>The default is port 3940. Enter any custom ports to scan in a comma separated list in the Change To column.</td>
</tr>
<tr>
<td>Valid Port States</td>
<td>When nmap runs port scans, it returns a result of open, closed or filtered. Using the check boxes you can choose which states are valid to investigate further.                                                                                                   * open/filtered: discover a device that should be accessible but isn't. It might be open, or filtered.</td>
</tr>
<tr>
<td></td>
<td>* filtered: this port is open but you still cannot connect to it. It must be filtered. A port for which a result of open is returned is always considered valid.</td>
</tr>
<tr>
<td>Check port 135 before using Windows access methods</td>
<td>Port 135 is usually open on Windows machines. Selecting Yes for this option means that nmap checks whether port 135 is open before a Windows proxy is used to discover an IP device. This is the default. You should select No in firewalled environments where a ping may be filtered by a firewall, but the Windows proxy may be able to connect to the target (for example, it is part of the same Workgroup).</td>
</tr>
</tbody>
</table>

Device identification settings
This section contains settings related to the methods that discovery uses to identify devices.
### Use Last Login Method
Discovery will use the discovery method recorded as having been used successfully for an IP address.

### Use SNMP SysDescr to Identify OS
Discovery will attempt to query the host's SNMP service for the "SysDescr" value to determine the operating system.

### Always try public SNMP community
Discovery will attempt to use the public SNMP community to query the host's SNMP service if no credential is available for that host. In this case, only device classification is possible.

### Use Host Server to Identify Mainframes
Discovery will attempt to connect to the host server port to determine whether the discovery target is a mainframe computer.

### Use Telnet Banner to Identify Mainframes
Discovery will telnet to a host and use the telnet "welcome" banner to determine host and operating system information.

### Use HTTP(S) HEAD Request to Identify OS
Discovery will attempt to connect to port 80 or 443 of the host and perform an HTTP or HTTPS HEAD request to determine the host and operating system.

### Use FTP Banner to Identify OS
Discovery will start an FTP session with the host and use the FTP "welcome" banner to determine host and operating system information.

### Use vSphere API to Identify OS
Discovery will make a TCP connection to examine the header and ensure that the VMware authentication daemon is really on port 902 (or the specified port). When confirmed discovery makes a webservice request. This requires an open VMware Authentication Daemon and HTTPS port, and a valid vSphere credential.

### Use IP Fingerprinting to detect OS
This option controls whether or not discovery will use IP fingerprinting to determine the operating system, if the previous methods have been unsuccessful. The network ports scanned during this phase of discovery can be configured. See Setting Up Ports For OS Fingerprinting.

### Use Open Ports to Identify OS
This option controls whether or not open ports are used to identify the operating system.

---

### Session settings
This section contains settings related to the way in which discovery uses sessions to login and run commands.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Line Delay</td>
<td>A delay of 10 ms is introduced between each line sent by Discovery. This avoids problems where remote shells are unable to cope with rapid command sequences. Select one of the following from the list: • 1, 2, 5, 10 (the default), 15, 20, 25, 50, 100 milliseconds.</td>
</tr>
</tbody>
</table>
### Field Name | Details
--- | ---
Session Login Timeout | The length of time for the discovery script to wait for a login prompt. If this is exceeded the attempt is abandoned.  
• Use default timeout.  
• 10, 20, 30, 60, 90, 120, or 180 seconds.

Authorised Prompt | Certain systems require an authorization step after logging in. At the command line you are asked something like "Enter session details:". The required response is usually a user name, and some other information.  
In the Authorised Prompt field, enter the text of the prompt.

Authorised Response | Where an Authorised Prompt has been entered, you must enter the expected response (that you would enter at the command line) in the Authorised Response field.

### Scanning settings

This section contains settings related to any scanning that discovery undertakes.

| Field Name | Details |
--- | ---
Authorized Scanning Levels | Select the scanning levels that you want to permit. Choose one or more levels from the following:  
• **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type. In particular, it will execute the getDeviceInfo discovery script on each platform - see Managing the discovery platform scripts for more information about platform scripts.  
• **Full Discovery**: Retrieve all the default information for hosts, and complete full inference.  
Scanning levels are described in #Scanning and Data Processing Levels.

Default Scan Level | Select the default scan level for this appliance from the list. The choices available are those selected in the Authorized Scanning Levels row above.

Ping hosts before scanning | If this option is disabled, then all hosts will be discovered, but discovery of empty IP ranges will be slower. The default is to allow discovery to ping the host first.  
If you enable this option, discovery will ping hosts before scanning. Discovery will be more rapid on empty IP ranges though hosts may be missed if there are firewalls configured to reject pings. In this situation you should specify IP ranges behind firewalls that you do not want to ping. See the Exclude ranges from ping option below.  
Note that this option only affects scanning of networks other than the one on which the appliance is physically located.  
If you are using ICMP filtering, you should set this option to No.  
See note on #Order of Operations below.

Use TCP ACK ping before scanning | Ping addresses with TCP ACK packets to determine which hosts are actually up. You should use this option when scanning networks that do not permit ping packets. You can specify multiple ports in a comma-separated list.  
This option is only available if the ping hosts before scanning option is set to Yes.  
• See note on #Order of Operations below.

Use TCP SYN ping before scanning | Ping addresses with TCP SYN packets to determine which hosts are actually up. You should use this option when scanning networks that do not permit ping packets. You can specify multiple ports in a comma-separated list.  
This option is only available if the ping hosts before scanning option is set to Yes.  
• Note that TCP SYN pings are likely to trigger IDS and firewall blocks as they are often regarded as ping floods.  
• Also see note on #Order of Operations below.

Exclude ranges from ping | |
**Configuration guide**

Enter a list of IP addresses or IP ranges that you do not want to ping. For example, you may want to scan IPs which are behind a firewall that blocks ICMP packets. If BMC Atrium Discovery pings an IP address and receives no response, it makes no further attempt to scan that IP address. Excluding a range from pinging enables you to scan IPs behind such firewalls. Note this option only affects scanning of networks other than the one on which the appliance is physically located.

**Scan retries**

Number of retries to be attempted on each host. The system will only retry for machines on which the operating system cannot be determined. The Scan retries and Default OS options work together in sequence to help locate host machines.

**Scan timeout**

Timeout (in minutes) that applies when BMC Atrium Discovery uses nmap to determine open ports or performs OS fingerprinting. It is not used to limit the time to scan devices. See also the [credential timeout](#) for the sessions.

**Minimum time before end of window to avoid starting new scheduled discovery operations**

The scan of a single IP address may take some time to complete. If it is started too close to the end of a Discovery window, it may not complete before the end of the window. To prevent this you can specify a period in which discovery operations (scans of new IP addresses, or new discovery calls to IP addresses currently being scanned) will not be started. The default is 30 minutes. That is, no discovery operations will be started within 30 minutes of the end of a discovery window. Select the period from the following values in the list:

- 5, 10, 15, 20, 25, 30, 35, 40, and 45 minutes.

**Allow scans even if no window defined**

Enables you to permit scanning outside permitted discovery windows. The default is no. If you change this option you must restart the tideway service.

**Discover neighbor information when scanning network devices**

Cause discovery to retrieve MAC and port information from neighboring scanned network devices. The default is **Yes**. Only select **No** if you do not want to collect any [edge connectivity](#) information.

### SQL integration settings

This section contains settings related to SQL integrations.

**Field Name** | **Details**
--- | ---
Timeout to establish a connection | The timeout for establishing a connection to the database. Select the timeout period in seconds from the following values in the list:
- 5, 10, 30 (the default), 60, 90, 120, and 180.

Maximum connections held open | Specifies the number of connections to databases that can be held open after they would otherwise be closed. Higher values can reduce connection delays but will consume extra resources. The default is unlimited. If you change this option you must restart the tideway service. Select the number of connections from the following values in the list:
- 0, 10, 20, 30, 40, 50, and Unlimited.

Maximum time to hold an unused connection open | Specifies the maximum time to hold an unused database connection open. Higher values can reduce connection delays but will consume extra resources. The default is 2 minutes. If you change this option you must restart the tideway service. Select the timeout period in minutes from the following values in the list:
- 2, 4, 6, 8, and 10.
Mainframe discovery

This section contains settings related to mainframe discovery.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timeout to establish a connection</td>
<td>The timeout for establishing a connection to the database. Select the timeout period in seconds from the following values in the list: 30, 60, 90, 120 (the default), 180, and 300.</td>
</tr>
</tbody>
</table>

Other discovery settings

This section contains other discovery settings.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recording Mode</td>
<td>Record and playback modes are intended for diagnostic support and testing. Select the discovery mode from the list, it may be one of the following:  • Off: the normal type of discovery in which the appliance scans IP ranges on the network, runs scripts on targets, and uses Reasoning to processes the results. This is the default.  • Record: record mode is the same as Normal mode but in addition, the raw discovered data is stored on the appliance so that it can be used in Playback mode.  • Playback: in Playback mode, data that has been recorded in Record mode is used to replay discovery. In this mode, Discovery does not scan any targets on the network.</td>
</tr>
<tr>
<td>Maximum Concurrent Discovery Requests per ECA Engine</td>
<td>Specifies the maximum number of concurrent discovery requests permitted. The maximum value and available range of settings is calculated for optimum performance depending on the appliance. Values shown in the list depend upon the number of ECA engines. The base values in the list are:  • 30 (default), 60, 90, 120, or 150.  Values shown will be the base values multiplied by the number of ECA engines.  You must restart Discovery for any changes to take effect.  You should leave this setting at its default unless you are experiencing many discovery commands timing out. As a general rule, for more discovery requests permitted concurrently, you increase network traffic, and the absolute time for discovering a single host increases. However, with the interleaving of discovery processing, total throughput may be improved.</td>
</tr>
<tr>
<td>Maximum retries to process event</td>
<td>When Reasoning writes to the datastore and is unable to get a lock on a node it needs to update then it cannot perform the update. Reasoning will attempt to write the data up to a maximum number of times. Specify the number of retries from the list:  • 3 (the default), 4, 5, 6, 7, 8, or 9.</td>
</tr>
<tr>
<td>Minimum Windows Proxy Version</td>
<td>The minimum version of the Windows proxy that the appliance will use for Windows Discovery. You can enter a new minimum Windows proxy version in this field. Ensure that you do not include any whitespace in the version number. The version number of a Windows proxy corresponds to the version number of BMC Atrium Discovery that the Windows proxy was released with, for example, 8.1.  <strong>Note:</strong> You must stop scanning to change the minimum Windows proxy version or release.</td>
</tr>
<tr>
<td>Enable running of arbitrary commands</td>
<td>This option controls whether or not arbitrary commands can be run or not. Disabling this option will prevent many patterns retrieving information needed to build SIs and BAIs.</td>
</tr>
<tr>
<td>Enable Automatic Grouping</td>
<td><strong>Automatic Grouping</strong> is the automatic grouping of hosts into logical groups called Automatic Groups. This is primarily intended to help in baselining. By default it is enabled. Select this option to enable Automatic Grouping. Disabling Automatic Grouping may improve scanning performance.</td>
</tr>
<tr>
<td>Scanner File Polling Interval</td>
<td></td>
</tr>
</tbody>
</table>
### Field Name Details

**Scanner files** are used to simulate discovery of inaccessible hosts. Discovery polls for new scanner files periodically. Select the polling interval from the following values in the list:
- Every minute, Every hour, and Every day.
If you change this option you must restart the tideway service.

*When set to Every day, the polling time is at midnight UTC time. Daylight saving time is not considered.*

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
| Scanner files | are used to simulate discovery of inaccessible hosts. Discovery polls for new scanner files periodically. Select the polling interval from the following values in the list:  
- Every minute, Every hour, and Every day.  
If you change this option you must restart the tideway service. |

### Scanning and data processing levels

The Discovery Engine and the Reasoning Engine, collectively the discovery process, cooperate to:

- scan selected ranges
- process the data
- create a detailed data model

The data model defines all discovered objects and the relationships between them and is defined in the system Taxonomy.

The processing that the discovery process uses to create this complex, detailed, and interrelated data model is considerable. You can control the level of processing used, and consequently the accuracy, complexity, and detail in the data model. This gives performance benefits at a cost of model accuracy. You may find that reducing the level of processing used speeds rollout of BMC Atrium Discovery throughout your organization.

The following levels are available:

- **Sweep Scan**: This will do a sweep scan, trying to determine what is at each endpoint in the scan range. It will attempt to login to a device to determine the device type.
- **Full Discovery**: Retrieve all the default information for hosts, and complete full inference.

### Order of operations

Where selected, these groups of operations are carried out in the following order:

- Ping hosts before scanning
- Use TCP ACK "ping" before scanning
- Use TCP SYN "ping" before scanning
- TCP ports to use for initial scan
- UDP ports to use for initial scan
- Use IP Fingerprinting to Identify OS

### TCP and UDP ports to use for initial scan

The initial port scan is an important part of discovery. If you remove a port from the initial port scan, that port is effectively removed from discovery. For example, if you remove port 22, you will effectively disable ssh access.
The Use Last Login settings override any settings made in ports for use for initial scan. For example, if you disable port 23 using this feature, but a host has previously been discovered using telnet, this host will still be discovered using telnet as it is listed as the last login for that host.

## Masking sensitive data

The View Object page of a Discovered Process shows the command used to start the process. In some cases, a user name and password, or some other sensitive data is shown in clear text. You can also view the contents of a discovered file, and in some cases these too can contain passwords or other sensitive data. You can prevent this using Sensitive data filters.

Sensitive data filters for processes only mask information from the discovered process or file; not from, for example, package names.

A sensitive data filter is a regular expression to define data that you do not want displayed. When matched, the sensitive portion of the data is hashed using MD5. The hashed data can be compared with earlier versions to determine whether it has changed, while the actual data remains hidden from users.

### Managing Sensitive Data Filters

1. From the Discovery section of the Administration tab, select Sensitive Data Filters. The Sensitive Data Filters window is displayed with the **Processes** tab visible.

   Shows the screen in which you can enter regular expressions to match and hide sensitive data like passwords.

2. To view or edit filters for files, click the **Files** tab.

3. To edit an existing filter, click **Edit**.

4. To delete an existing filter, click **Delete**.

5. To add a new filter, click **Add ...**. A new field is added into which you can enter a regular expression.

6. To create the filter, click **Apply**.

To reorder sensitive data filters, click the up or down arrow in the ordering column for the filter you want to move. You can also move a filter to the top or bottom of the list using the top or bottom arrow buttons.

### Creating a Sensitive Data Filter

The regular expression will usually match more than just the sensitive data, including for instance an identifying argument name like "-password". The portion of data to be hashed must be enclosed in brackets to form a regular expression group. Portions of the regular expression not enclosed in the brackets will be unmodified.
1. The following command has the "--password" in clear text. The regular expression needs to use "--password" to locate the data, and define how much to mask around it.

   ```bash
   ./pfg_serv -h -Hj -g lob -l full --user gussie --password finknottle --dominion emea
   ```

2. This regular expression adds "\S+" to identify a sequence of one or more non whitespace characters, making a regular expression of "--password \S+". Brackets are then added to define the portion that requires masking, making "--password (\S+)".

3. After rediscovery, the new process node will have the password portion replaced with an md5 hash.

   ```bash
   ./pfg_serv -h -Hj -g lob -l full --user gussie
               --password 4343ab718997a9570ab20c0c1b5e18ad --dominion emea
   ```

4. For more resilience against extra white space the single space in the regular expression should be replaced with \s+, which matches any whitespace character making "--password\s+(\S+)" which is the form that most sensitive data filters would take.

**Notes on Sensitive Data Filters**

1. When writing regular expressions for sensitive data filters, you should ensure that it does not match too much of the command. If the filter masks some of the command that a pattern uses to identify a piece of running software, that pattern will then be unable to identify the software. See [Writing efficient regular expressions](#) for more information.

2. The filters are not applied to the inferred data model until you perform a discovery run. Sensitive data discovered before applying a filter will remain in the history and DDD until it is aged.

3. If applied to files, the files must remain valid. For example, if applied to an XML file, the XML must remain valid otherwise Xpath processing will not work.

**Setting up ports for OS fingerprinting**

BMC Atrium Discovery maintains a list of the port numbers that it interrogates. These ports are only scanned if the "Use IP Fingerprinting to Identify OS" option is enabled. See [Configuring discovery](#) for more information on this option.

If you want to set up any additional ports, for example if you use a non-standard port number, you need to enter this here.
To set up port settings

1. You will find the Port Scanning page by navigating to the Discovery Configuration page, contained in the Discovery section of the Administration tab. Next to the Use IP Fingerprinting to Identify OS option you will find the Configure Port Scanning link.

2. The Port Scanning page is displayed.
   Any currently configured ports are listed.

3. To change any of the Port values, click Lock for Editing. This ensures no other users can access the settings while you are editing.

4. Edit the port settings:
   - To create a new port value, click Add. An additional entry row is displayed at the end of the table.
   - To amend an existing value, click Edit for that entry.
   - To remove an entry, click Delete.

5. Set up the values as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Port number to be used.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of application.</td>
</tr>
<tr>
<td>Description</td>
<td>Free-text description of the application.</td>
</tr>
<tr>
<td>TCP Enabled</td>
<td>Select this checkbox if TCP uses this port assignment.</td>
</tr>
<tr>
<td>UDP Enabled</td>
<td>Select this checkbox if UDP uses this port assignment.</td>
</tr>
<tr>
<td>Reason</td>
<td>Complete this if a non-standard port has been used.</td>
</tr>
</tbody>
</table>

6. Click OK to save the new or changed details.

7. Click Apply to remove the lock and allow other users to edit the settings. If you click Cancel at this point, any changes you have made are discarded.

Managing the discovery platform scripts

The discovery system runs various scripts through the login session to obtain information from the host systems. From the BMC Atrium Discovery user interface, you can:

- View the scripts
- Amend scripts (edit script parameters, or enable or disable scripts)

However, the BMC Atrium Discovery user interface does not enable you to add new scripts.

Where this page refers to "default scripts", it refers to the discovery scripts that were shipped with the release. For example, in a version 8.2.03 appliance, the default scripts are those that shipped with 8.2.03. If you upgrade the appliance to version 8.3, the default scripts are those that shipped with version 8.3.
If you have just upgraded your installation and have not updated the discovery scripts, you can use the Discovery Platforms page to view the script differences and choose to upgrade to the current version by clicking Reset to Default. This enables you, post-upgrade, to view the script differences and choose to upgrade to the current version by clicking **Reset to Default**.

**Viewing the existing scripts**

To view existing scripts, perform the following:

1. From the Discovery section of the Administration tab, select **Platforms**.
   
   The **Discovery Platforms** page is displayed.
2. The **Discovery Platforms** page lists the categories for which discovery commands are provided.
   
   The available categories are:
   - Windows Discovery
   - UNIX, Linux and Related Discovery
   - Mainframe Discovery
   - SNMP Supported Platforms
3. Each category displays headers which link to pages containing details of discovery methods used.

Some additional information associated with a header might be displayed as a tool tip.

The following table summarizes the available discovery methods in these pages:

<table>
<thead>
<tr>
<th>Category</th>
<th>Discovery method</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows discovery</strong></td>
<td>The discovery methods used are WMI, RemQuery, Shell Scripts, and SNMP.</td>
</tr>
<tr>
<td></td>
<td>Windows discovery uses WMI and RemQuery as the primary method of discovery. Even though two different techniques are used as the primary method of discovery, it is considered to be a single session.</td>
</tr>
<tr>
<td></td>
<td>If WMI and RemQuery access fails to establish the initial session, Windows discovery attempts an interactive login (ssh or telnet) and running shell scripts and SNMP in the given order and uses the first one with which the initial session is established.</td>
</tr>
<tr>
<td></td>
<td>Once an initial session is established, Discovery does not attempt another session (for example, if WMI and RemQuery establishes the initial session and even if some scripts fail or commands are not successfully executed, Discovery does not attempt another session with interactive login and shell scripts).</td>
</tr>
<tr>
<td><strong>UNIX, Linux &amp; Related Discovery</strong></td>
<td>The discovery methods used are Shell Scripts and SNMP. For VMware ESX and ESXi platforms, vSphere API calls are used.</td>
</tr>
<tr>
<td></td>
<td>UNIX, Linux and related discovery uses an interactive login (ssh, telnet, or rlogin) and running shell scripts as the primary method of discovery (in case of VMware ESX and ESXi platforms, vSphere API calls are used as the primary method of discovery).</td>
</tr>
<tr>
<td></td>
<td>If the primary method of discovery fails to establish the initial session, Discovery attempts SNMP.</td>
</tr>
<tr>
<td></td>
<td>Once an initial session is established, Discovery does not attempt another session (for example, if interactive login and running shell scripts establish the initial session and even if some scripts fail or commands are not successfully executed, Discovery does not attempt another session with SNMP).</td>
</tr>
<tr>
<td><strong>Mainframe</strong></td>
<td>Discovery uses the MainView Host Server to obtain mainframe information.</td>
</tr>
</tbody>
</table>
4. Where the discovery scripts have been changed from the default, a red change bar is shown to the left of the platform name.

5. To manage the changed scripts in the UNIX, Linux and Related Discovery section, you can use the following controls:
   - **Reset All**: click this to reset all scripts to the default.
   - **View Script Differences**: this link opens a page showing a list of changed discovery methods, sorted by platform.

   ![Change Bar Example](image)

   Click the discovery method header to reveal the detailed view of the differences between the default method and the current method:

   ![Differences Example](image)

6. Click the operating system link whose commands you want to edit. You cannot edit the SNMP methods, you can only view them.

**Amending the existing scripts**

You can only edit and enable or disable selected shell scripts from the Discovery Platforms page. You can only view and not amend the following methods:

- WMI
- RemQuery
- SNMP
- vSphere
- Mainframe

To amend existing scripts, perform the following:

1. On the Discovery Platforms page, click the operating system link whose commands you want to edit.
2. Click on the Shell Scripts tab.

   The commands for the operating system are displayed. The following table describes the fields in this page:
<table>
<thead>
<tr>
<th>Field name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download host script</td>
<td>To download the entire script, click this link.</td>
</tr>
<tr>
<td>Path</td>
<td>To edit the command path which is set when a shell is opened on the target, click the corresponding <strong>Edit</strong> link. Just the command path displayed is set, it is not added to any existing path in the user environment.</td>
</tr>
<tr>
<td>Show All Scripts</td>
<td>To display a view only version of all the scripts, click this link.</td>
</tr>
<tr>
<td>Method</td>
<td>Displays the discovery method used. * indicates methods that will successfully create a host.</td>
</tr>
<tr>
<td>Script</td>
<td>To display a view only version of a script, click this link for the corresponding script. Some scripts might be marked as <strong>Privileges</strong>. This means that a normal login does not have sufficient access rights to get all of the information required. In this case, the root, or another user with higher access rights is used.</td>
</tr>
<tr>
<td>Enabled or Disabled</td>
<td>Displays if the script is selected to be enabled or not.</td>
</tr>
</tbody>
</table>
| Actions          | In the Actions column, the following options are available:  
|                  | - **Edit**: To edit the script, click this link. You can edit the discovery script, notes, and enable or disable the script.       |
|                  | - **Disable** or **Enable**: To change the enable and disable status of a script, click this link.                                 |
|                  | - **Download**: To download a copy of the script, click this link. You can then edit it in a text editor and save it locally.    |
|                  | - **Upload**: To upload a script to replace the existing one, click this link. Where you edit or replace an existing script, a red change bar shows that the script has been changed and an additional **Reset To Default** link is displayed. Click this link to reset the script to the default. |

⚠️ **Maximum Line Length**

The maximum line length of an interactive script is OS and shell dependent, and exceeding such a limit will cause the commands to fail. Ensuring that all lines in discovery scripts contain fewer than 128 characters will prevent this occurring.

3. **Click Apply** to save the changes.

**Additional discovery**

In addition to the standard discovery commands described above, additional discovery methods can be called by patterns. See **manual pattern execution** and **DiscoveryAccess page**.

Methods such as the following are used:
- `getFileInfo` – used where a pattern uses the `discovery.fileGet` to return a file. The result is stored in a `DiscoveredFile` node.
- `getFileMetadata` – used where a pattern uses the `discovery.fileInfo` to return the metadata on a file. The result is stored in a `DiscoveredFile` node with no `content` attribute.
- `runCommand` – used where a pattern uses the `discovery.runCommand` function to run a command on a host during its execution. The result is stored in a `DiscoveredCommandResult` node.
- `getDirectoryListing` – used where a pattern uses the `discovery.listDirectory` function to return a list of the directory contents. Returns a list of `DiscoveredDirectoryEntry` nodes.

Returning command exit status data

The commands that Discovery runs on UNIX hosts are all standard UNIX commands, and can be viewed through the UI. When Discovery runs these commands they return an exit status code. Discovery provides the ability to record exit status codes and output to stderr where commands fail. Success is not recorded.

You should bear in mind standard scripting techniques when editing these commands. For example, some Discovery commands use pipelines, and may need to be modified so as not to mask the desired exit status code.

Exit status codes are operating system, operating system version, and command dependent. Consult your operating system documentation for information on exit status codes and their meanings.

Recording the exit status

To record the exit status you need to prefix the discovery commands with `tw_capture`. The first parameter is a name used to identify the captured information. The second parameter is the command to run, and any further parameters are passed to the command. For example:

```
tw_capture fileinfo_foo ls -ld /usr/bin/foo
```

⚠️ In order to be able to capture output using `tw_capture`, `/tmp` on the target host needs to be writable by the discovering account.

You can record an exit status from commands used in a pipeline, for example:

```
tw_capture foo dpkg -l '*' | egrep '^ii '
```
It can also be used in backticks, for example when running a command and assigning the result to a shell variable:

```bash
dns_domain=`tw_capture hostname -d | sed -e 's/(none)//'`
```

The following screen shows two example `tw_capture` commands, one which will succeed, and one which will fail. These have been added to the start of the `getDeviceInfo` method:

This screen illustrates a typographical error in one script that will prevent it from executing correctly.

**Viewing the exit status**

Once you have added the `tw_capture` commands, and discovered a host causing the method to be run, you can see any script failures by viewing the appropriate method link on the Discovery Access page.

To view the exit status:

1. From the Discovery Recent Runs tab, click the discovery run which you used to scan the host.
2. Click **DiscoveryAccess**.  
   If it is a link to a single DiscoveryAccess, then that DiscoveryAccess page is shown. If there are multiple DiscoveryAccesses, then a list page is displayed.
3. Click the method link for the method which you edited to add the return status.

**Using scanner files**

A scanner file is a plain text file that is used to simulate the discovery of a system that is unreachable, or one that you are not permitted to scan. You create a scanner file by running the standard discovery commands on a host and saving the output. Only the standard discovery commands are run on the host; information that is discovered by patterns is not available.
For Windows targets, the downloaded discovery commands do not run WMI queries, so some host data cannot be recovered. For more complete discovery, you should use the Standalone Windows scanning tool.

Process for using scanner files

The process for using scanner files is:

1. **Create a scanner file.**
   a. Download the `.sh` or `.bat` file from the BMC Atrium Discovery user interface.
   b. Copy the file to the remote host.
   c. Run and capture the output to a file.

2. **Load the scanner file onto the appliance.**
   a. Using the SCP utility, upload the results file to the appliance as the upload user.

Creating a scanner file

To create a scanner file:

1. From the Discovery section of the Administration tab, select **Platforms**.
2. Click the operating system link corresponding to the host for which you are creating the scanning file. For Windows hosts, click **Shell Scripts** in the Windows Discovery section. The commands for the operating system are displayed. The following example illustrates creating a scanner file using the Linux operating system.

   ![Linux Discovery Interface](image)

   **This diagram illustrates a scanning file created for a Linux operating system.**

3. Click **Download host script** (named Linux.sh, in this example) and save the file to the local computer as an executable.

4. Copy the file to the remote host.
   In the following example, the SCP utility is used to copy the files between the local host `teabag` and the remote host `teaspoon`:
5. Log on to the remote host and run the script, piping the output into a text file:

```
tideway@teabag:$ scp linux.sh tideway@teaspoon:linux.sh
tideway@teaspoon's password: linux.sh                                      100% 19KB 18.9KB/s 00:00
tideway@teabag:$
```

```
tideway@teabag:$ ssh teaspoon
tideway@teaspoon's password: Linux teaspoon 2.6.18-6-686 #1 SMP Sat Dec 27 09:31:05 UTC 2008 i686 ...
tideway@teaspoon:$
tideway@teaspoon:$ ./linux.sh > teaspoon.txt
tideway@teaspoon:$ more teaspoon.txt
FORMAT Linux
--- START device_info
hostname: teaspoon
fqdn: teaspoon
dns_domain: tideway.com
domain:
o: Debian Linux lenny/sid
--- END device_info
--- START host_info
kernel: 2.6.25-2-amd64
num_logical_processors: 2
cores_per_processor: 2
...
tideway@teaspoon:$
```

6. Copy the output text file to your local host.

```
tideway@teaspoon:$
tideway@teaspoon:$ scp teaspoon.txt tideway@teabag:linux.txt
tideway@teabag's password: teaspoon.txt                                      100% 265KB 264.7KB/s 00:00
tideway@teaspoon:$
```

The output file is copied to your local host.
Loading the scanner file onto the appliance

After you have created and copied the output file to your local host, you can copy it to the appliance. In this example, the appliance is called appliance, and the local host is called teabag. When loading scanner files onto the appliance, use the upload user, because it has a home directory that is the default location for uploading scanner files, and it has limited access to the appliance. See The upload user for information on enabling this user.

1. Ensure the file has the group read permission set:

```bash
dtweed@teabag:~$ chmod 640 teaspoon.txt
dtweed@teabag:~$
```

2. Copy the output file to the appliance. In this example, the SCP utility is used:

```bash
dtweed@teabag:~$ scp -p teaspoon.txt upload@appliance:~/linux.teaspoon.txt
```

When you load a scanner file onto the appliance, its name must be unique; otherwise, it might get overwritten by another scanner file being uploaded at the same time. For this reason, it is helpful to use a naming scheme that enables you to correlate scanner files and created hosts. Do not use a name starting with . or ending with .ignore. If you do, that file will be ignored. File names are used only for internal purposes.

⚠️ Using scanner files with consolidating appliances

If you are using scanner files with consolidating appliances, upload the scanner files to the consolidating appliance, rather than to the scanning appliance. Doing so correctly identifies the hosts as "Read from scanner file", rather than as "Retrieved by scanning appliance".

After a scanner file is loaded, you can look at the results of the discovery and view the host, as shown in the following illustration.
This diagram illustrates the properties displayed for a scanned host.

On the DiscoveryAccess page, in the Data Source field of the Discovery Details section "Read from scanner file" is displayed. This is shown in the following illustration.

This diagram illustrates Read from scanner file displaying on the DiscoveryAccess page.

Considerations when using scanner files

BMC Atrium Discovery initiates a scan of the IP address automatically. You do not need to initiate a scan manually. However, depending on how you set the Scanner File Polling Interval option, it may take up to an hour after the file is copied to the appliance for the scan to initiate. Scanner files are read from the $TIDEWAY/var/scanner directory periodically based on this setting. For more information on setting this option, see Scanning settings.

When scanner files are used, BMC Atrium Discovery creates non-expiring pool data by creating a . no-expiry file in the pool data directory $TIDEWAY/var/pool/192/168/1/100/.no-expiry, where the IP address is 192.168.1.100). The pool data will always be used for each subsequent discovery and return identical results until the scanner file is updated, or until the pool data is deleted.
- Hosts discovered by scanner files never age.
- BMC Atrium Discovery does not handle overlapping IP ranges, which occur in rare cases. Using the Windows scanning tool might increase the likelihood of ranges overlapping; however, the tool enables you to select a specific IP to avoid one you have already selected. For more information, see Standalone Windows scanning tool.

Standalone Windows scanning tool

In certain applications, computer and server assets are located on systems that typically cannot be reached by the BMC Atrium Discovery appliance, either because of network security or because the systems are on an isolated network.

The standalone Windows scanning tool enables you to perform discovery on these standalone systems. It enables you to run BMC Atrium Discovery from a USB drive inserted into the target Windows host and to inventory all assets on that system. The tool gathers data from Windows computers that are not connected to a network, and creates scanner files with the discovered data.

The standalone Windows scanning tool compliments the equivalent UNIX scanner scripts.

This functionality does not permit interactive running of patterns to gather the full depth of data that a Windows proxy provides; however, it enables BMC Atrium Discovery to contain data about hosts that would otherwise be unreachable and to synchronize this information to BMC Atrium CMDB. After the tool is run on the target host, the collected data must be manually uploaded to the appliance.

Warning

The standalone Windows scanner can be used to manually collect a limited set of information from a Windows host. The scanner is designed to be used solely on isolated systems or networks. It is *not* equivalent to a Windows proxy, because it will only collect basic host, process and package information that can be obtained by WMI queries, not additional data such as NIC registry information (for NIC discovery).

Accessing and downloading the tool

The Windows scanning tool is a .zip archive file that can be extracted onto the target system or onto some form of removable storage (such as a USB drive). The .zip archive file contains everything you need to scan the Windows system; no connection to a BMC Atrium Discovery appliance is required.

To access and download the file:

1. From the Discovery tab, click **Tools**.
2. In the Standalone Windows Scanner area of the Discovery Tools page, click the Download link at the bottom of the page.

   ![Image of Download Link]

   This diagram illustrates where to download the standalone Windows scanning tool from the Discovery Tools page.

3. Extract the .zip file to a directory on a writable a USB flash drive or similar removable media.

Using the tool

The standalone Windows scanning tool runs as a portable console application directly from an external flash drive.

To use the tool:

1. Insert the USB flash drive into the host system and explore the contents.
2. If necessary, change the command options. (For example, it is recommended that you select the target IP address, if known, to avoid the possibility of overlapping IPs).
3. Double-click the `tw_windows_scanner.exe` file.

   A command window opens, and the tool begins collecting data.

   The following example output illustrates what informational messages the tool displays during data collection:

   ```
   U:> tw_windows_scanner
   Output file is results\192.168.1.1.scan
   Collecting Host Information ... DONE
   Collecting Interface Information ... DONE
   Collecting Process Information ... DONE
   Collecting Service Information ... DONE
   Collecting File System Information ... DONE
   Collecting Package Information ... DONE
   ```

Changing the command options

By default, the scan files are named based on the IP address of the Windows system (the lowest selected by the tool, after it ignores the localhost 127.0.0.1 address). The system will not overwrite existing scan files unless you change the options shown in the following table.
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--id XXX</td>
<td>Sets the name of the scan file to <code>results:XXX.scan</code>. Scanner files are automatically named based on the host's first listed IP address. If you do not set the file name using this option, you might inadvertently generate the same result file from two computers.</td>
</tr>
<tr>
<td>--target IPADDR</td>
<td>Sets the IP address to be scanned. For more information, see Changing the IP address to be scanned.</td>
</tr>
<tr>
<td>-x, --overwrite</td>
<td>Specifies to overwrite any existing scan file.</td>
</tr>
<tr>
<td>-q, --quiet</td>
<td>Specifies to not display informational messages</td>
</tr>
<tr>
<td>--wmi-timeout</td>
<td>Specifies to alter the WMI timeout (the default is 2 minutes)</td>
</tr>
</tbody>
</table>

**Changing the IP address to be scanned**

In certain cases, the IP address of the Windows system (the lowest selected by the tool, after it ignores the localhost 127.0.0.1 address) might not be correct (for example, a VPN connection). Although these occurrences are uncommon, the tool will display an error message and exit. To help prevent these occurrences, it might be necessary to explicitly specify the IP address you want to use. To do so, run the tool and use the `--target IPADDR` option to set the target system.

It is also possible to scan other systems using this option, as long as your user account has the required privileges (which are typically Administrator privileges). Setting the IP address to a specific target is especially useful for scanning an isolated subnet, because you would only need to insert the tool into one computer to collect data from them all.

**Uploading the data to the appliance**

After you have collected the data, upload it to the appliance. To do this, you use the SCP utility to transfer the files to the appliance as the `user`. For more information on uploading scanner files to an appliance, see Loading a scanner file onto the appliance.

After the data is uploaded, it is processed by BMC Atrium Discovery. For more information about scanner files, see Using scanner files.

**Adding privileged execution to commands**

BMC Atrium Discovery is shipped without any commands that use privileged execution. The following example illustrates how to add privileged execution to `ls/of` commands. You must to do the same for any command that you want to execute as a privileged user. The individual discovery scripts for each platform, `getDeviceInfo`, `getFileSystem`, and so on, use a privilege mechanism which is configured in the `initialise` script. You do not need to edit the individual scripts to escalate privileges, only the `initialise` script.

To configure execution of a command as a privileged user:
1. In the Discovery section of the Administration page, click **Platforms**.
2. Click the operating system link corresponding to the commands on which you want to add the privileged execution.
3. Click **Edit** in the Action column of the **initialise** method row.
   The edit window is shown containing the script.
4. Click in the edit window to enlarge it, as illustrated in the following screen.

   ![Edit Window Enlarged](image)

   **This screen illustrates clicking in the edit window to enlarge it.**
5. Use the find function in your browser to search for the PRIV section (search for PRIV_XXX to find the beginning of the PRIV section).
6. In the PRIV function (in this example PRIV_LSOF), add the command required (such as `sudo`, `pbrun`, or `dzdo`) to run the commands as a privileged user.
   For example:

   ```bash
   ...
   PRIV_LSOF() {
     sudo "$@
   }
   ...
   ```

   Alternatively, if you need to specify the path:

   ```bash
   ...
   PRIV_LSOF() {
     /usr/bin/sudo "$@
   }
   ...
   ```

7. Click **Apply** to apply the changes. The screen is refreshed and the initialise method is highlighted to show that it has changed from the default.
This screen illustrates the highlighting in the initialise method showing that it has been changed from the default.

8. Click **Show Differences** to show the differences between the default script and the current script.

This screen illustrates the view showing the differences between the default script and the one just edited.

The $@ represents the command that BMC Atrium Discovery issues. Adding `sudo` (or similar privileged command) tells it how to escalate the privilege for that command. Now when a script needs to call lsof, it calls the PRIV_LSOF() command with the full command it needs to run, which then runs lsof with the correct privilege.

If the path is specified, it will affect all discovery commands that use that function. The privileged command may not always be at the same place on all discovery targets.

If the path is not specified, the privileged command will be found with the path of the user profile and the BMC Atrium Discovery path environment variable. You can check the path environment variable as it is displayed at the top of the Platforms page.

You must add a privileged execution method to whichever commands you require in order to gain the fullest possible discovery. The available commands, their impact on discovery and the platforms they are available on described on the Privileged commands page.

**Password prompt in privileged command execution**

Where the sudo (or similar privileged command) configuration on a target host requires the user password to be entered at the command line, discovery will resend the credential already used to log on to the target.
In such situation however, if the default sudo "Password:" prompt has been customized on target systems (e.g. by setting the SUDO_PROMPT environment variable, or specifying a passprompt entry in the target's sudoers file), then the initialize script for the corresponding platform would need to be edited to specify:

```bash
...
SUDO_PROMPT="Password:"
export SUDO_PROMPT
...
```

**Privileged commands**

This page describes the available privileged commands, their impact on discovery, and the platforms on which they are available. By default, each command is left unprivileged (for example, `PRIV_LSOF`/`ls@`). The user or administrator must modify the script to insert the relevant command to allow discovery to run the privileged commands. Examples are provided in adding privileged execution to commands.

**AIX**

PRIV_CAT: The `cat` command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_LSOF: The `ls@` command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_LSLPP: The `lslpp` command requires superuser privileges to list all installed packages.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.

**FreeBSD**

PRIV_CAT: The `cat` command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_LSOF: The `ls@` command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_DMIDECODE: The `dmidecode` command requires superuser privileges to read data from the system BIOS.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.
HPUX

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_LANADMIN: The lanadmin command requires superuser privileges to display any interface speed and negotiation settings.
PRIV_SWLIST: The swlist command requires superuser privileges to list all installed packages.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.

IRIX

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.

Linux

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.
PRIV_DMIDECODE: The dmidecode command requires superuser privileges to read data from the system BIOS.
PRIV_HWINFO: The hwinfo command requires superuser privileges to read data from the system BIOS.
PRIV_MIITOOL: The mii-tool command requires superuser privileges to display any interface speed and negotiation settings.
PRIV_ETHTOOL: The ethtool command requires superuser privileges to display any interface speed and negotiation settings.
PRIV_NETSTAT: The netstat command requires superuser privileges to display process identifiers (PIDs) for ports opened by processes not running as the current user.
PRIV_LPUTIL: The lputil command requires superuser privileges to display any HBA information.
PRIV_HBACMD: The hbacmd command requires superuser privileges to display any HBA information.
PRIV_XE: The xe command command requires superuser privileges to report CPU information on Xen platforms.
PRIV_ESXCFG: The esxcfg-info command requires superuser privileges to report hardware information on a VMWare ESX controller.

Mac OS X
PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.

NetBSD
PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.
PRIV_DMIDECODE: The dmidecode command requires superuser privileges to read data from the system BIOS.

OpenBSD
PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.
PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.
PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_TEST: This function supports privilege testing of attributes of files.
PRIV_LS: This function supports privilege listing of files and directories.
PRIV_DMIDECODE: The dmidecode command requires superuser privileges to read data from the system BIOS.

OpenVMS
Not applicable to this platform. The Normal privilege category is sufficient to run the commands in the discovery script.
POWER HMC

Not applicable to this platform.

Solaris

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.

PRIV_EMLXADM: The emlxadm command requires superuser privileges to display any HBA information.

PRIV_FCINFO: The fcinfo command requires superuser privileges to display any HBA information.

PRIV_DMIDECODE: The dmidecode command requires superuser privileges to read data from the system BIOS on Solaris X86 platforms only.

PRIV_IFCONFIG: The ifconfig command requires superuser privileges to display the MAC address of each # interface.

PRIV_NDD: The ndd command requires superuser privileges to display any interface speed and negotiation settings.

PRIV_PS: The /usr/ucb/ps command requires superuser privileges to display full command line information (without this, command lines will be limited to 80 characters). This affects Solaris 10 and Solaris 8 & 9 with certain patches.

PRIV_LPUTIL: The lputil command requires superuser privileges to display any HBA information.

PRIV_HBACMD: The hbacmd command requires superuser privileges to display any HBA information.

PRIV_PFILES: The pfiles command requires superuser privileges to display open port information for processes not running as the current user.

Tru64

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_SETLD: The setld command requires superuser privileges to display information on installed packages.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.
UnixWare

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.

VMware ESX

This refers to ssh discovery rather than discovery via the vSphere API.

PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.

PRIV_CAT: The cat command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.

PRIV_DMI: The dmidecode command requires superuser privileges to read data from the system BIOS.

PRIV_HWINFO: The hwinfo command requires superuser privileges to read data from the system BIOS.

PRIV_MII: The mii-tool command requires superuser privileges to display any interface speed and negotiation settings.

PRIV_ETH: The ethtool command requires superuser privileges to display any interface speed and negotiation settings.

PRIV_NETSTAT: The netstat command requires superuser privileges to display process identifiers (PIDs) for ports opened by processes not running as the current user.

PRIV_LPUTIL: The lputil command requires superuser privileges to display any HBA information.

PRIV_HBACMD: The hbacmd command requires superuser privileges to display any HBA information.

PRIV_XE: The Xen xe command requires superuser privileges.

PRIV_ESXCFG: The esxcfg-info command requires superuser privileges.

VMware ESXi

This refers to ssh discovery rather than discovery via the vSphere API.

PRIV_LSOF: The lsof command requires superuser privileges to display information on processes other than those running as the current user.

PRIV_RUNCMD: This function supports running privileged commands from patterns.
PRIV_CAT: The `cat` command requires superuser privileges to display the contents of files not readable by the current user. For example, configuration files owned by the root user.

PRIV_TEST: This function supports privilege testing of attributes of files.

PRIV_LS: This function supports privilege listing of files and directories.

Extending discovery

This section details how to extend discovery coverage in BMC Atrium Discovery.

- Discovering mainframe computers
- Extended discovery of IBMi
- Extended discovery of Tomcat
- Extended discovery of WebSphere
- Extended discovery of WebLogic
- Integrating with BMC Atrium Orchestrator
- Power System discovery
- Discovering VMware ESX and ESXi hosts

Discovering mainframe computers

Mainframe computers are powerful computers that tend to be used by large organizations for critical bulk data processing. They are characterized by high reliability and security, strict backward compatibility with older software, and high utilization rates and very large data throughput.

See Viewing a mainframe for a description of how a mainframe is represented in BMC Atrium Discovery.

Configuring mainframe discovery

BMC Atrium Discovery undertakes mainframe discovery as part of a normal discovery scan. When discovery heuristics indicate a mainframe computer is on a particular IP address, then the methods unique to mainframe discovery are initiated. Mainframe discovery methods use an agent, the z/OS Discovery Agent, which is installed on the mainframe to collect information from a logical partition (LPAR).

1. **BMC Atrium Discovery for z/OS agent**

   BMC Atrium Discovery cannot natively discover z/OS systems and requires **BMC Atrium Discovery for z/OS** to be installed on the z/OS systems. This is a separately licensed product. Unless the support ID you use has been registered as licensed for this additional product then you may be unable to see the references linked to on this page. Contact your BMC sales representatives if you need to discuss this further.
Discovering all mainframes and LPARs

To discover all mainframes and LPARs, a BMC Discovery for z/OS agent must be installed on every LPAR. Where LPARs are connected through CAS to CAS communication (known as a CASPlex), then at least one MainView Explorer (host server) must be running on each CASPlex. You must then scan the IP addresses for each of the MainView Explorer instances.

Where LPARs are not connected through the CAS then a MainView Explorer (host server) instance must be running on each LPAR.

For information on installing and configuring the BMC Discovery for z/OS Agent, see the **BMC Discovery for z/OS Agent Installation Guide** available from the BMC support site.

Multiple CASPlexes on a single mainframe

There is a known limitation when there are multiple CASPlexes on a single mainframe. You can work around this by having a separate BMC Atrium Discovery instance to discover each CASPlex, or by changing the configuration so that all the LPARs on a given mainframe connect to a single CASPlex.

Required z/OS Discovery Agent version

Supported versions of the z/OS Discovery Agent are 1.6 and 1.7. Version 1.7 enables discovery of peer-to-peer and client-server relationships between SoftwareInstance nodes. To enable discovery by BMC Atrium Discovery, the z/OS Discovery Agent should be patched according to Technical Bulletin 172149. This Technical Bulletin is available from the BMC support site: Navigate to the page **BMC Discovery for z/OS** and choose the document "Describes BMC Atrium Discovery for z/OS License Add-On 1.6.00 requirements for BMC Atrium Discovery and Dependency Mapping 8.2.0"

**LPAR naming and SMF ID**

BMC Atrium Discovery sets the names of LPARs (the CAS system names) on the \_<discovery_context>_ attribute of the DiscoveredMainframe node. Sometimes, these names are not the same as the SMF ID of the LPAR which the agent returns to BMC Atrium Discovery. In such cases, there may be partial or no results for discovery methods other than \_getMainframeInfo_. The following Program Temporary Fixes (PTFs) address this issue:

- BMC Discovery for z/OS Agent 1.6: PTFs BPA1472 and BPA1473.
- BMC Discovery for z/OS Agent 1.7: PTFs BPA1479 and BPA1480.
Multiple mainframe discovery

In BMC Atrium Discovery version 8.2.01, only a single Mainframe node can be inferred, even if the DiscoveryAccess reports multiple Discovered Mainframes. Where multiple mainframes exist, discovery could sometimes infer other nodes (for example, MFPart and Sysplex nodes for multiple mainframes). These nodes could be created but not linked to a mainframe.

In version 8.3, multiple Mainframe nodes can be created in the inferred model. A scan of a BMC Discovery for z/OS agent results in only one inferred mainframe (the one on which the agent is running). The following illustration shows an example visualization.

This screen illustrates a visualization of multiple Mainframe nodes created from the inferred model.

A separate agent must be configured for each additional mainframe to be discovered, even if agents for the mainframes are communicating with each other and each agent is able to gather details of more than one mainframe.

The ability to infer multiple Mainframe nodes depends on the following PTF being applied on the BMC Discovery for z/OS agent:

- BPA1401

With BMC Discovery for z/OS Agent 1.6, if the PTF is not applied, BMC Atrium Discovery will function the same way as version 8.2.01, and be unable to infer multiple mainframes (the orphan nodes previously described, however, will no longer be created).

With BMC Discovery for z/OS Agent 1.7, there is no need for BPA1401. It has been superseded.

Optional Additional Discovery Tools

Some of the detail data that the z/OS Discovery Agent collects is dependent on additional MainView products being installed. The following table shows the MainView products used to obtain additional detail information. See the BMC Discovery for Z/OS documentation for further information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Script Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>getMainframeInfo</td>
<td>View Z</td>
</tr>
<tr>
<td>Method</td>
<td>Script Views</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>getMFCPart *</td>
<td>View Z</td>
</tr>
<tr>
<td>getApplication</td>
<td>Views 49Z, 4HZ and 4WZ (requested as View 49HWZ) — Requires MainView for WebSphere, Application Server, and MainView Transaction Analyzer products to be installed.</td>
</tr>
<tr>
<td>getCouplingFacility</td>
<td>View Z</td>
</tr>
<tr>
<td>getDatabase</td>
<td>Views 1IZ and 1XZ (requested as View 1IXZ) — Requires MainView for DB2 and MainView for IMS products to be installed.</td>
</tr>
<tr>
<td>getDatabaseDetail</td>
<td>Views 1IJZ, 1ILZ and 1IKZ (requested as View 1JKLZ) — Requires MainView for DB2 product to be installed.</td>
</tr>
<tr>
<td>getDependency</td>
<td>View Z</td>
</tr>
<tr>
<td>getDiskDrive</td>
<td>View #</td>
</tr>
<tr>
<td>getMQDetail</td>
<td>Version 8.3 – Views 5UZ, 5SZ and 5NZ (requested as View 5USNZ) Version 8.3 SP2 – Views 5UZ, 5VZ and 5NZ (requested as View 5NUVZ) — Requires MainView for WebSphere MQ product to be installed.</td>
</tr>
<tr>
<td>getSoftware</td>
<td>Views 0Z, 1Z, 2Z, 3Z, 4Z, 5Z, 6Z and 7Z (requested as View 01234567Z)</td>
</tr>
<tr>
<td>getStorageSubsystem</td>
<td>View -</td>
</tr>
<tr>
<td>getSysplex</td>
<td>View Z</td>
</tr>
<tr>
<td>getTapeDrive</td>
<td>View -@</td>
</tr>
<tr>
<td>getTransaction</td>
<td>View 0YZ — Requires MainView for CICS and MainView for IMS products to be installed.</td>
</tr>
<tr>
<td>getTransactionProgram</td>
<td>Version 8.3 SP3 – View 0YZ — Requires MainView for CICS and MainView for IMS products to be installed.</td>
</tr>
</tbody>
</table>

*indicates methods that must succeed for a Mainframe to be created.

Though the DB2/IMS/MQ/CICS servers will be discovered, this detailed data will not be available in a z/OS Discovery Agent only install.

**Credentials**

To discover a mainframe computer you require a z/OS user ID and password pair that is also defined in RACF, ACF2, Top Secret, or other external security managers. You configure the credential in the Management Systems tab in the Discovery Credentials page.

1. From the Discovery home page, click **Credentials**.
2. Click **Management Systems**.
3. Click **Mainframe**.
4. Click **Add**.
5. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td></td>
</tr>
</tbody>
</table>
5. **Table:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The IP range for which this credential will be used. This option can be one</td>
</tr>
<tr>
<td></td>
<td>of the following:</td>
</tr>
<tr>
<td></td>
<td>• an IP address (10.10.10.3)</td>
</tr>
<tr>
<td></td>
<td>• a range specification (10.10.10.* or 10.10.1-5.* or 10.10.10.0/24)</td>
</tr>
<tr>
<td></td>
<td>• a regular expression matching an IP address (.* or 10.10.10.(23</td>
</tr>
<tr>
<td>Username</td>
<td>The z/OS username with which to log in to the mainframe computer.</td>
</tr>
<tr>
<td>Password</td>
<td>The password corresponding to the username above.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a free text description of the credential.</td>
</tr>
<tr>
<td>Custom Mainframe Host Server Port</td>
<td>The port to use to connect to the mainframe. By default this is 3940. To use a different port, select the Enable custom mainview port? checkbox and choose a port number from the list. The list is populated with port numbers specified on the Discovery Configuration page.</td>
</tr>
</tbody>
</table>

6. To save the details, click **Apply**.

### Testing mainframe credentials

**Recommendation**

You should confirm that the BMC Discovery for z/OS Agent is installed and functioning correctly with the credential testing tool before attempting discovery of the mainframe as the test includes a number of diagnostics. Problems with configuration are much simpler to resolve using this approach.

To test an existing mainframe credential:

1. From the mainframe credential list, select **Actions => Test**.
2. Enter the IP address for which you want to test credentials.
3. Click **Test**.
   
   The *Management System Credentials* page is displayed showing the test in progress.
4. When the test completes, the page is refreshed with the result.
   
   You are shown whether the test ultimately resulted in a success or a failure. By clicking through the state link you can view the results of the credential test in more detail.
This screen illustrates how to view more detailed results of the credential test.

The credential test result page shows the discovery methods enabled in BMC Atrium Discovery, whether corresponding views are detected in the Discovery for z/OS agent, and the z/OS agent version.

For information on configuring security for the BMC Discovery for z/OS Agent, see the *BMC Discovery for z/OS Agent Installation Guide*.

**Enabling additional mainframe methods**

You can view the methods for mainframe discovery by clicking Mainframe Discovery in the Discovery Platforms page. The following mainframe methods are disabled by default as they are not required for a basic discovery:

- `getDiskDrive`
- `getTapeDrive`
- `getTransactionProgram` – *(introduced in BMC Atrium Discovery 8.3 SP3)*

**Enabling the remaining mainframe discovery methods**

To enable the remaining discovery methods:

1. From the Discovery section of the Administration tab, select **Platforms**.
2. Select **Mainframe**.
3. Select the Enable link in the following rows:
   - `getDiskDrive` *(see note below)*
   - `getTapeDrive`
   - `getTransactionProgram`
4. From the Discovery tab, select **Pattern Management**.
5. Select **Pattern Templates**.
6. For the `getDiskDrive` and `getTapeDrive` methods, select the `template_mainframe_storage` template.
   For the `getTransactionProgram` method, select the `template_mainframe_transaction` template.
7. Edit the patterns according to the instructions contained in the comments. You need to add a single trigger for each pattern contained in the template. See Pattern Management for more information on using pattern templates.
8. If you do not see additional discovery data, ensure that you have uncommented the lines as instructed in the pattern.

⚠️ Using getDiskDrive, getTapeDrive, and getTransactionProgram with CMDB Synchronization

When enabling getDiskDrive, getTapeDrive, and getTransactionProgram in a system where CMDB synchronization is used, you should be aware that these methods cause a large number of CIs to be created.

💡 You can view and download an example pattern module created from the templates here

Mainframe discovery and CMDB synchronization

For versions of BMC Atrium CMDB prior to 7.6.03, you must apply the mainframe extension, extension-703-800-Mainframe.zip to use CMDB synchronization with mainframe discovery. For complete instructions on setting up CMDB synchronization and applying BMC Atrium CMDB extensions, see Applying the ADDM Integration Extensions.

Mainframe template example

💡 File Download

The file can be downloaded from here

```plaintext
// This module contains example patterns based on the Mainframe pattern // templates.
//
// THIS IS FOR EXAMPLE USE ONLY
//

tpl 1.5 module Mainframe.Examples;

metadata
  origin := "ONLINE_DOCS";
end metadata;
```
from SupportingFiles.Mainframe.Support import MainframeModel 1.0;

pattern Mainframe_TapeDrive 1.0
'''
This pattern creates a Storage node for all TapeDrives.
'''

overview
  tags IBM, TapeDrive;
end overview;

triggers
  on dtd := DiscoveredTapeDrive;
end triggers;

body
  MainframeModel.createTapeStorage(dtd);
end body;
end pattern;

pattern Mainframe_DASD 1.0
'''
This pattern creates a Storage node for DASD Drives with a volume_id beginning with AL.
'''

overview
  tags IBM, DASD;
end overview;

triggers
  on dasd := DiscoveredDiskDrive where volume_id matches regex '^AL';
end triggers;

body
  MainframeModel.createDiskStorage(dasd);
end body;
end pattern;
pattern Mainframe_Transaction 1.0

This pattern creates a Detail node for all Transactions with a name beginning with CICSTRAN-C.

overview
tags IBM, Transaction;
end overview;

triggers
  on trn := DiscoveredTransaction where name matches regex '^CICSTRAN-C'
end triggers;

body
  MainframeModel.createTransaction(trn);
end body;
end pattern;

pattern Mainframe_MQ 1.0

This pattern creates a Detail node for all MQDetails with a name beginning with MQCHNL-.

overview
tags IBM, MQ;
end overview;

triggers
  on dmq := DiscoveredMQDetail where name matches regex '^MQCHNL-';
end triggers;

body
  MainframeModel.createMQDetail(dmq);
end body;
end pattern;
Extended discovery of IBMi

BMC Atrium Discovery enables SNMP discovery of IBMi (AS/400) targets. IBMi discovery consists of a UDP request from an ephemeral port on the appliance to port 161 on the target. The IBMi system responds using the same ephemeral port that initiated the request. BMC Atrium Discovery listens for a response on only that port.

Extended discovery of Tomcat

Apache Tomcat is an Application Server, otherwise known as a Web Container, developed by the Apache Software Foundation (ASF).

Tomcat implements the Java Servlet and the JavaServer Pages (JSP) specifications from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server, in addition it adds tools for configuration and management, which can also be configured by editing configuration files that are normally XML-formatted, and includes its own internal HTTP server.

Discovering Tomcat

BMC Atrium Discovery uses the ApacheFoundation.Tomcat.Tomcat pattern to discover the Tomcat instance, identify the home directory (catalina.home), identify the base directory (catalina.base), and determine the Tomcat version. The pattern extracts information from the Tomcat configuration files to create and populate a Tomcat SI and its attributes.

Extended Tomcat discovery is enabled by the activation of the Tomcat.ExtendedDiscovery.DiscoverTomcat pattern. This is activated by default in a new installation of BMC Atrium Discovery, but in an upgraded appliance, it must be activated manually. The Tomcat.ExtendedDiscovery.DiscoverTomcat pattern triggers on the creation or update of a Tomcat SI. The Tomcat.ExtendedDiscovery.DiscoverTomcat pattern is fully described in Configipedia.

Creation of a "JDBC Resource" Detail node triggers the CreateJDBCToDatabaseSI pattern which searches the BMC Atrium Discovery model for an SI representing that database. If the database SI is found the pattern creates relationships between the Tomcat Application Server SI and the nodes representing the database (see below). If the host that the database runs on has not been scanned, no further work is undertaken.

Creation of a "J2EEApplication" SoftwareComponent node does not trigger any further operations.

See the Tomcat documentation for additional information on Tomcat datasources.

Requirements for a full discovery

For a full discovery of Tomcat, the database or databases that it is using, and the relationships between them, you need the following credentials:

- Tomcat host login credentials
• Database host login credentials
• Database credentials

Tomcat Discovery results
The following screen shows a successfully scanned Apache Tomcat instance.

This screen illustrates a successfully scanned Apache Tomcat instance.
The attributes section of the Tomcat SI contains sections for Components, and Details.

• Components are the SoftwareComponent nodes representing J2EE applications on Tomcat.

• Details are detail nodes representing resources on Tomcat. These may be application specific or globally defined. They may be one of the following:
  • Custom Resources: a custom resource can be any kind of JavaBean declared as a resource.
  • User Database Resource: the default Tomcat user management database.
  • Java Mail Resources
  • JDBC Resources

Improvements over extended discovery using JMX
Previously, extended Tomcat discovery relied on JMX. This required configuration on Tomcat to ensure that JMX was configured to permit local and remote monitoring. Additionally, discovery using JMX only permitted discovery of globally defined resources; discovery using configuration files enables you to discover application specific resources too.

Extended discovery of WebSphere
IBM WebSphere is an Application Server, otherwise known as a Web Container, developed by IBM.
WebSphere implements the Java Servlet and the JavaServer Pages (JSP) specifications from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server, in addition it adds tools for configuration and management which can be configured through a web interface, and includes its own internal HTTP server.

**Discovering WebSphere**

BMC Atrium Discovery uses the `IBM.WebSphereApplicationServer` pattern to discover the WebSphere instance, identify the installation directory and determine the WebSphere version. The pattern extracts information from the WebSphere configuration files to create and populate a WebSphere SI and its attributes.

Extended WebSphere discovery is enabled by the activation of the `WebSphere.ExtendedDiscovery.DiscoverWebSphere` pattern. This is activated by default in a new installation of BMC Atrium Discovery, but in an upgraded appliance, it must be activated manually. The `WebSphere.ExtendedDiscovery.DiscoverWebSphere` pattern triggers on the creation or update of a WebSphere SI and performs a deep discovery of WebSphere instances via configuration files. It then parses the results to build a J2EE inferred model of its Applications and Resources.

Creation of a JDBC Resource Detail Node triggers the `CreateJDBCToDatabaseSI` pattern which searches the BMC Atrium Discovery model for an SI representing that database. If the database SI is found the pattern creates relationships between the WebSphere Application Server SI and the nodes representing the database (see below). If the host that the database runs on has not been scanned, no further work is undertaken.

Creation of a J2EEApplication Component node does not trigger any further operations.

The pattern attempts to:

- Get the application names from `serverindex.xml` and create the application SoftwareComponent node.
- Get the JNDI names of all the resources used by each application from the `<appname.ear>/WEB-INF/web.xml` file
- Read the `resources.xml` files for the server, node and cell and get database and mail resource info.
- Create the database and mail Detail nodes.
- Link each resource with the apps that use it.

The `WebSphere.ExtendedDiscovery.DiscoverWebSphere` pattern is fully described in Configipedia.
Attempting to discover a host server running version 2.5 of the optional MainView for WebSphere Application Server product results in the script failure "message View 49Z not available", and no WebSphere Discovered Application Components are created, preventing extended discovery.

Requirements for a full discovery

For a full discovery of WebSphere, the database or databases that it is using, and the relationships between them, you need the following credentials:

- WebSphere host login credentials
- Database host login credentials
- Database credentials

Database nodes and relationships

The relationships created depend on the way that the database type is represented. (For example, an Oracle database is represented by an SI whereas a MySQL database server is represented as an SI and the individual databases by Detail nodes with contained by relationships to the database server SI).

The use of detail nodes is not intended to be permanent.

WebSphere Discovery results

The following screen shows a successfully scanned IBM WebSphere instance.

This screen shows the SI representing a successfully scanned IBM WebSphere instance.

The attributes section of the WebSphere SI contains sections for Components, and Details.

- Components are J2EE applications on WebSphere.
• **Details** are resources on WebSphere. These may be application specific or globally defined. They may be one of the following:
  - User Database Resource: the default WebSphere user management database.
  - Java Mail Resources
  - JDBC Resources

### Extended discovery of WebLogic

Oracle WebLogic server is an enterprise-class J2EE application server. Oracle WebLogic server is part of the Oracle WebLogic platform and supports Oracle, IBM DB2, Microsoft SQL Server, MySQL, and other JDBC-compliant databases.

#### Discovering WebLogic

BMC Atrium Discovery uses the `BEA.WebLogicApplicationServer` pattern to discover a WebLogic application server instance and its version, to identify the JMX port, and most importantly for extended discovery, to determine whether JMX access is enabled.

Extended WebLogic discovery attempts to discover detailed information related to the WebLogic application server such as the J2EE domain, the J2EE applications running on the WebLogic application server, and the JDBC resources that the WebLogic application server is using. To do this, an additional pattern, `WebLogic.ExtendedDiscovery`, initially determines whether JMX access is enabled, and the JMX port has been identified. It then attempts to determine whether the WebLogic application server version is supported (see [Supported product versions](#)). If the WebLogic server version cannot be determined using a JMX query, then pattern execution ends.

If the JMX port has not been identified, the extended WebLogic discovery uses port 7001 by default. The `WebLogic.ExtendedDiscovery` pattern then queries the **WebLogic Administration Server’s** JMX monitoring agent for details about the J2EE applications, application servers, databases, database servers, mail servers, web servers, J2EE domain, and J2EE clusters. Information returned is stored in the J2EEApplication Component, J2EEDomain Collection, JDBCResource Detail, or JavaMailResource Detail nodes.

Creation of a JDBCResource Detail node triggers the `CreateJDBCToDatabaseSI` pattern that searches the BMC Atrium Discovery model for a software instance (SI) representing that database. If the database SI is found, the pattern creates relationships between the WebLogic Application Server SI and the nodes representing the database (see [Database nodes and relationships](#)). If the host that the database runs on has not been scanned, no further work is undertaken. The `WebLogic.ExtendedDiscovery.DiscoverWebLogic` pattern is fully described in [Configipedia](#).

Creation of a J2EEApplication Component node does not trigger any further operations.

If extended discovery fails, it falls back to using a host login and extracts information from the WebLogic configuration files to create and populate a WebLogic Application Server SI and its attributes.
Requirements for a full discovery

For a full discovery of WebLogic you need the following credentials:

- WebLogic host login credentials
- WebLogic application server login credentials (JMX) – see Configuring extended WebLogic discovery

Database nodes and relationships

The relationships are created based on the way that the database type is represented. (For example, an Oracle database is represented as an SI whereas a MySQL database server is represented as an SI and the individual databases by Detail nodes with contained by relationships to the database server SI).

The use of detail nodes is not intended to be permanent.

Supported product versions

The following WebLogic versions are supported:

- Oracle WebLogic Server 8.1
- Oracle WebLogic Server 9.x
- Oracle WebLogic Server 10.3 to 11g

Extended WebLogic discovery results

The following screen shows a successfully scanned WebLogic instance that is using an Oracle database server as its datasource. If a Microsoft SQL Server database is used, the Database Elements This Depends On row is displayed to indicate the actual database, because in this case the database server is represented by an SI. See Database nodes and relationships for more information.

This screen illustrates a successfully scanned WebLogic instance that is using an Oracle database server as its datasource.

The attributes section of the WebLogic SI contains sections for Components, Details, and Collections.

- **Components** are deployed EAR and WAR modules on WebLogic
Details are resources on WebLogic. These may be application specific or globally defined. They may be one of the following:

- Java Mail Resources
- JDBC Resources

Collections are J2EE Domains on WebLogic

Configuring extended WebLogic discovery

The extended WebLogic discovery is enabled by the activation of the WebLogic.ExtendedDiscovery pattern. This pattern is activated by default in a new installation of BMC Atrium Discovery, but in an upgraded appliance, it must be activated manually.

To use extended WebLogic discovery, you must configure the credentials for the WebLogic application server in the Credentials tab.

⚠️ Middleware credential always required

You must set up a middleware credential to perform extended discovery of WebLogic even if the target system requires no authentication. In this case, any values may be entered in the username and password fields.

To configure extended WebLogic discovery

1. Ensure that the WebLogic.ExtendedDiscovery pattern is activated.
2. From the Discovery home page, click Credentials.
3. Click the Middleware tab.
4. Click the Oracle WebLogic credential group heading.
5. Click the Credentials tab.
6. From the Credentials tab, select Create.

Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Credential (For example, ExtendedWebLogic).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a free text description of the Credential.</td>
</tr>
<tr>
<td>Username</td>
<td>The logon ID with which to connect to the WebLogic application server.</td>
</tr>
<tr>
<td></td>
<td>You must specify a logon ID that has a security role of Monitor, Operator,</td>
</tr>
<tr>
<td></td>
<td>Deployer, or Admin.</td>
</tr>
<tr>
<td>Password</td>
<td>The password corresponding to the username above.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the WebLogic host. This option can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• an IP address (10.10.10.3)</td>
</tr>
<tr>
<td></td>
<td>• a range specification (10.10.10.* or 10.10.1–5.* or 10.10.0/24)</td>
</tr>
<tr>
<td></td>
<td>• a regular expression matching an IP address (.* or 10.10.10.23</td>
</tr>
</tbody>
</table>

7. To save the details, click Apply.
   The new credential is displayed.
Integrating with BMC Atrium Orchestrator

BMC Atrium Orchestrator integrates, automates, and orchestrates processes across multiple applications and tools, as well as across multiple IT groups, such as support and operations.

The integration between BMC Atrium Discovery and BMC Atrium Orchestrator currently supports a single as well as multiple VMotion events. When a running virtual machine is moved either manually (VmMigratedEvent), or by distributed resource scheduler (DRS) (DrsVMMigratedEvent) using VMware VMotion, this is detected by BMC Atrium Orchestrator. When integrated with BMC Atrium Discovery, BMC Atrium Orchestrator triggers a rescan of the virtual machine that was moved, and the source and destination hosts.

The following screen illustrates a rescan of two IP addresses that was automatically triggered by BMC Atrium Orchestrator:

This screen illustrates a rescan of two IP addresses that was automatically triggered by BMC Atrium Orchestrator.

Requirements

To detect when a running virtual machine is moved from one physical host to another.

1. Discovery must be running.
2. The physical hosts and the virtual host must already have been scanned by BMC Atrium Discovery.

If these requirements are not fulfilled, the VMotion event is not stored for BMC Atrium Discovery to catch up. However, this will occur as part of routine discovery.

⚠️ Non-matching hostnames

BMC Atrium Orchestrator derives hostnames from the VMware API and BMC Atrium Discovery derives hostnames by using the discovery techniques. The derived hostnames could either be a Fully Qualified Domain Name (FQDN), or an actual host name. For successful integration between BMC Atrium Orchestrator and BMC Atrium Discovery, the derived hostnames must match (that is, in both the products, the derived hostname for a specific host must be either be an FQDN, or an actual hostname). If there is a hostname mismatch, Discovery rescan is not triggered for that particular host.
Configuration in BMC Atrium Orchestrator

BMC Atrium Orchestrator must have the Discovery-SA-Synchronization runbook installed.

Use the BMC Atrium Orchestrator Grid Manager to specify the correct BMC Atrium Discovery appliance, username, and password.

1. From the Manage tab, click Modules.
2. From the Modules in Repository panel, select the Discovery-SA-Synchronization module.
3. Click Activate.
4. From the Activated on Grid panel, click on the Discovery-SA-Synchronization module.
   The Edit Module Configuration page is displayed.
5. Select Virtualization-SA-Management.
6. Expand the Configuration tree to expand the following:
   Configuration  VM  Discovery
   For example:

   ![Configuration tree example](image)

   This screen illustrates the Configuration tree expanded.
7. Enter values for the following items appropriate to your system.

   | HTTP_POST_URL | a. Click on the HTTP_POST_URL link.  
   |               | b. For the Value (string) enter https://appliancename/ui/aoint where appliancename is the name of your BMC Atrium Discovery appliance. This URL must use https.  
   |               | c. To save the changes, click OK.  
   | password      | a. Click on the password link.  
   |               | b. For the Value (string) field, enter the password corresponding to the username specified below.  
   |               | c. To save the changes, click OK.  
   | username      | a. Click on the username field.  
   |               | b. For the Value (string) field, enter the username on the BMC Atrium Discovery system with permissions to launch scans, that is, a member of the Discovery group. For more information, see Group Permissions.  
   |               | c. To save the changes, click OK.  

   | Recommendation  
   | Create a dedicated user to simplify security, support, and auditing.  

8. To exit from BMC Atrium Orchestrator, click Logout.
Power System discovery

IBM Power Systems are Power Architecture-based servers that run AIX or Linux operating systems. Power System discovery extends the discovery of the AIX LPARS and WPARS (kernel virtualization) and Linux LPARS to include dependencies between applications running on LPARs and physical networks and storage that they rely on.

In a Power System, the frame (modeled as a Host Container node) contains one or two Virtual I/O (VIO) LPARs and a number of host LPARs. The frame also contains a hypervisor that enables direct communication between LPARs. The VIO LPAR controls host LPARs access to the host container resources (disk, I/O) and acts as a network bridge between the internal VLAN (on which the VIO server is connected) and the external physical network.

Multiple frames can be managed by a Hardware Management Console (HMC) a separate host that is used to configure and manage logical partitions, move running LPARS within a frame, and workload sharing and balancing.

⚠️ In some early versions of HMC, hmcbash shell does not exist. HMC hosts which do not have hmcbash installed cannot correctly interpret the Discovery commands and are therefore not supported by BMC Atrium Discovery.

IBM Virtual I/O (VIO) Server discovery

The Virtual I/O (VIO) Server is implemented as a management software layer that runs on top of an AIX 5.3 OS instance. The VIO management layer is not used for discovery; rather, the underlying AIX instance is used. The VIO management layer provides command line access using the ioscli command, which is a limited and restricted shell environment. The restrictions on users of this shell make it unsuitable for discovery by BMC Atrium Discovery (for example, key commands are unavailable and shell I/O redirection is not permitted).

In order to discover a VIO server you must add a normal UNIX user to the underlying AIX 5.3 instance, which requires root access. To obtain root access, you must either log into the AIX 5.3 instance directly as the root user (if such access has been enabled, it is not enabled by default) or log in to the VIO restricted shell and "escape" to the "OEM environment" using the following command:

```
$ oem_setup_env
```

After you have root access, you can add the discovery user using the `useradd` command as you would for any other AIX host:
Before you can use this account you need to configure a password.

```
# passwd discovery
```

You are prompted twice to enter a new password.

After the user is configured and a corresponding credential added to BMC Atrium Discovery, VIO Servers are discovered using the standard AIX discovery scripts. A discovered VIO server is shown in the following screen.

![This screen illustrates a discovered VIO server.](image)

It is also possible to avoid adding the local UNIX user account by escaping to the OEM environment in the standard AIX discovery script. However, this would give BMC Atrium Discovery unrestricted root access to the operating system. This would also affect normal AIX hosts (where the `oem_setup_env` command does not exist). However, in this case you might only receive a runtime error message that you can ignore. It is not possible to detect the presence of `oem_setup_env` on the VIO server due to the shell restrictions.

Hardware Management Console (HMC) discovery

The Hardware Management Console consists of a dedicated host with application software that runs on a Linux OS instance. The HMC layer provides command line access, but only in a limited and restricted shell environment. Unlike the VIO Server, this environment is sufficient for discovery by BMC Atrium Discovery with the following caveats:

- No process information is returned. There is no HMC command to report processes running on the HMC host. Because the HMC is a dedicated host running nothing but the HMC application, this should not be an issue.
- No port to process information. There is no HMC command to report this information. The `lsof` command would be used on other platforms.
- No HBA information is available. There are no HMC commands to report HBA information. The HMC hardware does not use an HBA.

The HMC management software SI contains the details on the hosts, host containers, and Power Systems that the HMC is managing. The Power Systems are represented as Detail nodes, as illustrated in the following screen.

This screen illustrates Power Systems represented as Detail nodes.

**Example visualization**

The following screen shows a visualization of an HMC management software SI with links to the Host Containers (frames) managed by the HMC. Contained within each of the frames is a single VIO server and a number of LPARS. To view this visualization, select Management from the Visualizations menu on the HMC management software SI.

This diagram illustrates a HMC management software SI visualization.
Discovering VMware ESX and ESXi hosts

Unpatched VMware vSphere known problems

Unpatched versions of VMware vSphere have known problems when scanned by various tools. We strongly recommend that you apply the appropriate patches to affected systems. There is more information on this issue on the following Configipedia link.

VMware ESX and ESXi

VMware ESX and ESXi are *bare-metal* embedded hypervisors, built on a Linux kernel, and run directly on server hardware without requiring an underlying operating system. VMware ESXi is a smaller footprint version of VMware ESX. In VMware ESX and ESXi versions before 3.5.0 the Linux environment was available through an ssh connection, with the introduction of version 3.5.0 the ssh capability must be enabled by the user. Discovery using the web services API (introduced with VMware ESX version 3.0.2) is the preferred method of discovering VMware ESX and ESXi.

ESX and ESXi 3.0 and onwards are classified as hypervisors. Previous versions are classified as Linux hosts.

VMware vCenter

VMware vCenter Server provides centralized management of VMware vSphere (ESX and ESXi) virtual machines. BMC Atrium Discovery uses the VMware vSphere API to communicate via a proxy with VMware vCenter to discover VMware ESX and ESXi hosts.

VMware vSphere API

VMware vSphere is a virtual infrastructure management suite. BMC Atrium Discovery uses the vSphere API to communicate directly with VMware ESX and ESXi hosts where no VMware vCenter credentials are available.

Discovered versions

VMware ESX and ESXi discovery uses version 2.5 of the vSphere API. This supports discovery of the following versions and later:

- ESX 3.5
- ESXi 3.5
- vCenter Server 4.0
- VirtualCenter 2.5

Discovering VMware ESX and ESXi hosts

Discovery of VMware ESX and ESXi hosts is performed in the following way.
1. A scan of an IP address detects the following:
   a. Port 902 is open and responds to a vSphere API call with a message from the VMware Authentication Daemon.
   b. Port 443 (HTTPS) is open.
2. If VMware vCenter credentials are defined, then discovery attempts to connect to vCenter on port 443 with a request to discover the target. vCenter then uses vSphere API calls to attempt discovery of the target. If this is successful then the ESX/ESXi host is discovered. There may be multiple vCenter credentials deployed for vCenter servers on the network. These are tried in turn until the host is discovered or the credentials are exhausted.
3. If unsuccessful, discovery attempts to make direct vSphere API calls to the target. This requires vSphere credentials and again, each is tried in turn until the host is discovered or the credentials are exhausted.
4. If vSphere is unsuccessful, and port 22 or an alternative ssh port is configured, an ssh discovery is attempted.

The following screen shows a discovered VMware ESX host.

![VMware ESX host](image)

Shows a VMware ESX host page.

**VMware vCenter based discovery**

VMware vCenter Server provides centralized management of VMware vSphere (ESX and ESXi) virtual machines.

**Discovery of vCenter**

Discovery of a vCenter instance itself is simply a matter of standard host discovery and the creation of a vCenter SI. It does not rely on vSphere API calls, or ports 902 or 443 being open. However, to use vCenter to discover ESX/ESXi hosts, discovery uses port 443 to communicate with the vCenter server.
Discovery of VMware ESX and ESXi hosts via vCenter

BMC Atrium Discovery can discover ESX and ESXi hosts via the vSphere web services API, or a fallback to an ssh login. However, if the host is being managed by vCenter and it is put into "lockdown mode", these discovery techniques are disabled and access is only available via vCenter. VMware vCenter based discovery uses vCenter as a proxy in a similar manner to the Windows proxies.

To discover an ESX or ESXi host using vCenter, scan the IP address of the target host. Once discovery has determined that the host is an ESX or ESXi host, the discovery request is passed to the vCenter proxy which uses a vCenter credential to pass vSphere API calls through vCenter onto the target hosts.

The API calls described on the vSphere API Support page at Administration => Discovery Platforms => VMware ESX or VMware ESXi are used to discover the system.

![Image showing API calls](image)

**Shows the API calls made to discover the vCenter managed system.**

**VMware vSphere based discovery**

---

**Unpatched VMware vSphere known problems**

Unpatched versions of VMware vSphere have known problems when scanned by various tools. We strongly recommend that you apply the appropriate patches to affected systems. There is more information on this issue on the following Configipedia link.
VMware vSphere based discovery

VMware vSphere based discovery of VMware ESX and ESXi hosts is a part of the overall discovery methodology of ESX and ESXi hosts that is outlined in Discovering VMware ESX and ESXi hosts. It takes place as follows:

Discovery checks that ports 443 (HTTPS) and 902 (VMware Authentication Daemon) are open. The initial connection is a web services request to port 902 to ensure that the vSphere API is available. The vSphere discovery method then attempts to access the vSphere API using port 443.

The API calls described on the vSphere API Support page at Administration => Discovery Platforms => VMware ESX or VMware ESXi are used to discover the system.

Shows the API calls made to discover the vCenter managed system.

If the API is not contacted then discovery falls back to an ssh login as used in previous BMC Atrium Discovery versions.

VMware ESX and ESXi ssh discovery

VMware ESX and ESXi ssh discovery is used as a fallback when the other methods of discovering VMware ESX and ESXi hosts outlined in Discovering VMware ESX and ESXi hosts fail.

If the vSphere API is not contacted then discovery falls back to an ssh login as used in previous BMC Atrium Discovery versions. and the discovery methods detailed in Administration => Discovery Platforms => VMware ESX or VMware ESXi are used to discover the system. If ssh access has not been enabled, the ESX or ESXi system is not discovered.
Shows the discovery methods used to discover the vSphere based system in the case that the API was not accessed.

VMware ESX and ESXi ssh discovery must be done as the root user
VMware ESX and ESXi ssh discovery must be done as the root user. You should login directly as the root user. It is possible to login as a non-root user but such a user cannot close its sessions properly. This results in sessions hanging and inactive sessions building up on the ESXi host.

VMware ESX and ESXi discovery limitation
VMware ESX and ESXi ssh discovery cannot determine any network connection details as there is no equivalent to the `netstat` command.

Improving discovery

BMC Atrium Discovery provides as much information as it can about your environment. To maximize this ability, there are features in the product to help you improve the level and quality of access to the environment.

- **Monitoring credential usage**: Discovery relies on access credentials. The credentials management tools provide an overview of the success rate of the credentials to assist you in monitoring the roll out and currency of the credentials in use. This can monitor Login Credentials, Windows proxies and SNMP Credentials.
- **Troubleshooting via SessionResults**: Discovery records a lot of useful metadata information about each access to the environment. This page describes some of the information available and how to use the results to troubleshoot access issues.
- **Discovery Conditions**: There are many scenarios where the system can detect that data could be improved. The Discovery Condition tools enable you to see advice on what actions you can take, and which hosts are impacted by these actions.

Discovery Conditions

Discovery Conditions are hints to administrators. They describe configuration issues in an estate that, if resolved, can help BMC Atrium Discovery retrieve more detailed or complete data. Doing this improves the view of the estate, so that users can act on the knowledge it gathers with greater confidence.
The knowledge of Discovery Conditions are encoded in patterns so full details of which conditions can be detected and advice is available on the following Configipedia link. Here the focus will be how to use the tools.

Viewing current Discovery Conditions

Overall view

1. From the Discovery tab, select Discovery Reports.
2. In the Directly Discovered Data Index section, select Discovery Conditions.

Discovery Conditions are not logged until a Host with the issue is scanned.

From a host view

1. Scroll towards the bottom of the host view to find the Inference section.
2. If Discovery Conditions have been logged, they are summarized under the Discovery Conditions section, following Discovery Access section.

This screen illustrates a summary displayed of logged Discovery Conditions.

Viewing hosts with Discovery Conditions logged

Discovery Condition Detailed List report

This report shows a list of hosts with logged Discovery Conditions along with the time the condition was first logged sorted so the most recent are at the top. Clicking through will show the Host page. This report is ideal for exporting to CSV to make a tasklist for resolving the issues.

1. From the Discovery tab, select Discovery Reports.
2. In the Discovery Dashboard Reports section, select Discovery Condition Detailed List.

This report is also available from the Discovery Dashboard.
Hosts impacted by Discovery Conditions report

This report shows a detailed list of hosts that have Discovery Conditions logged. This report is ideal for filtering the selection of Hosts on the detailed criteria to prioritise.

1. From the Discovery tab, select Discovery Reports.
2. In the Discovery Dashboard Reports section, select Hosts impacted By Discovery Condition.

This report is also available from the Discovery Dashboard.

Understanding Discovery Conditions

Discovery Conditions have the following fields:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The overview of the condition.</td>
</tr>
<tr>
<td>Impact</td>
<td>The impact of the condition.</td>
</tr>
<tr>
<td>BMC Link</td>
<td>Link to our online detailed description of the condition and advice on how best to resolve it.</td>
</tr>
<tr>
<td>Description</td>
<td>A short description of the condition</td>
</tr>
<tr>
<td>Resolution</td>
<td>A short summary of the resolution steps.</td>
</tr>
<tr>
<td>Vendor Links</td>
<td>Links to vendor descriptions and fixes if relevant.</td>
</tr>
<tr>
<td>Applies to</td>
<td>Link to all the Host impacted by this condition.</td>
</tr>
</tbody>
</table>

The following screen shows an example view of a Discovery Condition:

This screen illustrates an example view of a Discovery Condition.

Credentials

During discovery, the BMC Atrium Discovery system attempts to access host systems to obtain details of processes running. Credentials including IDs and passwords, and credential-like entities (Windows proxies and SNMP credentials) for different access methods, can be stored on the system to allow the required level of access. You can set up the following:
• The **login credentials** (user IDs and passwords) for interactive log-in to different host systems.

• The **Windows proxies** used to discover Windows systems.

• The **SNMP credentials** used on particular host systems. SNMP queries are only tried if an attempted login fails and if the SNMP port (UDP 161) is open on the target host.

• The **vSphere credentials** used to discover VMware ESX and ESXi hosts.

• The **vCenter credentials** used to discover VMware ESX and ESXi hosts by querying the vCenter server.

• You can also run and view the progress of Device Credential Tests.

• **Databases** used to query databases.

• **Middleware** used to query middleware such as web and application servers.

• **Management Systems** used to query management systems such as VMware Virtual Center.

### About credential storage

BMC Atrium Discovery stores all passwords in a secure credential vault. Secure credential vaults are generated using public and private key pair when the appliance is commissioned. The contents of the vault is encrypted, and can be secured using a passphrase.

### User accounts on the target system

When creating a user account (the account that BMC Atrium Discovery logs into to discover a host) on a target host, you should ensure that the full path to the shell is entered in the user's profile. If you do not do this, the credentials will be considered invalid. For example: SHELL=/bin/sh

⚠️ **Shell support**

BMC Atrium Discovery is tested to work with Bourne and Bourne-compatible shells. Support for other shells such as the Korn shell is best effort only. The product has been sporadically tested and may work but with known issues and we may not fix bugs that affect these shells.

### Device credentials

Device credentials are those credentials which provide means of logging into hosts running a Unix, or Linux operating system, a Windows operating system, or any SNMP enabled device such as routers and switches. The configuration of device credentials is described in the following sections:

• Configuring host login credentials

• Configuring Windows discovery

• Configuring SNMP credentials

• Configuring vCenter credentials
1. Configuring vSphere credentials
2. Testing credentials
3. User privileges and information access

Configuring host login credentials

The preferred method of accessing remote hosts using discovery is by a remote login. You can set up different login credentials to use on different machines, by individual IP address or a range of addresses.

Available access methods are ssh, telnet, rlogin, and windows. You can set up several access methods and define the order in which they are to be attempted. Each access method is attempted until a working credential is found or the list is exhausted.

When you enter a user name and password for use by a credential Windows proxy, you must prefix the user name with localhost (for example, localhost\Administrator).

For each host that is successfully logged into, the successful access method is recorded. On subsequent scans the first access method attempted is the one that succeeded for that host on the previous attempt, so long as the appropriate option is selected in the Discovery Configuration page.

If an access login method is disabled (for example, telnet) and that method is recorded as the last successful login method, it is tried again on a subsequent scan. If it fails on that scan then that method will not be tried again until it is re-enabled.

An access method is only attempted if it is seen to be available (for example, SSH access will only be attempted if the SSH port is open).

Viewing login credentials

To view existing login credentials:

1. From the secondary navigation bar on the Discovery tab, click Credentials.
2. Click Devices.

The following screen illustrates an example of the host login credentials page:

At the top of the host login credentials page, the system displays the total number of host login credentials and also the number of host login credentials by each access method.
The credentials are checked in sequence, and the first matching entry is used. After a working credential is found, further credentials are not checked. If you want to reorder login credentials, drag the credential to the required position in the list.

The credentials are shown in color coded boxes. The colors represent the level of login success achieved with that credential:

- **Green**: 100% success rate.
- **Yellow**: partial success.
- **Blue**: the credential has never been used.
- **Red**: 0% success rate.

**Show matching credentials – new in 8.3 SP2**

A new feature is introduced in BMC Atrium Discovery 8.3 SP2 which enables you to highlight all credentials which match a specified IP address.

To show matching credentials:

1. From the Credentials > Devices > Hosts page, click the **Show Matching Credentials** button.
2. Enter the IP address that you want to check into the dialog box and click **Search**.
3. Any credential which has an IP range matching the specified IP address is highlighted in yellow and a banner summarizing the results is displayed just below the page heading.

![Page showing the configured credentials whose valid IP range match or contain a specified IP address.](image)

If no matching credentials are found this is stated in the banner.

The **Show matching credentials** button is available on the following credential pages:

- Hosts
- SNMP
- vCenter
- vSphere
Mainframe

The following information is shown for each credential:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>This is the first part of the heading link for the credential. The range of IP addresses on which this credential is intended to be used. A link is also provided showing the last successful use of the credential. This links to the Discovery Access for that use.</td>
</tr>
<tr>
<td>Username</td>
<td>This is the second part of the heading link for the credential. The user name used for this credential.</td>
</tr>
<tr>
<td>Description</td>
<td>A free text description of the credential supplied by the user who created the credential.</td>
</tr>
<tr>
<td>Usage</td>
<td>A summary of the success rate when the credential has been used, information about failures, and links to DiscoveryAccesses, credential lists and other useful diagnostic pages.</td>
</tr>
<tr>
<td>Options</td>
<td>Additional options used with this credential. With the exception of No Password (use ssh key exchange), the options are those selected from the Options section when the credential is set up. The No Password (use ssh key exchange) option is selected by not entering a password. For information about these, see the Field Name-Details table for # Setting up host login credentials.</td>
</tr>
<tr>
<td>Actions</td>
<td>A list with the following options:</td>
</tr>
<tr>
<td></td>
<td>Edit: Select this to edit the credential. See #Setting up host login credentials for information about the fields and settings available from the Edit Login Credential page.</td>
</tr>
<tr>
<td></td>
<td>Delete: Select this to delete the credential.</td>
</tr>
<tr>
<td></td>
<td>Test: Select this to test the credential. See #Setting up host login credentials and #Testing login credentials for more information.</td>
</tr>
<tr>
<td></td>
<td>Move to top: moves the credential to the top of the list.</td>
</tr>
<tr>
<td></td>
<td>Move to bottom: moves the credential to the bottom of the list.</td>
</tr>
</tbody>
</table>

Setting up host login credentials

1. From the login credentials page, click Add.
2. Set up the login credentials as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>Enter an IP address, a range of IP addresses, or a regular expression representing the IP addresses for which this credential is valid. IP address: for example, 10.10.10.3</td>
</tr>
<tr>
<td></td>
<td>Range of IP addresses: 10.10.10.* or 10.10.1-5.* or 10.10.10.0/24</td>
</tr>
<tr>
<td></td>
<td>Regular expression: .* or 10.10.10.(23</td>
</tr>
<tr>
<td>Username</td>
<td>Username used to log in to hosts identified by the key. If this is a Windows credential that will be used by a credential Windows proxy, ensure you prefix the user name with localhost e.g. localhost\Administrator.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password into the password entry field; the password text is not echoed to the screen. In the Edit Login Credential page, this field is displayed as Set Password. The existing password is shown as a series of asterisks in this field and it cannot be edited. To enter a new password, select the checkbox. The password entry field is cleared. Now enter the new password.</td>
</tr>
<tr>
<td>Description</td>
<td>A free-text description of this login credential.</td>
</tr>
</tbody>
</table>
### Field Name | Details
--- | ---
**Access Methods** | Choose the access methods to be attempted for any host identified by the key by selecting them and moving them to the right-hand (enabled) list box using the right arrow button. By default, all access methods are placed in this box, that is, they are all enabled. You can also change the order in which the access methods are attempted by selecting them and moving them up or down with the up or down arrow buttons.

**Session Logging** | If you want to create a session log, select **Enabled**. This logs all communication between the BMC Atrium Discovery appliance and a host and should only be used for diagnosing discovery problems with that host. There is currently no option for recording a session log for Windows hosts.

**Prompt** | A regular expression to define valid prompt characters expected.

**SU** | To use the su command to change to the root or any other user, select **Switch User**. Enter the user to change to, and the corresponding password. The password text is not echoed to the screen.

**Timeout** | Enter a timeout period (in seconds) for a session. This timeout includes the credential handshaking (see also the Session Login Timeout). This timeout is used to control sessions. The default is 180 seconds. In general, it is not used to limit the time to scan devices. Note that more than one session can be used to scan one device. For this reason, a scan can take more time than this timeout. A typical consequence of this timeout (when the execution of the platform script for getInterfaceList takes more than this timeout) is that the scan will fail with a script failure (error message **Connection timed out**).

**Force Subshell** | To force the session to open a Bourne (`/bin/sh`) subshell, if the default login shell is a C shell (`/bin/csh`/`/bin/tcsh`), select **Yes**. This enables you to cater for machines using non-standard shells.

**SSH Key** | Specify an existing SSH key which you already have deployed in your organization. Click **Browse** to locate the private key and click **Open** to select it. Enter the passphrase in the passphrase field. When you click **Apply** to save the credential, the key and passphrase are validated. When you upload the private key to the appliance it is strongly recommended that you protect it with a passphrase. See [#SSH keys](#SSH keys) below for more detailed information.

**SSH Authentication** | To use an SSH key or password, select **Key** or **Password**. If you have not configured an SSH key, **Key** is dimmed.

**Custom SSH Port** | If the host for which this credential is intended is configured to listen for SSH connections on a non-standard port, enter this here. To do this, select the **Enable custom ssh port?** checkbox and enter the port number in the entry field. If you add a port here, it is automatically added to the TCP ports to use for initial scan. For more information, see the **TCP and UDP ports to use for initial scan** section in **Configuring discovery**.

**Custom Telnet Port** | If the host for which this credential is intended is configured to listen for Telnet connections on a non-standard port, enter this here. To do this, select the **Enable custom telnet port?** checkbox and enter the port number in the entry field. If you add a port here, it is automatically added to the TCP ports to use for initial scan. For more information, see the **TCP and UDP ports to use for initial scan** section in **Configuring discovery**.

3. To add the credentials, click **Apply**.
4. Repeat for all the credentials you want to add.

#### Editing host login credentials

1. From the login credentials page, click **Actions** for the credential.
2. Select **Edit**.
3. In the Edit Login Credential page, edit the host login credential fields. The fields in this page are the same as the fields in the Create Login Credential page. For more information about the fields, see the field-details table for #Setting up host login credentials.

4. To add the edited credentials, click Apply. Repeat this for all the credentials you want to edit.

**SSH keys**

You can attach an SSH key to any credential using the SSH access method.

- BMC Atrium Discovery supports only RSA2 and DSA private keys for certificate-based authentication. For the hosts that only support SSH v1 it is recommended to use credentials for authentication.

When using SSH keys, the appliance must identify itself to discovery targets so must use the private key. It is strongly recommended that you protect the private key with a strong passphrase. When they are uploaded to the appliance, the key and the passphrase are stored in the credential vault.

If the attempted login is unsuccessful using the SSH key, the credential falls back and attempts to login using the configured username and password.

It is important to configure a username and password even when an SSH key is to be used. When privileged command execution is required, that password is used in the command, for example `sudo password command`.

- After the key is stored in the credential vault, it is encrypted and cannot be recovered from the vault. You are strongly recommended to keep copies of private keys in secure storage according to your local security guidelines.

**Testing login credentials**

When you have added the credentials, you can test them by performing the following actions:

1. On the login credentials page, click Actions for the login credential.
2. Select Test.

- If the test link is not displayed, click START ALL SCANS on the Discovery Status page.
3. To test the credential, enter a single IP address in the **IP Address** field. For example, 137.72.93.222.
4. Click **Test**. The page is refreshed to show that the test in progress and when complete, the results are shown.
5. You can perform other credential tests from the **Credential Tests** page.

**Configuring Windows discovery**

Windows discovery requires a Windows proxy host because the methods that are used to access Windows hosts are only available from Windows systems. Windows discovery is handled in one of the following ways:

- **Credential Windows proxy**: A BMC Atrium Discovery application that runs on a customer-provided Windows host and uses credentials supplied by the BMC Atrium Discovery appliance to perform Windows discovery.
- **Active Directory Windows proxy**: A BMC Atrium Discovery application that runs on a customer-provided Windows host that is part of an Active Directory domain. The user that the Windows proxy service runs as is configured when it is installed. Where that user is configured on hosts in the domain, the Windows proxy can log in and run discovery commands. The Active Directory Windows proxy does not use any credentials entered using the BMC Atrium Discovery user interface.

Starting with BMC Atrium Discovery, version 8.2, the **Workgroup Windows proxy** is no longer supplied with the appliance. All of its functionality has been moved into the Active Directory Windows proxy.

Windows proxies are grouped into Windows proxy pools. This enables the appliance to distribute discovery requests in order to balance the load of the proxies. Each proxy pool can only hold one type of Windows proxy (for example, a credential proxy pool can hold only credential proxies).

All proxies in a pool must have identical access to Windows hosts, as only one proxy per pool is tested for access. Unless proxy pools are restricted by IP address, a typical configuration consists of one proxy pool per Active Directory domain containing one or more Active Directory proxies, and a proxy pool containing one or more Credential proxies.

The Windows proxy pools are displayed in the order (from top to bottom) in which you have added them to the appliance. You can change their order. For discovery tasks, the proxies in a Windows proxy pool are selected depending on their loading.

Before you can use a Windows proxy to discover your Windows IT infrastructure, you must perform the following tasks:
1. Install and run the Windows proxy software.
   For more information, see Installing Windows proxies.
2. Add Windows proxy pools to the appliance.
   For more information, see Adding Windows proxies and proxy pools.
3. Add the Windows proxies to the proxy pools.
   For more information, see Adding Windows proxies and proxy pools.

⚠️ **Potential user lock out**

By default, AD accounts have a limited number of login attempts, for example three attempts in fifteen minutes. Access Denied errors from WMI, DCOM, and local commands such as systeminfo are counted as unsuccessful login attempts. Where target hosts are incorrectly configured, this limit can be exceeded and the account locked out.

To avoid this, configure the Discovery account to accept unlimited login attempts.

---

### Windows discovery utilities no longer shipped in BMC Atrium Discovery

From version 8.1 the following utilities are no longer shipped with BMC Atrium Discovery. You can download them freely and install them where required.

- `rcmd`: see the [Microsoft Download Center](https://www.microsoft.com) and search for the resource kit for the version of Windows that you are running.
- `pulist`: download this from the [Microsoft Download Center](https://www.microsoft.com).
- `tlist`: download this from the [Microsoft Download Center](https://www.microsoft.com).

### Windows proxy management

#### Proxy changes in 8.3 SP2

In BMC Atrium Discovery 8.3 SP2, installation and management of proxies has been improved with the introduction of a new Windows proxy manager tool. It is also possible to install multiple proxies of each type on a single host. For information on the changes, see [Windows proxy manager](#).

You can manage Windows discovery using the Windows proxy management window. The Windows proxy management window contains the list of the available Windows proxy pools and the Windows proxies in each pool. Each proxy pool can only hold one type of Windows proxy (for example, a credential proxy pool can hold only credential proxies). The Windows proxy management window can contain multiple Windows proxy pools. For more information about the Windows proxy pool list, see [Windows proxy pool list](#).
The minimum version and release options are set on the Discovery Configuration page.

To navigate to the Windows proxy management window:

1. From the secondary navigation bar on the Discovery tab, click Credentials.
2. Click Windows Proxies.

The Device Credentials page displays the Windows proxy pools.

Windows proxy pool list

The Device Credentials page for Windows proxies lists the available Windows proxy pools and the Windows proxies in each pool. The Windows proxy pools are displayed in the order (from top to bottom) in which you have added them to the appliance.

You can change the order of the Windows proxy pools by the following ways:

- Using the colored margin at the left of the row, drag and drop the row to the required position in the user interface.
- Click the Actions list for the Windows proxy pool and select Move up or Move down.
- To move a Windows proxy pool to the top or bottom of the list, click the Actions list and select Move to top or Move to bottom.

⚠️ Reordering of Windows proxies in a Windows proxy pool is not supported, as the proxy used is selected automatically.

For each Windows proxy pool, the following fields are displayed:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Windows proxy pool.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of the Windows proxy pool (for example, Active Directory).</td>
</tr>
<tr>
<td>Domain</td>
<td>This field is available for Active Directory Windows proxy pools only. It displays the applicable domains.</td>
</tr>
<tr>
<td>Actions</td>
<td>A list with the following options:</td>
</tr>
</tbody>
</table>

- Add Windows proxy: Enables you to add Windows proxies to the Windows proxy pool. For more information, see Adding Windows proxies and proxy pools.
- Manage: Opens the Edit Windows Proxy Pool page. For more information, see Managing Windows proxy pools.
- Delete: Enables you to delete the Windows proxy pool. If you delete a Windows proxy pool, the Windows proxies in the pool are also deleted.
- Move to top: Moves the Windows proxy pool to the top of the list.
- Move to bottom: Moves the Windows proxy pool to the bottom of the list.

Proxy ordering in upgraded appliances

Proxy pools themselves can be ordered, the proxies in them cannot. Consequently it is not possible to preserve the ordering that has been configured in pre-version 8.3 systems.
The following ordering and distribution of proxies occurs automatically during the upgrade.

1. All Workgroup proxies are put into their own pool.
2. AD proxies are grouped by domain and IP restriction list. AD proxies with the same domain and restriction lists are placed in the same pool.
3. Credential proxies are grouped by IP restriction list.

**Windows proxy list**

Each proxy pool displays the Windows proxies in rows. For discovery tasks, the Windows proxy pool checks for a Windows proxy. If a proxy has not previously been used to discover the endpoint, then for each proxy pool (matching the domain) in the order that the pools appear:

1. a proxy is selected, and discovery attempts to contact it
   - if successful then that proxy is used.
   - if unsuccessful due to a timeout, then other proxies in the pool are tried.
   - if unsuccessful due to an error, then no more proxies in the pool are tried and the remaining pools are tried in the order in which they appear.

The Windows proxies are shown in color-coded boxes where each color represents the level of login success achieved:

- Green: 100% success rate.
- Yellow: Partial success.
- Blue: The credential has never been used. Credential proxies always appear blue. To check their success rate, see the credential list.
- Red: 0% success rate.

For each Windows proxy, the following fields are displayed:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the Windows proxy and the IP address and port. A link is also provided showing the last successful use of the credential. This links to the proxy management screen.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows a summary including if the Windows proxy is Active, Disabled, Incompatible, or Unreachable.</td>
</tr>
<tr>
<td></td>
<td>- See Managing Windows proxies for information on how to enable the Windows proxy.</td>
</tr>
<tr>
<td></td>
<td>- Windows proxies are reported as unreachable if it has not been pinged successfully by the appliance.</td>
</tr>
<tr>
<td></td>
<td>- For a Windows proxy to be considered active, its version number and release number must be equal to or greater than the minimums specified.</td>
</tr>
<tr>
<td>Version</td>
<td>The version and release of the Windows proxy.</td>
</tr>
<tr>
<td>Usage</td>
<td>A summary of the success rate when the Windows proxy has been used, information on failures, and links to DiscoveryAccesses, credential lists and other useful diagnostic pages.</td>
</tr>
<tr>
<td>Actions</td>
<td>A list with the following options:</td>
</tr>
<tr>
<td></td>
<td>- Manage: Opens the Manage Windows proxy page. See Managing Windows proxies.</td>
</tr>
<tr>
<td>Field Name</td>
<td>Details</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
</tr>
<tr>
<td>Ping</td>
<td>Pings the Windows proxy to ensure that it can be contacted. This is only available if it is enabled. On a successful ping, the information is refreshed. If the ping is unsuccessful, no version number is displayed.</td>
</tr>
<tr>
<td>Test</td>
<td>Tests connectivity between the Windows proxy, if it is enabled, and a supplied IP address. See #Testing connectivity.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the entry.</td>
</tr>
</tbody>
</table>

**Testing connectivity**

To test the connectivity between a Windows proxy and a supplied IP address, perform the following actions:

1. Select **Actions > Test** for the Windows proxy.
2. Enter the IP address to use for the test and click **Test**.

   The credential tests page is displayed with the test in progress. For more information about the credential tests page, see **Testing credentials**.

**Installing Windows proxies**

1. **Proxy changes in 8.3 SP2**

   In BMC Atrium Discovery 8.3 SP2, installation and management of proxies has been improved with the introduction of a new Windows proxy manager tool. It is also possible to install multiple proxies of each type on a single host. For information on the changes, see **Windows proxy manager**.

Windows proxies are downloaded as install files from the appliance and installed onto the local Windows host. You must be logged in as an administrator to install Windows proxies. If the software is not installed as this user then you need to grant permissions to write to C:\Program Files\BMC Software\ADDM Proxy.

The user that runs the Windows proxy must have necessary permissions to read from and write to the etc, log, and record directories.

As a user on the appliance, you must have been granted the admin/software/slave/download permission to download the Windows proxy installers.

**Windows proxy version and operating system compatibility**

The following table provides information on compatibility between Windows proxy types and versions, and the operating systems that the Windows proxy runs on for BMC Atrium Discovery version 8.3.
### Windows Proxy Type

<table>
<thead>
<tr>
<th>Windows Proxy Type</th>
<th>Earliest Windows Proxy Version Supported</th>
<th>Windows Proxy Available for Supported Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential Windows proxy</td>
<td>7.3</td>
<td>Windows 2003 SP2 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2008 - Service Pack 2 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Active Directory Windows proxy</td>
<td>7.3</td>
<td>Windows 2003 SP2 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2008 - Service Pack 2 (x86 and x86_64)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2008 R2</td>
</tr>
</tbody>
</table>

### getServices

The `getServices` discovery method was introduced with BMC Atrium Discovery version 8.1. Windows proxies before version 8.1 do not support this method although are supported in all other respects.

### getFileSystem

The `getFileSystem` discovery method was introduced with BMC Atrium Discovery version 8.2. Windows proxies before version 8.2 do not support this method although are supported in all other respects.

### Workgroup Windows proxy deprecated

The Workgroup Windows proxy has not been supplied since before BMC Atrium Discovery version 8.2. All of its functionality has been moved into the Active Directory Windows proxy.

<table>
<thead>
<tr>
<th>Windows Proxy type</th>
<th>Earliest Windows Proxy Version Supported</th>
<th>Windows Proxy Available for Supported Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workgroup Windows proxy</td>
<td>7.3</td>
<td>Windows Server 2008 (x86 - 32bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows XP - Service Pack 2 (x86 - 32bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows 2003 - Service Pack 2 (x86 - 32bit)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Refers to 8.1 version.</td>
</tr>
</tbody>
</table>

### Minimum host specification

The following are the minimum recommended specifications for the Windows proxy host:

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>As stated in tables above</td>
</tr>
<tr>
<td>CPU</td>
<td>2GHz Intel Pentium® 4 CPU 512k Cache (or equivalent from other manufacturer)</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Hard disk</td>
<td>60GB</td>
</tr>
</tbody>
</table>
To avoid any impact during resource-intensive periods of discovery, it is strongly recommended not to install the Windows proxy on any host supporting other business services. This is true even if the minimum Windows proxy specification is exceeded, since the Windows proxy will attempt to use what resources are available, in order to optimize scan throughput.

Windows discovery communications
You should also consider the ports that will need to be opened in any firewall between the appliance and the proxy or proxies, and the proxies and target hosts.

Windows discovery metadata
Discovery metadata covers Windows as well as UNIX. This provides information about why sessions failed to be established and why scripts failed to run, including information about what credential or Windows proxy was used.

Windows proxy upgrade and installation

Previous versions of the Windows proxy have used an omniORB configuration file (C:\omniOrb.cfg). Version 7.2 and later Windows proxies do not use this file in the same way. If you have a C:\omniOrb.cfg file on your system before installing the Windows proxy, you should rename it to C:\omniOrb.cfg.old before installing a new Windows proxy. If you do not, you may experience connectivity problems with the new Windows proxy.

Installing or upgrading Windows proxies where anti-virus software is installed
Before installing Windows discovery proxies you should either disable the anti-virus software or configure it to exclude remquery from triggering a virus alert. You can enable the anti-virus software once the Windows proxy has been installed.

Downloading a Windows proxy installer
To download a Windows proxy installer:

1. From the Tools section of the Discovery page, click the appropriate link for the type of Windows proxy to download:
   - Download installer for Active Directory Proxy, version 8.3
   - Download installer for Credential Proxy, version 8.3
2. Save the installation file to your file system.

Upgrading a Windows proxy
Before upgrading an existing Windows proxy, you must:

- Ensure that the existing Windows proxy is not running. If you fail to do this you will need to reboot the computer after the upgrade.
- Accept the default installation directory, or enter a new installation directory. You must not use the same directory as the existing Windows proxy.
- Enter the username used in the current Windows proxy when prompted for the username that the service should run as.
Installing a Windows proxy

To install a Windows proxy:

1. Run the installer by double-clicking on the downloaded installer file.
   A welcome screen is displayed.
2. Click **Next**.
3. Click **Browse** to select an installation directory, and then click **Next**.
   To accept the default installation directory (C:/Program Files/BMC Software/ADDM Proxy), click **Next**.
4. To create the Windows proxy application’s shortcuts, click **Browse** to select a different folder,
   or click **Next** to accept the default folder.
5. On the **Select Additional Tasks** screen, choose options that will be available in the Start menu,
   and then click **Next**. If you chose **Don't create a Start Menu Folder** in the preceding step, clear all the check boxes and click **Next**.
6. To display the Service Credentials window, click **Next**.
7. Enter the credentials for the user account that will run the Windows proxy.
   If you do not enter the credentials at this point you can do so later, see **Specifying the account used to run the Windows proxy**. The Windows proxy will run as the Local System user if credentials are not entered.

   ![Credential Windows proxy User](image)

   You should not run the Credential Windows proxy as the Local System user, but as a valid local user account, which should be in the local Administrators group.

8. Review the details in the Ready to Install window and, if they are correct, click **Install**.
   If the details are incorrect, click **Back** and navigate through the installer to correct the error.
9. Click **Finish** to exit the installer.
10. A dialog box is displayed showing whether the Windows proxy has been successfully installed. On the dialog box is a checkbox marked **Register with appliance**. Select this checkbox to open the **BMC Atrium Discovery UI Create Windows proxy** page, prepopulated with details of this Windows proxy when this part of the setup is complete. You may see a dialog box regarding File Download. Accept this to go to the prepopulated **Create Windows proxy** page.
11. Click **Finish**.
    The Windows proxy is now installed and if you have selected the **Register with appliance** checkbox, the prepopulated **Create Windows proxy** page is displayed.

   ![Service startup failure](image)
Sometimes Windows may refuse the installer permission to start the Windows proxy service, resulting in a dialog box along the lines of *service installed but could not be started*. This is remedied by manually supplying the credentials directly to the service using the Windows UI. See Specifying the account used to run the Windows proxy.

Post installation settings

The following sections detail post installation settings and modifications that might be required for Windows proxies.

Modifying the Windows proxy host firewall

The Windows firewall blocks the ports that the Windows proxies use by default. To enable an appliance to communicate with a Windows proxy, you must amend the firewall rules to permit communication on one of the following ports for each Windows proxy type installed on the host:

- 4323: Credential Windows proxy.

To do this, select Windows Firewall from the Windows Control Panel. You can add a Windows proxy as an exception (as a program or a port) on the exceptions tab.

Specifying the account used to run the Windows proxy

The Active Directory Windows proxies gain their permissions on the discovery target from the user account that they run as, whereas the Credential proxies gain their permissions on the discovery target from the credentials entered in Discovery > Credentials > Devices > Hosts. To configure this:

1. From the Start Menu, select Settings => Control Panel. The Control Panel is displayed.
2. Double-click Administrative Tools and then Services.
3. The Services list is displayed in the right-hand pane.
4. Right-click on the Windows proxy entry and select Properties from the popup menu.
5. Switch to the Log On tab and select This account.
6. Depending on the proxy type to be configured, perform the following:
   - For a Credential Proxy, enter the user name and password for a valid local user account, which should be in the local Administrators group.
   - For an Active Directory proxy, enter the user name and password of the Domain account that the service is to run as.
     You may see a dialog saying that the user has been granted the Log on as a Service right.
7. To apply the changes and dismiss the window, click OK.

Starting or stopping the Windows proxy
To do this, from the Control Panel, navigate to Administrative Tools and access the Services list. Select the Windows proxy that you want to start or stop. The services panel is refreshed with information and links enabling you to start, restart, or stop the Windows proxy.

- To start the Windows proxy (if it is not running) click **Start the service**.
- To restart the Windows proxy (if it is running) click **Restart the service**.
- To stop the Windows proxy (if it is running) click **Stop the service**.

Starting the Windows proxy automatically

When the Windows proxy is working satisfactorily, you should set it to start automatically. To do this, from the Control Panel, navigate to Administrative Tools and access the Services list. Select the Windows proxy that you want to start automatically and select Properties from the popup menu.

Select **Automatic** from the Startup type: drop-down list, and click **OK** to apply the changes.

Specifying additional startup options

When the Windows proxy is working satisfactorily, you can then specify additional startup options. Many of these can also be specified through the Manage Windows Proxy page. These are noted in the table below.

You can also enter the start up options described in the table below in the registry key appropriate for the Windows proxy type and host architecture. On a 32 bit system this is one of:

- **Active Directory Windows proxy**
  
  HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Atrium Discovery\ADPROXY\CommandLine

- **Credential Windows proxy**
  
  HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Atrium Discovery\PROXY\CommandLine

On a 64 bit system this is one of:

- **Active Directory Windows proxy**
  
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BMC Software\Atrium Discovery\ADPROXY\CommandLine

- **Credential Windows proxy**
  
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BMC Software\Atrium Discovery\PROXY\CommandLine

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--auto-purge-all</td>
<td>You can configure the Windows proxy to automatically purge its log and record data directories. The default behavior is not to purge. Specifies that log and record data directories will be purged. Set via UI.</td>
</tr>
<tr>
<td>--auto-purge-logs</td>
<td>Specifies that only log directories will be purged. Set via UI.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--auto-purge-record</td>
<td>Specifies that only record data directories will be purged. Set via UI.</td>
</tr>
<tr>
<td>--auto-purge-max-data-age value</td>
<td>Specify an age above which data is automatically purged. This is set in days and the default is seven. Set via UI.</td>
</tr>
<tr>
<td>--auto-purge-period value</td>
<td>The frequency at which the automatic purge occurs. This is set in hours and the default is 24 (daily). Set via UI.</td>
</tr>
<tr>
<td>--log-soft-limit value</td>
<td>A size limit (in MB) for the log directories. If this limit is exceeded the oldest records will be deleted. The default behavior is not to specify a limit (zero).</td>
</tr>
<tr>
<td>--record-soft-limit value</td>
<td>A size limit (in MB) for the record data directories. If this limit is exceeded the oldest data will be deleted. The default behavior is not to specify a limit (zero).</td>
</tr>
<tr>
<td>--enable-config-upload</td>
<td>Enable or disable uploading configuration, overriding the setting specified in the configuration file.</td>
</tr>
<tr>
<td>--disable-config-upload</td>
<td>Set via UI.</td>
</tr>
<tr>
<td>--config-file-limit value</td>
<td>The number of backup configuration files to keep. The default is none. If this is exceeded, the oldest file is deleted.</td>
</tr>
<tr>
<td>--conf &lt;config file&gt;</td>
<td>Specify a configuration file to use.</td>
</tr>
<tr>
<td>--openports</td>
<td>Enable or disable OpenPorts, overriding the setting specified in the configuration file.</td>
</tr>
<tr>
<td>--no-openports</td>
<td>Enable or disable OpenPorts, overriding the setting specified in the configuration file.</td>
</tr>
<tr>
<td>--tcpvcon</td>
<td>Enable or disable Tcpvcon, overriding the setting specified in the configuration file.</td>
</tr>
<tr>
<td>--no-tcpvcon</td>
<td>Enable or disable Tcpvcon, overriding the setting specified in the configuration file.</td>
</tr>
<tr>
<td>--dont-resolve-hostnames</td>
<td>The <code>getInfo</code> method retrieves patch, device, and host information. If no hostname is found then a reverse DNS lookup is performed to determine the hostname. Specify <code>--dont-resolve-hostnames</code> to prevent this.</td>
</tr>
<tr>
<td>--remquery</td>
<td>Enable or disable RemQuery, overriding the setting specified in the configuration file. Set via UI.</td>
</tr>
<tr>
<td>--no-remquery</td>
<td>Enable or disable RemQuery, overriding the setting specified in the configuration file. Set via UI.</td>
</tr>
<tr>
<td>--remquery-timeout value</td>
<td>Specify a timeout value (in seconds) for RemQuery calls. The default is 60 seconds. Set via UI.</td>
</tr>
<tr>
<td>--wmi</td>
<td>Enable or disable WMI, overriding the setting specified in the configuration file. Set via UI.</td>
</tr>
<tr>
<td>--no-wmi</td>
<td>Enable or disable WMI, overriding the setting specified in the configuration file. Set via UI.</td>
</tr>
<tr>
<td>--wmi-timeout value</td>
<td>Specify a timeout value (in seconds) for WMI queries. The default is 120 seconds. Set via UI.</td>
</tr>
</tbody>
</table>

**Testing Windows credentials and communication**

You can test the credentials by using it to discover a Windows machine that you know the user can access. To do this, from a command prompt on the Windows proxy, use the `runas` command to run a Discovery command such as `systeminfo` as the Domain user:

```
C:\> runas /user:DOMAIN\username "systeminfo /S TARGET"
```
Replace **DOMAIN** with the domain name, for example **TIDEWAY**, **username** with the user name, for example discovery, and **TARGET** with the resolvable hostname or IP address.

**Windows proxy downgrade**

If you need to downgrade a Windows proxy, you *must* stop the Windows proxy, uninstall it, and then install the new Windows proxy according to the instructions for that Windows proxy version.

**Adding Windows proxies and proxy pools**

Adding Windows proxies to the appliance enables the appliance to use them for discovering Windows devices.

The appliance and the Windows proxies run CORBA services to communicate using SSL with one another. See **Introduction to Discovery** for more information.

After installing the Windows proxies on the appliance, you must do the following:

1. Add Windows proxy pools. For more information, see **Adding a Windows proxy pool**.
2. Add the proxies to the proxy pools. For more information, see **Adding Windows proxies to proxy pools**.

**Adding a Windows proxy pool**

Adding Windows proxy pools enables the appliance to organize sets of Windows proxies together and balance the proxy load for discovery tasks.

To add a Windows proxy pool, perform the following steps:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Windows Proxies**.
3. Click **Add**.
4. Enter the following information about the new Windows proxy pool:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name that the Windows proxy pool will be referred to in the user interface. This name must be unique. The system validates it to be unique.</th>
</tr>
</thead>
</table>
| IP Range | The IP addresses that the Windows proxy pool can scan. The acceptable values could be any one of the following:  
  • IP address: for example, 10.10.10.3  
  • Range of IP addresses: for example, 10.10.10.* or 10.10.1-5.* or 10.10.0/24  
  • Regular expression: for example, .* or 10.10.10.(23|25) |
| Type | Select the type of the Windows proxy pool. A Windows proxy pool can contain only one type of Windows proxy. The available types are:  
  • Windows Active Directory Proxies  
  • Windows Credential Proxies  
  • Windows Workgroup Proxies |
| Domains | The domain or a space-separated list of domains that the Windows proxy pool will discover. This specifies that the pool is preferred for the discovery of these domains. |

5. Click **Apply**.

The Windows proxy pool is added to the appliance.
You can add multiple Windows proxy pools to the appliance. The Windows proxy pools are displayed in the order (from top to bottom) in which you have added them to the appliance.

**Adding Windows proxies to proxy pools**

Adding Windows proxies to the proxy pools enables the appliance to organize sets of Windows proxies together and balance the proxy load for discovery tasks.

To add a Windows proxy to a Windows proxy pool, perform the following steps:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Windows Proxies**.
3. Click the **Actions** list for the corresponding Windows proxy pool.
4. Select **Add Windows Proxy**.

⚠️ You can add one type of Windows proxy only to a proxy pool of the same type. For example, you can add a credential Windows proxy only to a credential Windows proxy pool.

5. Enter the following information about the new Windows proxy:

<table>
<thead>
<tr>
<th>Proxy pool</th>
<th>Select the Windows proxy pool from the list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name that the Windows proxy will be referred to in the user interface. This name must be unique. The system validates this name to be unique.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the Windows proxy.</td>
</tr>
</tbody>
</table>
| Port        | The port on which to communicate with the Windows proxy.  
  - For AD Windows proxy, the default port number is 4321.  
  - For Workgroup Windows proxy, the default port number is 4322.  
  - For credential Windows proxy, the default port number is 4323. |
| Enabled     | To enable the Windows proxy, select the check box. |

6. Click **Apply**.

The Windows proxy management window displays the new Windows proxy in the corresponding pool.

Each proxy pool displays the Windows proxies in rows. For discovery tasks, the Windows proxy pool checks for a Windows proxy. If a proxy has not previously been used to discover the endpoint, then for each proxy pool (matching the domain) in the order that the pools appear:

- a proxy is selected, and discovery attempts to contact it  
  - if successful then that proxy is used.  
  - if unsuccessful due to a timeout, then other proxies in the pool are tried.
• if unsuccessful due to an error, then no more proxies in the pool are tried and the remaining pools are tried in the order in which they appear.

Managing Windows proxy pools

The appliance enables you to manage the Windows proxy pools from the Edit Windows Proxy Pool page.

To manage a Windows proxy pool:

1. From the secondary navigation bar on the Discovery tab, click Credentials.
2. Click Devices.
3. Click Windows Proxies.
   The Device Credentials page for the Windows proxy pools is displayed.
4. Corresponding to the proxy pool you want to manage, click Actions and select Manage.
   The Edit Windows Proxy Pool page is displayed which has the following two sections:

<table>
<thead>
<tr>
<th>Edit Windows Proxy Pool</th>
<th>Pool contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>This section enables you to change the IP address range and domains associated with the Windows proxy pool. The fields in this section are:</td>
<td>Displays the following information on the contents of the Windows proxy pool:</td>
</tr>
<tr>
<td>• IP Range: The IP addresses that the Windows proxy pool can scan. The acceptable values could be any one of the following:</td>
<td>• Name: Name of the Windows proxy</td>
</tr>
<tr>
<td>• IP address: for example, 10.10.10.3</td>
<td>• Status: Displays whether the Windows proxy is active or not</td>
</tr>
<tr>
<td>• Range of IP addresses: for example, 10.10.10.* or 10.10.1-5.* or 10.10.10.0/24</td>
<td>• Version: Displays the version number of the Windows proxy</td>
</tr>
<tr>
<td>• Regular expression: for example, ..* or 10.10.10.(23</td>
<td>25)</td>
</tr>
<tr>
<td>• Type: Displays the type of the Windows proxy pool.</td>
<td>• If you want to delete the Windows proxy, click Delete.</td>
</tr>
<tr>
<td>• Domains: The domain or a space-separated list of domains that the Windows proxy pool will discover. This specifies that the pool is preferred for the discovery of these domains.</td>
<td>• If you want to ping the Windows proxy, click Ping.</td>
</tr>
<tr>
<td>Apply: To apply any changes that you have made, click Apply.</td>
<td>• Add: If you want to add a new Windows proxy to this pool, click Add.</td>
</tr>
<tr>
<td>For more information about adding a Windows proxy to a pool, see Adding Windows proxies and proxy pools.</td>
<td></td>
</tr>
</tbody>
</table>

Managing Windows proxies

The BMC Atrium Discovery user interface (UI) enables you to manage the Windows proxies. To manage the Windows proxies, you can perform the following:

• view whether a Windows proxy is active or not and the name and version of the proxy service
• view and edit the details used to create the Windows proxy resource (for example, the proxy pool, IP addresses, port, and so on)
• view and edit the proxy settings (for example, setting the log level, recording mode, and timeout values, modifying Discovery methods, flagging overloads, and so on)
You can manage a Windows proxy from the proxy management page. To access the proxy management page, perform the following actions:

1. From the secondary navigation bar on the Discovery tab, click **Credentials**.
2. Click **Devices**.
3. Click **Windows Proxies**.
   
   The Device Credentials page is displayed which contains the Windows proxy pools and the corresponding Windows proxies.
4. To access the proxy management page, perform one of the following actions:
   
   - Click on the Windows proxy name that you want to manage, or
   - Click on the **Actions** list of the corresponding Windows proxy and select **Manage**.
   
   The proxy management page is displayed.

The top section of the proxy management page (following the bread crumb navigation trail and preceding the General Details section) displays the following information:

- **Type**: the Windows proxy type (for example, Active Directory)
- **Version**: the version number of the Windows proxy
  
  The version is displayed on a colored banner. The color of the banner indicates whether a proxy is active or not (for example, a Green banner indicates that the proxy is active). For more information about configuring the colored banner, see [Configuring the banner color](#).

The proxy management page contains the following sections which enable you to view the details of and manage the Windows proxy:

- **General Details**
- **Proxy Settings**
- **Proxy Configuration**

### General Details

This section list the details used to create the Windows proxy. You can manage the following details about the Windows proxy from this section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Pool</td>
<td>The Windows proxy pool for the Windows proxy. If you want to change the Windows proxy pool for the Windows proxy, select from the corresponding proxy pool list. The list is only populated with pools that contain the same proxy type.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The Windows proxy IP address. If you want to change the current IP address, enter the new IP address in the <strong>IP Address</strong> field.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number associated with the Windows proxy. If you want to change the current port number, enter the new port number in the <strong>Port</strong> field.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Displays whether the Windows proxy is enabled or not. You can enable the windows proxy by selecting the checkbox or disable it by clearing the checkbox.</td>
</tr>
</tbody>
</table>

If you have modified any of the general details and want to apply those, click **Apply General Details**.
### Field Name | Details
---|---
**Apply General Details**<br>**Reset General Details**<br>**Proxy Settings**<br>You can manage the following settings of the Windows proxy from this section:<br>**Field Name** | **Details**
---|---
**Log Level**<br>You can change the log level of the Windows proxy at runtime here in the same way as you can for the service log levels from the main Logging page in BMC Atrium Discovery. For more details, see [Changing Log Levels at Runtime](#).<br>The **Log Level** list has the following levels:<br>• Debug: Fine-grained informational events that are most useful to debug an application.<br>• Info: Informational messages that highlight the progress of the application at coarse-grained level.<br>• Warning: Potentially harmful situations.<br>• Error: Error events that may still allow the application to continue running.<br>• Critical: Severe error events that may cause the application to abort.<br><br>**Recording Mode**<br>(8.3 and later proxies only) Displays the recording mode of the Windows proxy. The recording mode can be one of the following:<br>• Record<br>• Playback<br>• None<br><br>**Discovery Methods**<br>(8.3 and later proxies only) Select the discovery methods and their timeouts for the Windows proxy. The available methods are:<br>• WMI<br>• RemQuery

⚠️ If you disable RemQuery, network connection information will not be discovered, and consequently CAM will be unable to model communication.<br><br>**Overload Notification**<br>If you select this option, Windows proxy informs the main Discovery service when it is overloaded (that is, the Windows proxy has a large number of requests in progress). In such a situation, Discovery, if possible, will try another Windows proxy from the same Windows proxy pool. However, if you do not select this option, Discovery will wait for all the requests in progress to complete, which can take a long time if the Windows proxy is overloaded.<br>**Log Directory Disk Usage**<br>Displays the disk usage of the log directory.<br><br>**Display the disk usage of the record directory.**
Field Name | Details
---|---
Record Directory Disk Usage | Enables you to automatically purge stored data for a specific time period for log files and record data. A selection list is displayed which enables you to select the purge date. Once you have selected the time period to purge data from the Windows proxy, select the Log Files checkbox, or Record Data checkbox, or both, and click Apply. The selected data is now set to automatically get deleted on the specified duration. If you want to immediately purge data, select the data (either the Log Files checkbox, or the Record Data checkbox, or both) to delete and click Purge Files Now.

Proxy Configuration

You can view, download, and apply the Windows proxy configuration data from this section.

Field Name | Details
---|---
Retrieve Current Configuration | If you want to view the current Windows proxy configuration in XML format, click View winproxy.conf. The current Windows proxy configuration in the XML format is displayed. If you want to download the Windows proxy configuration in XML format, click (download). You can either choose to open the configuration file with an XML editor or save the file and open it later.

Apply New Configuration | If you want to apply a new Windows proxy configuration file, perform the following:
- Click Browse... and navigate to the new Windows proxy configuration XML file.
- Select the file in the File Upload box and click Open.
- Click Upload Proxy Configuration.

Additional Windows proxy configuration

The following sections detail additional ways you might configure the Windows proxy outside of the user interface.

Proxy port changes in 8.3 SP2

In BMC Atrium Discovery 8.3 SP2, the default port of a proxy can be changes using the Windows proxy manager.
Changing the default port of the proxy

The following sections detail how to change the default port of a Windows proxy.

Changing the default port of an Active Directory Windows proxy

To change the default port (4321) for an Active Directory Windows proxy:

1. Change the registry to configure the proxy to listen to a different port based on your computer type:
   a. For 32-bit computers:
      HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Atrium Discovery\ADProxy\CommandLine
   b. For 64-bit computers:
      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BMC Software\Atrium Discovery\ADProxy\CommandLine
2. Edit the CommandLine value by changing '--port 4321' to the required port.

Changing the default port of a Credential Windows proxy

To change the default port (4323) for a Credential Windows proxy:

1. Change the registry to configure the proxy to listen to a different port based on your computer type:
   a. For 32-bit computers:
      HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Atrium Discovery\Proxy\CommandLine
   b. For 64-bit computers:
      HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BMC Software\Atrium Discovery\Proxy\CommandLine
2. Edit the CommandLine value by changing '--port 4323' to the required port.

Configuring the Appliance for SSL Communications

BMC Atrium Discovery is supplied with keys for secure communications. If your organization’s security policies do not allow keys to be supplied by a third party such as BMC, you will need to replace the keys with your own.

Stopping a Windows proxy from the appliance command line

The tw_terminate_winproxy utility, located in the $TIDEWAY/bin/ directory, sends a request to the Windows proxy to terminate. To use the utility, you must have the discovery/kslave/write permission. When the utility successfully sends a terminate request to a Windows proxy an audit event is logged. The audit event is called windows_proxy_process_terminate and contains the name of the Windows proxy that the terminate request was sent to.

When using the utility, you must always specify a Windows proxy and a user name. Also, if you do not specify a password, you are prompted for one.
Note

If a Windows proxy is not running as either the Local System account or as a member of the Administrators group, `tw_terminate_winproxy` will fail to stop the Windows proxy. The following error is logged in the Windows proxy log file:

```
ERROR: Failed to terminate slave service: [(5, 'OpenSCManager', 'Access is denied.')]  
```

**Workaround:** Allow the user that the Windows proxy is running to stop the service. This is documented on the Microsoft Support Site.

For more information on the utility and the command line options, see `tw_terminate_winproxy`.

**Windows proxy platform minimum specification**

The following specification provides a guide to the minimum recommended specification for the Windows proxy hardware. This specification has been verified on Microsoft Windows 2003 Service Pack 2:

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>3GHz Intel Pentium® 4 CPU 512k Cache</td>
</tr>
<tr>
<td>Memory</td>
<td>2GB</td>
</tr>
<tr>
<td>Hard disk</td>
<td>60GB</td>
</tr>
</tbody>
</table>

**Windows proxies on Windows XP SP2**

A feature introduced in Windows XP SP2 can cause Windows proxies running on that platform to log the following warning in the Windows system log:

```
TCP/IP has reached the security limit imposed on the number of concurrent TCP connect attempts.
```

This means there were more than 10 un-ACKed TCP SYNs in a second (normally from attempting to connect to an invalid address). The patched version of Windows XP interprets this as a potential virus and starts to queue connections. This can cause other network activity on the host to be very slow.

More information on the warning can be found on the Microsoft Support Site.

This feature has also been included in Windows Vista and Service Packs for Windows 2003 Server.

**Configuring Windows NIC discovery**

Windows NIC discovery is configured in the `$TIDEWAY/etc/winproxy.conf` file. There are two sections for each card type:

- a regex to identify the card type
- a lookup list for speed, duplex, and negotiation information
The various adapters are configured in the `<adapters>` section. An annotated excerpt of the `winproxy.conf` file is shown below:

**Adapters section**
The adapters section begins with the `<adapters>` statement

```
<adapters>
```

**Search expression**
The next statement is a regular expression to search for in the adapter key in the registry. This is specified in the `<adapter>` statement.

```
<!-- regex to find the adapter type eg. "^Intel(R) PRO/100" -->
<adapter match="^Intel(R) PRO/100">  
```

The search is performed on the hive "HKLM" and the key `SYSTEM\CurrentControlSet\Control\Class\ {4D36E972-E325-11CE-BFC1-08002BE10318}`

**Search parameter**
You specify the parameter name which in this case is SpeedDuplex.

```
<adapter-key name="SpeedDuplex"/>  
<!-- name in registry key to search for info eg. SpeedDuplex -->
```

The names of some network cards may contain special characters (for example, `"`). For these cards, you must specify the actual attribute. For example:

```
<adapter-key name="SpeedDuplex" actual="*SpeedDuplex"/>
```

While defining the network card name, make sure that the adapter-key name matches with the adapter-map name. In this example, it is SpeedDuplex.

With other network cards you may need to search for different parameter names in the registry key, for example:

```
<adapter match="^Realtek RTL8139 Family PCI Fast Ethernet NIC">  
<adapter-key name="DuplexMode"/>
```
Speed Duplex and Negotiation Determination
The parameter name which you search for returns an integer. The value of the integer represents the particular combination of speed, duplex, and negotiation currently in use on that card. An example, in this case for the SpeedDuplex parameter in the Intel® PRO/100 network card is shown in the Table below.

<table>
<thead>
<tr>
<th>Parameter Value</th>
<th>Speed</th>
<th>Duplex</th>
<th>Negotiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N/A</td>
<td>N/A</td>
<td>AUTO</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
<td>HALF</td>
<td>FORCED</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>FULL</td>
<td>FORCED</td>
</tr>
<tr>
<td>3</td>
<td>100</td>
<td>HALF</td>
<td>FORCED</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>FULL</td>
<td>FORCED</td>
</tr>
</tbody>
</table>

An `<adapter-map ParameterName="value">` statement block is entered for each value expected for the parameter name. Contained in this statement are adapter-value statements with name-value pairs for, in this case, speed, duplex, and negotiation. For example:

```xml
<adapter-map SpeedDuplex="1">
  <adapter-value name="speed" value="10"/>
  <adapter-value name="duplex" value="HALF"/>
  <adapter-value name="negotiation" value="FORCED"/>
</adapter-map>
```

Example Mapping
An example for the Intel® PRO/100 network card is shown below:

```xml
<adapter-key name="SpeedDuplex" actual="*SpeedDuplex"/>
<adapter-map SpeedDuplex="0">
  <adapter-value name="speed" value=""/>
  <adapter-value name="duplex" value=""/>
  <adapter-value name="negotiation" value="AUTO"/>
</adapter-map>
<adapter-map SpeedDuplex="1">
  <adapter-value name="speed" value="10"/>
  <adapter-value name="duplex" value="HALF"/>
  <adapter-value name="negotiation" value="FORCED"/>
</adapter-map>
<adapter-map SpeedDuplex="2">
  <adapter-value name="speed" value="10"/>
  <adapter-value name="duplex" value="FULL"/>
  <adapter-value name="negotiation" value="FORCED"/>
</adapter-map>
<adapter-map SpeedDuplex="3">
  <adapter-value name="speed" value=""/>
  <adapter-value name="duplex" value=""/>
  <adapter-value name="negotiation" value=""/>
</adapter-map>
```

Finally, the adapter and adapters XML statements are closed.

```xml
<adapter>
  <adapter-map SpeedDuplex="4">
    <adapter-value name="speed" value="100"/>
    <adapter-value name="duplex" value="FULL"/>
    <adapter-value name="negotiation" value="FORCED"/>
  </adapter-map>
  <adapter-map SpeedDuplex="6">
    <adapter-value name="speed" value="1000"/>
    <adapter-value name="duplex" value="FULL"/>
    <adapter-value name="negotiation" value="AUTO"/>
  </adapter-map>
</adapter>
</adapters>
```

The Windows proxy configuration file

The Windows proxy is configured using a configuration file (winproxy.conf), which is located at:

C:\Program Files\BMC Software\ADDM Proxy\etc\winproxy.conf

You can download winproxy.conf files from Windows proxies that are connected to your appliance. Any modifications can be made to the file which can then be uploaded to the Windows proxy or to multiple Windows proxies. This simplifies the management of your Windows proxies. See Windows proxy configuration for more information.

The file is divided into the following sections:

- Access methods
- Optional commands
- Commands to run
- Checksum

Access methods

This section is a list of access methods, in the order in which they should be attempted. In this section you can enable or disable an access method. For example:

```xml
<setting name="wmi" enabled="True"/>
```

or
The access methods available are:

- wmi - WMI commands.
- remquery - RemQuery commands.

Optional commands
This section lists the additional executables which are available on the Windows proxy. These are generally tools which are not standard on all versions of Windows, or are third-party supplied tools such as the PSINFO utility described in Windows operating systems. In this section you can enable or disable the optional commands. For example:

```xml
<setting name="tcpvcon" enabled="True/>
```

or

```xml
<setting name="tcpvcon" enabled="False/>
```

Commands to run
This section lists the commands and provides the actual command string that is executed. The commands are referred to by the setting name defined in the previous section. For example:

```xml
<command name="tcpvcon">tcpvcon -anc</command>
```

or

```xml
<command name="tcpvcon">tcpvcon -anc 160</command>
```

Checksum
In this section a checksum is written to ensure that the file has not been tampered with since being copied or uploaded from the appliance.
You can add the checksum without uploading the file using the `tw_sign_winproxy_config` utility. You can then copy the signed file to multiple appliances using ftp or similar.

Example Windows proxy configuration file part

```xml
<slave>

<!-- These settings control the various access methods -->
<setting name="wmi" enabled="True"/>
<setting name="remquery" enabled="True"/>

<!-- These settings control the use of optional commands -->
<setting name="wmi-query-creation" enabled="True"/>
<setting name="openports" enabled="False"/>
<setting name="tcpvcon" enabled="True"/>

<!-- These are the commands that will be run -->
<command name="systeminfo">echo begin wmic_values: && wmic bios get serialnumber 2>&1 && wmic csproduct get uuid 2>&1 && echo end wmic_values: && systeminfo /fo csv /nh</command>
<command name="infocmds">hostname && ver</command>
<command name="ipconfig">ipconfig /all</command>
<command name="tasklist">tasklist /fo csv /nh /v</command>
<command name="netstat">netstat -ano</command>
<command name="netstat">netstat -anc</command>
<command name="openports">openports.exe -netstat</command>
<command name="tcpvcon">tcpvcon.exe -anc</command>

<!-- lputil commands for Emulex HBAs -->
<command name="lputil-listhbas">lputil listhbas</command>
<command name="lputil-count">lputil count</command>

<!-- %s is replaced with the board index number: -->
<command name="lputil-fwlist">lputil fwlist %s</command>

<!-- hbacmd commands for Emulex HBAs -->
<command name="hbacmd-listhbas">hbacmd listhbas</command>
<command name="hbacmd-listhbas">"%ProgramFiles%\HBAnyware\hbacmd" listhbas</command>

<!-- %s is replaced with the WWPN: -->
<command name="hbacmd-hbaattr">hbacmd hbaattrib %s</command>
<command name="hbacmd-hbaattr">"%ProgramFiles%\HBAnyware\hbacmd" hbaattrib %s</command>

<adapters>

<!-- <adapter> may have an optional key attribute (default: name) -->
```
Configuring SNMP credentials

The discovery system will attempt SNMP queries if remote login attempts have not been successful. However, discovery will attempt SNMP queries, but will only use it if the SNMP port (UDP 161) is open on the target host.

You generally do not need to set the SNMP parameters unless you use a read community other than Public. Different SNMP parameters can be set for different host systems.

Discovery using SNMP is supported for hosts (see the Discovery Platforms page for a complete list) if only an SNMP credential is available for the host's IP address. However, SNMP only provides basic host information, running processes, network connections and installed packages. It does not support interrogating files, HBAs or running operating system commands. If a host is discovered using SNMP, Reasoning always checks to see whether a login credential is available for that host as discovered data is richer when a login is achieved. If a login credential is found and used successfully, the host node created using SNMP discovery is updated. In rare cases, duplicate nodes could be created when the host is subsequently discovered using a login credential (for example, this can happen when the IP configuration changes).

Viewing SNMP credentials

To view SNMP credentials:

1. From the secondary navigation bar on the Discovery tab, click Credentials.
2. Click Devices.
3. Click SNMP.

The SNMP credentials page is displayed and the following information is shown for each credential:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>This is the first part of the heading link for the credential and displays the range of IP addresses on which this credential is intended to be used. If you click on this heading link, the Edit SNMP Credential page is displayed. For more information about this page, see #Setting up SNMP credentials. A link is also provided showing the last successful use of the credential. This links to the Discovery Access for that use.</td>
</tr>
<tr>
<td>Description</td>
<td>A free text description of the SNMP credential supplied by the user who created the credential.</td>
</tr>
</tbody>
</table>
The SNMP credentials are checked in sequence, and the first matching entry is used. After a working SNMP credential is found, further credentials are not checked. To reorder SNMP credentials, drag the credential to the required position in the list.

The SNMP credentials are shown in color-coded boxes. The colors represent the level of login success achieved with that credential:

- Green: 100% success rate.
- Yellow: partial success.
- Blue: the credential has never been used.
- Red: 0% success rate.

### Setting up SNMP credentials

To add or edit an SNMP credential, perform the following:

1. From the SNMP credentials page, perform one of the following actions:
   a. To add a new credential, click **Add**.
      The *Create SNMP Credential* page is displayed.
   b. To edit an existing SNMP credential, click **Actions => Edit**.
      The *Edit SNMP Credential* page is displayed.

2. You can then enter the SNMP credential details as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>Enter an IP address, a range of IP addresses, or a regular expression representing the IP addresses for which this credential is valid.</td>
</tr>
<tr>
<td>SNMP Version</td>
<td>The SNMP version to use. From the SNMP version list, select one of the following: 1, 2c, or 3. The default is Version 2c. Note that if you are setting up credentials for discovering Netware, you must select Version 1 from the SNMP version list.</td>
</tr>
<tr>
<td>SNMP v1/v2c</td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td>Community used for SNMP read access to the defined host(s). For SNMP V1 and V2c credentials only.</td>
</tr>
</tbody>
</table>
### Field Name | Details
--- | ---
**SNMP v3** |  
**Username** | For SNMP V3 credentials only.  
**Security Level** | For SNMP V3 credentials only. Shows the security level selected using the authentication and privacy protocols.  
- noAuthNoPriv: no authentication and no privacy.  
- authNoPriv: authentication, no privacy.  
- authPriv: authentication and privacy.  
  Note that there is no setting for privacy without authentication.  
**Authentication Protocol** | The protocol used to encrypt the authentication with the client. For SNMP V3 credentials only. Select one of the following from the drop down list:  
- None: no encryption used. Operates in the same way as v1 and v2.  
- MD5: an authentication passphrase is entered and MD5 hashed. The MD5 hashed passphrase is used to access the target system.  
- SHA: an authentication passphrase is entered and SHA hashed. The SHA hashed passphrase is used to access the target system.  
**Authentication Key** | The key (passphrase) which will be used to encrypt the credentials. For SNMP V3 credentials only, and only if you have chosen an authentication protocol. Must be at least 8 characters.  
**Privacy Protocol** | The protocol used to encrypt data retrieved from the target. Encrypting the data retrieved from a discovery target causes performance degradation over no encryption. This is for SNMP V3 credentials only, and only if you have chosen an authentication protocol. That is, you cannot have privacy without authentication. Select one of the following from the drop down list:  
- None: no data encryption is used. Operates in the same way as v1 and v2.  
- DES: uses a privacy key to encrypt data using the DES algorithm.  
- AES CFB128: uses a privacy key to encrypt data using the AES algorithm.  
**Private key** | The key (passphrase) which will be used to encrypt the data. For SNMP V3 credentials only, and only if you have chosen a privacy protocol. Must be at least 8 characters.  
**General** |  
**Description** | A free-text description of this SNMP credential.  
**Retries** | The number of attempts made if no response is received. The default is five.  
**Timeout** | The time (in seconds) in which a response is expected. The default is one second.  
**Custom SNMP Port** | To choose a custom SNMP port, select the checkbox and choose from the ports in the list. You must already have configured a custom SNMP port in the Discovery Configuration window.

3. Click **Apply**.  
The SNMP Credentials page is refreshed to show details of the new credentials.

**SNMP v3 permissions**

When SNMP v3 is used to discover a device that uses different security contexts for different instances of a MIB (in the same way that community string indexing is used for v1 or v2), the SNMP v3 user may not have access to the different security contexts.
If a device is discovered where access to different contexts is required, but access has not been granted to the user, discovery will gather less information and topology discovery may not be complete. A ScriptFailure node will be associated with the DeviceInfo for the DiscoveryAccess, with a message of the type, Failed to access vlan-1 (AuthorizationError), where vlan-1 is the name of the security context that discovery attempted to access.

To ensure discovery has full access, the user should be granted access to all of the contexts on the network device. For example, to grant access to all contexts to the group privgroup on a Cisco device with a recent version of IOS, you can use this configuration command:

```
snmp-server group privgroup v3 auth context vlan- match prefix
```

You should consult your device's documentation or manufacturer for more details.

**Testing SNMP credentials**

When you have added the credentials, you should test them to ensure that they work by performing the following actions:

1. Click **Actions => Test** for the SNMP credential.
   A dialog box is displayed with the credential values, and a field in which you enter the IP address against which to test the credential.
2. Enter the target IP address to test.
3. Click **Test**.
   The page is refreshed to show that the test in progress and when complete, the results are shown on the Credential Tests page; this may take a few minutes.

Repeat the preceding steps for all the credentials you want to test.

**Configuring vCenter credentials**

VMware vCenter Server provides centralized management of VMware vSphere (ESX and ESXi) virtual machines.

BMC Atrium Discovery can discover ESX and ESXi hosts through the vSphere web services API, or a fallback to an ssh login. However, if a host is being managed by vCenter and it is put into **lockdown mode**, these discovery techniques are disabled and access is only available through the vCenter server managing it.

**vCenter credentials are not host credentials**

The vCenter credentials that you enter in this page are only used for the vCenter server. Unmanaged, or ESX and ESXi instances that have not been put into **lockdown mode** can be discovered using VMware vSphere credentials.
Viewing vCenter credentials

To view existing vCenter credentials:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Devices**.
3. Click **vCenter**.

The vCenter Credentials page is displayed and the following information is shown for each credential:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential link</td>
<td>A heading link describing the credential. This consists of the following three parts: <strong>Credential name</strong>: the name of the credential. <strong>IP range</strong>: the IP address or addresses of the vSphere (ESX and ESXi) targets that may be managed by the vCenter server. <strong>Username</strong>: the username used to access the vCenter server. Note that this is <strong>not</strong> a credential for the vSphere (ESX and ESXi) targets, but the vCenter server. If you click on this heading link, the <strong>Edit vCenter Credential</strong> page is displayed. For more information about this page, see #Setting up vCenter credentials below.</td>
</tr>
<tr>
<td>Description</td>
<td>A free text description of the vCenter server credential supplied by the user who created the credential.</td>
</tr>
<tr>
<td>vCenter IP address</td>
<td>The IP address of the vCenter server.</td>
</tr>
<tr>
<td>Usage</td>
<td>A summary of the success rate when the credential has been used, information on failures, and links to <strong>Discovery Accesses</strong>, credential lists and other useful diagnostic pages.</td>
</tr>
<tr>
<td>Actions</td>
<td>A drop down menu with the following options: <strong>Edit</strong>: Select this to edit the credential. The <strong>Edit vCenter Credential</strong> page is displayed. See #Setting up vCenter credentials for information on the fields and settings available from this page. <strong>Delete</strong>: Select this to delete the credential. <strong>Test</strong>: Select this to test the credential. For more information, see #Testing vCenter credentials. <strong>Move to top</strong>: moves the credential to the top of the list. <strong>Move to bottom</strong>: moves the credential to the bottom of the list.</td>
</tr>
</tbody>
</table>

The vCenter credentials are checked in sequence, and the first matching entry is used. After a working vCenter credential is found, further credentials are not checked. To reorder vCenter credentials, drag the credential to the required position in the list.

The vCenter credentials are shown in color-coded boxes. The colors represent the level of login success achieved with that credential:

- **Green**: 100% success rate.
- **Yellow**: partial success.
- **Blue**: the credential has never been used.
- **Red**: 0% success rate.
Setting up vCenter credentials

⚠️ vCenter credentials entered using the Devices tab

A vCenter credential button is also available on the Management System tab. This is a holder for credentials provided by the vCenter DIP provider. These credentials are populated when patterns containing vSphere queries are activated.

You can manually add vCenter credentials from the Management System tab. However, the recommended procedure to add or edit vCenter credentials is from the Devices tab as it is a lot simpler. If you edit a vCenter credential on the Devices tab, the same changes are reflected in that credential on the Management System tab.

To add or edit a vCenter credential, perform the following:

1. From the vCenter credentials page, perform one of the following actions:
   a. To add a new credential, click Add.
      The Create vCenter Credential page is displayed.
   b. To amend an existing credential, click Actions => Edit.
      The Edit vCenter Credential page is displayed.
2. You can then enter the vCenter credential details as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
| IP Range        | The IP address or addresses of the vSphere (ESX and ESXi) targets that may be managed by the vCenter server.  
                 **IP address**: for example, 10.10.10.3  
                 **Range of IP addresses**: 10.10.10.* or 10.10.1-5.* or 10.10.0/24  
                 **Regular expression**: .* or 10.10.10.(23|25) |
| Name            | The name used to identify the connection.  
                 It may contain only letters, numbers, and underscores and must begin with a letter or underscore. |
| Username        | Username used to access the vCenter server. Note that this is not a credential for the target host, but the vCenter server. The permission level required is read-only. |
| Password        | The corresponding password.  
                 In the Edit vCenter Credential page, this field is displayed as Set Password. When editing a credential, the password is shown as a series of asterisks in this field and it cannot be edited. To enter a new password, select the checkbox. The password entry field is cleared. Enter the password into the password entry field; the password text is not echoed to the screen. |
| vCenter IP Address | The IP address of the vCenter server managing the vSphere (ESX and ESXi) targets. |
| Port            | To choose a custom HTTPS port, choose from the ports in the list. You must already have configured a custom HTTPS port in the Discovery Configuration window. |
| Timeout         | The time (in milliseconds) in which a response is expected. The default is 60 seconds. |
| Description     | A free-text description of this login credential. |
3. Click **Apply**.
   The vCenter credential page is refreshed to show details of the new credentials.

**Testing vCenter credentials**

When you have added the credentials, you should test them to ensure that they work by performing the following actions:

1. Click **Actions** => **Test** for the vCenter credential.
   A dialog box is displayed with the valid IP range, vCenter IP address, description, and username pre-populated.
2. Enter the target IP address to test. This is the IP address of a vSphere (ESX and ESXi) target, *not* the vCenter server.
3. Click **Test**.
   The page is refreshed to show that the test in progress and when complete, the results are shown on the *Device Credentials* page; this may take a few minutes.
4. Repeat this for all the credentials you want to test.

**Configuring vSphere credentials**

---

**Unpatched VMware vSphere known problems**

Unpatched versions of VMware vSphere have known problems when scanned by various tools. BMC Software strongly recommends that you apply the appropriate patches to affected systems. There is more information on this issue on the following Configipedia link.

---

The VMware vSphere API is used to discover VMware ESX and ESXi systems. Where the vSphere API cannot be accessed, discovery falls back to an ssh login to access the underlying Linux operating system.

---

**vSphere credentials are not host credentials**

The vSphere credentials that you enter in this page are only used for the vSphere API. If this is not accessible and ssh discovery is attempted, a separate host login credential for the endpoint is required.

---

**Viewing vSphere credentials**

To view existing vSphere credentials:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **vSphere**.

The vSphere credentials page displays the following information for each credential:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Range</td>
<td>This is the first part of the heading link for the credential and displays the range of IP addresses on which this credential is intended to be used. If you click on this heading link, the Edit vSphere Credential page is displayed. For more information about this page, see #Setting up vSphere credentials. A link is also provided showing the last successful use of the credential. This links to the Discovery Access for that use.</td>
</tr>
<tr>
<td>Description</td>
<td>A free text description of the vSphere credential supplied by the user who created the credential.</td>
</tr>
<tr>
<td>Usage</td>
<td>A summary of the success rate when the credential has been used, information on failures, and links to DiscoveryAccesses, credential lists and other useful diagnostic pages.</td>
</tr>
</tbody>
</table>
| Actions   | A drop down menu with the following options:  
**Edit**: Select this to edit the credential. See #Setting up vSphere credentials for information on the fields and settings available from this page.  
**Delete**: Select this to delete the credential.  
**Test**: Select this to test the credential. For more information, see #Testing vSphere credentials.  
**Move to top**: moves the credential to the top of the list.  
**Move to bottom**: moves the credential to the bottom of the list. |

The credentials are checked in sequence, and the first matching entry is used. After a working credential is found, further credentials are not checked. If you want to reorder login credentials, drag the credential to the required position in the list.

The vSphere credentials are shown in color coded boxes. The colors represent the level of login success achieved with that credential:

- **Green**: 100% success rate.
- **Yellow**: partial success.
- **Blue**: the credential has never been used.
- **Red**: 0% success rate.

### Setting up vSphere credentials

⚠️ **vSphere credentials entered using the Devices tab**

A vSphere credential button is also available on the Management System tab. These credentials are populated when patterns containing vSphere queries are activated. You can manually add vSphere credentials from the Management System tab. However, the recommended method to add or edit vSphere credentials is from the Devices tab. If you edit a vSphere credential on the Devices tab, the same changes are reflected in the credential on the Management System tab.

To add or edit a vSphere credential:

1. From the vSphere credentials page, perform one of the following actions:
   a. To add a new credential, click **Add**.
To amend an existing credential, click **Actions > Edit**.

**2.** You can enter the vSphere credential details as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
| IP Range   | Enter an IP address, a range of IP addresses, or a regular expression representing the IP addresses for which this credential is valid.  
  **IP address:** for example, 10.10.10.3  
  **Range of IP addresses:** 10.10.10.* or 10.10.1-5.* or 10.10.10.0/24  
  **Regular expression:** .* or 10.10.10.(23|25) |
| Name       | The name used to identify the connection.  
  It may contain only letters, numbers, and underscores and must begin with a letter or underscore. |
| Username   | Username used to access the vSphere API. See #Required vSphere privileges for information on the privileges required. |
| Password   | The corresponding password.  
  When editing a credential, the password is shown as a series of asterisks in this field and it cannot be edited. To enter a new password, select the checkbox. The password entry field is cleared. Enter the password into the password entry field; the password text is not echoed to the screen. |
| Port       | To choose a custom HTTPS port, choose from the ports in the list. You must already have configured a custom HTTPS port in the Discovery Configuration window. |
| Timeout    | The time (in milliseconds) in which a response is expected. The default is 60 seconds. |
| Description| A free-text description of this login credential. |

**3.** Click **Apply**.  
The vSphere credential page is refreshed to show details of the new credentials.

**Required vSphere privileges**

The minimum privilege required to use the vSphere API for discovery is the **System.View** privilege. This is given by default to all users who can log in, including read only users.

**Privileges in the VMwareVM.VMwareVSphereLicenseDetail pattern**

The **VMwareVM.VMwareVSphereLicenseDetail** pattern requires additional privileges to gain complete information. This pattern requires access using a credential with the **Global.Licenses** privilege. Without this, the license key information will either be partially (if discovered via vCenter) or fully (if discovered via vSphere) redacted.

<table>
<thead>
<tr>
<th>Privilege and discovery method</th>
<th>Returned key information</th>
</tr>
</thead>
<tbody>
<tr>
<td>With <strong>Global.Licenses</strong> privilege</td>
<td>30DCK--DUMMY--KEY!!--DUMMY--911F0</td>
</tr>
<tr>
<td>vCenter with <strong>System.View</strong> privilege</td>
<td>30DCK--#####--#####--#####--911F0</td>
</tr>
<tr>
<td>Direct (vSphere) with <strong>System.View</strong> privilege</td>
<td>XXXXX--XXXXX--XXXXX--XXXXX--XXXXX--XXXXX</td>
</tr>
</tbody>
</table>

The same information is returned by the VMware client when accessing the target using the same methods and privileges.
Testing vSphere credentials

When you have added the credentials, you should test them to ensure that they work by performing the following actions:

1. Click Actions > Test for the vSphere credential.
   A dialog box is displayed with the the credential values, and a field in which you enter the IP address against which to test the credential.
2. Enter the target IP address to test.
3. Click Test.
   The page is refreshed to show that the test in progress and when complete, and the results are shown on the Device Credentials page (this may take a few minutes).
4. Repeat this for all the credentials you want to test.

Testing credentials

The credential test page

You can test discovery credentials using the Credential Tests page. To access this page:

1. From the secondary navigation bar on the Discovery tab, click Credentials.
2. Click Devices.
3. Click Credential Tests.
   The Credential Tests page is displayed.

The Credential Tests page displays the credential tests that are currently in progress and the tests run in the last ten minutes. You can delete completed tests, or run them again. However, you cannot cancel tests that are currently in progress. You can also test whether credentials exist for any IP address on your network.

- To delete a credential test, in the Actions list of that test, click Delete.
- To run a credential test again, in the Actions list of that test, click Retry.

Testing credentials for an arbitrary IP Address

You can test whether BMC Atrium Discovery can access any IP address on your network. You do not need to have previously scanned the IP address.

This way you can see whether any of your existing credentials or Windows proxies will allow you to access this IP.
1. From the Credential Test page, click **Test IP Access** at the bottom right corner of the page.
2. In the Test IP Access dialog box, enter the IP address for which you want to test credentials.
3. Click **Test**.
   The Test Credentials Page is displayed showing the test in progress.
4. When the test completes, the page is refreshed with the result.
   You are shown whether the test ultimately resulted in a success or a failure. By clicking through the state link you can view the results of the credential test in more detail.

```
Test result for arbitrary IP address.
```

5. For ssh credentials, a verbose session log is displayed.
   To view the session log, click the show session log link.

The credential test results page shows you all the credentials, access methods and Windows proxies that were tried during the test, and which failed (if any). As would happen during a normal discovery, BMC Atrium Discovery continues until either a successful access is obtained, or it runs out of methods to try.

**Testing existing login credentials from the Host page**

You can test existing login credentials when viewing a host's details.

1. From a Host page, click **Actions**.

```
Testing credentials from the host page.
```

2. Click **Test Discovery Credentials**.
   The results are displayed; this may take a few minutes.

```
⚠️ If you do not have the correct credentials, a message will be displayed to this effect. If this occurs you must exit the test and select another host or configure an appropriate credential.
```

**User privileges and information access**

This chapter contains information on the type of information discovered by users with varying access privileges from different operating systems. It contains the following sections:
• **UNIX and related operating systems**: describes the information categories discovered for different user privileges on Unix systems.

• **Windows operating systems**: describes the information categories discovered for different user privileges on Windows systems.

• **Windows proxy permissions**: describes the information that is retrieved for different levels of permissions granted to the Windows proxy.

• **The Windows proxy configuration file**: describes the `winproxy.conf` file that is used to configure Windows proxies.

**Windows operating systems**

**Windows discovery notes**

This section provides some useful notes on discovering Windows hosts.

**Potential user lock out**

By default AD accounts have a limited number of login attempts (for example, three attempts in fifteen minutes). Access Denied errors from WMI, DCOM, and RemQuery are counted as unsuccessful login attempts. Where target hosts are incorrectly configured, this limit can be exceeded and the account locked out.

To avoid this, configure the Discovery account to accept unlimited login attempts.

**Firewalls**

Some versions of Windows have a default firewall configuration that does not permit discovery. You should configure the firewall to permit access otherwise you will be unable to discovery your Windows hosts. See **Discovery communications** for information on the ports that should be open.

---

**Credential Windows proxy user**

You should not run the Credential Windows proxy as the Local System user, but as a valid user account, which should be in the Administrators group. Using a local system account on a domain network may result in system problems.

**Windows Vista and Windows 7**

The account being used to discover the target host must be one of the following:

- A domain user with Administrator privileges on the target host.
- A non-domain user with Administrator privileges and with remote UAC disabled on the target host.

**Windows Server 2008 and Windows Server 2008 R2**

The account being used to discover the target host must be one of the following:

- A domain user with Administrator privileges on the target host.
- A non-domain user with Administrator privileges and with remote UAC disabled on the target host.

**Windows 2012 Server**
You must have the June 2012 or later TKU installed. The account being used to discover the target host must be one of the following:

- A domain user with Administrator privileges on the target host.
- A non-domain user with Administrator privileges and with remote UAC disabled on the target host.

**Windows Server 2003 Standard Edition Domain Controller**

**Windows 2000 and Windows NT**

⚠️ **getServices method requires WMI**

In Windows 2000 and Windows NT the `sc.exe` executable is not provided. The getServices method requires WMI to run successfully.

**Windows discovery commands**
The following table show the commands that are run on Windows platforms. The following methods are used:

- **WMI**: Windows Proxies use Windows Management Instrumentation (WMI) as the primary means of discovery. Discovery uses both WMI queries and WMI registry access.
- **RemQuery**: If WMI does not succeed, the Proxies use various command line tools via the RemQuery utility. When it is used, it is copied onto the admin$ share of the scanned host, installed and started as a service. The service is then used to execute the discovery scripts. At the end of the scan, the service is stopped and uninstalled, but the executable is left in the admin$ share. If a copy already exists, it is not copied again.
- **Shell scripts**: These discovery scripts are ONLY used for Windows Discovery via a shell session (ssh or telnet).
- **SNMP**: SNMP discovery is supported for all devices with an accessible SNMP agent. Discovery supports SNMP v1, v2c and v3. For some older platforms (e.g. Netware) the use of SNMP v1 may be required. This is defined on a per-credential basis. Note that only read (GET, GETNEXT, GETBULK) access is required.

**WMI**
<table>
<thead>
<tr>
<th>Method</th>
<th>Notes</th>
<th>WMI Namespace</th>
<th>WMI Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo'</td>
<td>Handled by getHostInfo call</td>
<td></td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td></td>
<td>root\CIMV2</td>
<td>ASSOCIATORS OF (Win32_Directory='\path') WHERE ResultClass = CIM_LogicalFile</td>
</tr>
<tr>
<td>getFileSystems</td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_LogicalDisk WHERE DriveType = 3 or DriveType = 4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_LogicalDiskToPartition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\WMI</td>
<td>SELECT * FROM MSFC_FCAdapterHBAAttributes</td>
</tr>
<tr>
<td>getHBAInfo</td>
<td></td>
<td>root\WMI</td>
<td>SELECT * FROM MSFC_FibrePortHBAAttributes</td>
</tr>
<tr>
<td>getHostInfo'</td>
<td>This query must succeed.</td>
<td>root\CIMV2</td>
<td>SELECT Name, Manufacturer, Model, Domain, SystemType FROM Win32_ComputerSystem</td>
</tr>
<tr>
<td></td>
<td>Optional, This query may fail.</td>
<td>root\CIMV2</td>
<td>SELECT Workgroup FROM Win32_ComputerSystem</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT DNSDomain FROM Win32_NetworkAdapterConfiguration WHERE IPEnabled = 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT SystemUpTime FROM Win32_PerfFormattedData_PerfOS_System</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT Capacity FROM Win32_PhysicalMemory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT SerialNumber FROM Win32_BIOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT Vendor, IdentifyingNumber, Name, UUID FROM Win32_ComputerSystemProduct</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_Processor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT HotFixID, ServicePackInEffect FROM Win32_QuickFixEngineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\default:StdRegProv</td>
<td>HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0-MHz</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td></td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_NetworkAdapterConfiguration</td>
</tr>
<tr>
<td></td>
<td>Optional, This query may fail.</td>
<td>root\WMI</td>
<td>SELECT * FROM MSNdis_LinkSpeed</td>
</tr>
<tr>
<td>getPackageList</td>
<td>See notes below.</td>
<td>root\default:StdRegProv</td>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\DisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\default:StdRegProv</td>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\QuietDisplayName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>root\default:StdRegProv</td>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\HiddenDisplayName</td>
</tr>
<tr>
<td>Method</td>
<td>WMI Namespace</td>
<td>WMI Query</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>---------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td>root\default: StdRegProv</td>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\DisplayVersion</td>
<td></td>
</tr>
<tr>
<td></td>
<td>root\default: StdRegProv</td>
<td>HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall*\Publisher</td>
<td></td>
</tr>
<tr>
<td>getPatchList</td>
<td></td>
<td>Handled by getHostInfo call, specifically:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SELECT HotFixID, ServicePackInEffect FROM Win32_QuickFixEngineering</td>
<td></td>
</tr>
<tr>
<td>getProcessList Calls getOwner() on each WMI object returned.</td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_Process</td>
<td></td>
</tr>
<tr>
<td>getRegistryListing Registry keys are passed directly to the standard registry provider.</td>
<td>root\default: StdRegProv</td>
<td>%key%</td>
<td></td>
</tr>
<tr>
<td>getRegistryValue Registry values are passed directly to the standard registry provider.</td>
<td>root\default: StdRegProv</td>
<td>%key%</td>
<td></td>
</tr>
<tr>
<td>getServices</td>
<td>root\CIMV2</td>
<td>SELECT * FROM Win32_Service</td>
<td></td>
</tr>
</tbody>
</table>

*indicates methods that must succeed for a Host to be created

getPackageList

Package information is obtained by walking these registry keys described in the table above rather than using Win32_Product as it provides more reliable data.

In order to speed this process up, a temporary WMI class is created on the remote machine to query the registry locally. This temporary class is given a unique name and is removed once the registry data has been retrieved.

getHBAInfo

WMI support for gathering HBA information uses the following queries to populate the HBA information if it is safe to do so:

```
SELECT * FROM MSFC_FCAdapterHBAAttributes
SELECT * FROM MSFC_FibrePortHBAAttributes
```

The OS version and patch list is checked to see whether HBA queries are safe. On Microsoft Windows Server 2003, Vista, and Server 2008 the HBAAPI.DLL module used by WMI leaks handles unless patched with KB957052. If this patch is not installed, no WMI requests are made.

By inspection, no current version of Windows 2003 (5.2.x) or Windows 2008 (6.0.x) has this patch included (current versions including service packs) but Windows 2008 R2 (6.1.x) has. It is not clear whether the problem exists on Windows 2000, though there is no patch available.
We make the following assumptions:

- Windows 2000 HBA queries are safe via WMI.
- Newer versions of Windows do not have the bug.
- This check is unnecessary when running `FCINFO.EXE`. This does use `HBAAPI.DLL` and could experience the same handle leak, but is a short lived process and they are cleared on exit.

The Microsoft `FCINFO.EXE` command line tool is also used by RemQuery. This is used where WMI is deemed unsafe (or has failed for some reason). This provides equivalent information on HBAs since it uses the same API as the WMI provider.

**RemQuery**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>Handled by getHostInfo call.</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>REMQUERY DIR /-C /TW /4 %path%</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>Handled by getFileInfo call.</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td>REMQUERY CMD /C DIR /-C /TW /4 %path%</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REMQUERY CMD /C TYPE %path%</td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>REMQUERY CMD /C DIR /-C /TW /4 %path%</td>
<td></td>
</tr>
<tr>
<td>getHBAInfo</td>
<td>REMQUERY FCINFO /DETAILS</td>
<td>Requires Microsoft <code>FCINFO.EXE</code> to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY HBACMD LISTHBAS</td>
<td>Requires Emulex HBAnywhere to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY HBACMD HBAATTRIB % wwpn%</td>
<td>Requires Emulex HBAnywhere to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY LPUTIL LISTHBAS</td>
<td>Requires Emulex LPUTIL.EXE to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY LPUTIL COUNT</td>
<td>Requires Emulex LPUTIL.EXE to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY LPUTIL FWLIST % board_id%</td>
<td>Requires Emulex LPUTIL.EXE to be installed on the target system.</td>
</tr>
<tr>
<td>getHostInfo*</td>
<td>REMQUERY WMI BIOS GET SERIALNUMBER</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REMQUERY WMI CSPRODUCT GET UUID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REMQUERY SYSTEMINFO /fo csv /nh</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REMQUERY &quot;HOSTNAME &amp; &amp; VER&quot;</td>
<td></td>
</tr>
</tbody>
</table>
### Method Script Notes

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>getInterfaceList</td>
<td>REMQUERY IPCONFIG /ALL</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>REMQUERY NETSTAT -ano</td>
<td></td>
</tr>
<tr>
<td></td>
<td>REMQUERY NETSTAT -an</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>REMQUERY NETSTAT</td>
<td>Uses Windows API to request same registry keys as WMI Queries.</td>
</tr>
<tr>
<td>getPatchList</td>
<td>REMQUERY NETSTAT</td>
<td>Handled by getHostInfo call.</td>
</tr>
<tr>
<td>getProcessList</td>
<td>REMQUERY NETSTAT</td>
<td>Uses Windows API to query process information.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY TASKLIST /fo /csv /nh /v</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>REMQUERY TCPVCON -ano</td>
<td>Requires TCPVCON.EXE to be installed on the target system.</td>
</tr>
<tr>
<td></td>
<td>REMQUERY OPENPORTS -netstat</td>
<td>Optional, must be enabled in the Proxy configuration. Requires OPENPORTS.EXE to be installed on the target system.</td>
</tr>
<tr>
<td>getRegistryListing</td>
<td>REMQUERY REG QUERY %hive%%key%</td>
<td></td>
</tr>
<tr>
<td>getRegistryValue</td>
<td>REMQUERY REG QUERY %hive%%key% /v %value%</td>
<td></td>
</tr>
<tr>
<td>getServices</td>
<td>REMQUERY SC QUERYEX state= all</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates methods that must succeed for a Host to be created.

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>systeminfo-device</td>
</tr>
<tr>
<td>infocmds-device</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>dir</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
</tr>
<tr>
<td>getFileInfo</td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>systeminfo-host</td>
</tr>
<tr>
<td>infocmds-host</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ipconfig</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat-o</td>
</tr>
<tr>
<td>openports-netstat</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>Script</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>getPatchList</td>
<td>systeminfo-patchlist</td>
</tr>
<tr>
<td>getProcessList</td>
<td>tasklist</td>
</tr>
<tr>
<td></td>
<td>tlist</td>
</tr>
<tr>
<td></td>
<td>pulist</td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>tcpvcon</td>
</tr>
<tr>
<td></td>
<td>openports</td>
</tr>
</tbody>
</table>

*indicates methods that must succeed for a Host to be created.

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td></td>
<td>LanMgr-Mib-II-MIB::domPrimaryDomain.0</td>
<td>1.3.6.1.4.1.77.1.4.1.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask]</td>
<td>[.1, .2, .3]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td>[ifIndex, ifDescr, ifSpeed, ifPhysAddress]</td>
<td>[.1, .2, .5, .6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>[tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress,</td>
<td>[.1, .2, .3, .4, .5]</td>
</tr>
<tr>
<td></td>
<td>tcpConnRemPort]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td>[udpLocalAddress, udpLocalPort]</td>
<td>[.1, .2]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td>[hrSWInstalledName]</td>
<td>[.2]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
<tr>
<td></td>
<td>[hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters]</td>
<td>[.1, .2, .4, .5]</td>
</tr>
</tbody>
</table>

*indicates methods that must succeed for a Host to be created.
Windows proxy permissions

This document describes the user permissions required by the Windows proxy to obtain information from target Windows hosts for each discovery method available to the Windows proxy. The discovery methods are:

- WMI
- RemQuery

For each of the discovery methods, different levels of permissions are defined and the corresponding effect on the discovery function calls is described.

The permissions are defined in sets, with the first set being the minimal set of permissions required by a normal (non-administrator) user for the discovery method to return any data. Subsequent permission sets build on the minimal permission set so that more data can be retrieved. The last permission set is for accessing the target machine as an administrator user. In each case, OK means that the all possible information for that function is retrieved. Not available means that no information can be retrieved for that function.

The permissions defined in the permissions sets are:

- DCOM: Configuring DCOM for remote access
- WMI: Granting permissions on a WMI namespace
- User Rights: Granting system privileges
- Remote Registry: Granting access to the Remote Registry service

Windows NT 4.0 discovery targets have not been considered in this section.

WMI Access and discovery behavior

<table>
<thead>
<tr>
<th>Permission set</th>
<th>getDeviceInfo</th>
<th>getHostInfo</th>
<th>getDirectoryListing</th>
<th>getFileSystems</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (minimal)</td>
<td>No CPU</td>
<td>OK</td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>OK</td>
<td>OK</td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>OK</td>
<td>OK</td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>OK</td>
<td>OK</td>
<td>Not available</td>
<td></td>
</tr>
<tr>
<td>5 (administrator)</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permission set</th>
<th>getHBAInfo</th>
<th>getInterfaceList</th>
<th>getPackageList</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (minimal)</td>
<td>Not available</td>
<td>No speed/negotiation</td>
<td>Not available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No msndis_link_speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No manufacturer</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Not available</td>
<td>No msndis_link_speed</td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No manufacturer</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Not available</td>
<td>No manufacturer</td>
<td>OK</td>
</tr>
<tr>
<td>Permission set</td>
<td>getHBAInfo</td>
<td>getInterfaceList</td>
<td>getPackageList</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>4</td>
<td>Not available</td>
<td>No manufacturer</td>
<td>OK</td>
</tr>
<tr>
<td>5 (administrator)</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permission set</th>
<th>getProcessList</th>
<th>getRegistryListing</th>
<th>getRegistryValue</th>
<th>getServices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (minimal)</td>
<td>No arguments</td>
<td>No command path</td>
<td>No user name</td>
<td>Not available</td>
</tr>
<tr>
<td>2</td>
<td>No arguments</td>
<td>No command path</td>
<td>No user name</td>
<td>OK</td>
</tr>
<tr>
<td>3</td>
<td>No arguments</td>
<td>No command path</td>
<td>No user name</td>
<td>OK</td>
</tr>
<tr>
<td>4</td>
<td>No user name</td>
<td>OK</td>
<td>OK</td>
<td>Not available after Windows 2003 SP1</td>
</tr>
<tr>
<td>5 (administrator)</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td></td>
</tr>
</tbody>
</table>

**WMI access permission set definitions**

<table>
<thead>
<tr>
<th>Permission Set</th>
<th>Details</th>
</tr>
</thead>
</table>
| 1             | DCOM: Remote access enabled  
WMI: Root\CIMV2 namespace: Remote Enable, Account Enable |
| 2             | As 1 plus:  
WMI: Root\Default namespace: Remote Enable, Account Enable, Execute Methods |
| 3             | As 2 plus:  
WMI: Root\WMI namespace: Remote Enable, Account Enable |
| 4             | As 3 plus:  
User Rights: Debug programs privilege granted |
| 5             | Access as a member of the Administrators group, for example, to scan a Domain Controller, use Domain Controller credentials. |

**Notes**

- `getNetworkConnectionList` is not available using WMI.
- The NIC manufacturer cannot be retrieved by a non-administrator because the Plug and Play Manager is queried and there is no way to grant a non-administrator access to this.
- The user name for a process cannot be retrieved by a non-administrator user.
- A user assigned the `Debug programs` user right can take control of the operating system, which is a security risk.
- An error is written in the Windows proxy's log when discovering a Windows 2003 machine as non-administrator. For example:

This does not lead to any missing information because a different method is then used to retrieve the system’s uptime. If the error is a problem, the user can be assigned to the "Performance Monitor Users" group, which allows this WMI query to succeed.

RemQuery access and discovery behavior
The RemQuery utility cannot be run as a non-administrator user. This is because you can only create a service as administrator, which RemQuery needs to do after copying its service to the ADMIN$ share on the remote machine.

Granting permissions
The following sections list possible ways to grant the various permissions required to a user. This should be seen as a guide only.

Setting DCOM permissions
This section describes three methods to grant remote DCOM permission to a user. This is only required for discovery targets running XP SP2 or later or 2003 SP1 or later.

Method 1
Add the user to the Distributed COM Users group. This group was made available in Windows 2003 SP1.

Method 2
Use Group Policy Objects in an Active Directory environment to grant the permission; this is described in this Microsoft article.

Method 3
Use the following steps to configure DCOM permissions on a machine:

1. Select Start => Run, enter dcomcnfg and click OK - this launches the Component Services configuration GUI.
2. Expand Console Root => Component Services => Computers => My Computer.
3. Right-click My Computer and select Properties.
4. Go to the COM Security tab.
5. In the Launch and Activation Permissions section, click Edit Limits....
6. Click Add.
7. Enter your domain user name or group name in the text entry field and click Check Names.
8. Click OK.
9. Set the permissions for the user to Allow for Local Launch, Remote Launch, Local Activation, and Remote Activation.
10. Click OK to close the permissions dialog, then OK again on My Computer Properties. The user should now be able to remotely access DCOM applications including WMI.

Setting WMI permissions
This method enables you to manually configure WMI permissions on a machine. You cannot configure WMI security with Group Policy Objects.

Use the following steps to configure WMI permissions on a machine:

1. Select **Start** => **Run**, enter wmicmgmt.msc and click **OK** - this will launch the WMI management tool.
2. Right-Click WMI Control (Local) and select **Properties**.
3. Select the **Security** tab in the WMI Control Properties dialog.
4. Expand the Root object.
5. Select the namespace (Root\CIMV2, Root\Default, and Root\WMI in turn) and click **Security**.
6. Click **Advanced**.
7. Click **Add...**
8. Enter your domain user name or group name in the text entry field and click **Check Names**.
9. Click **OK**.
10. Set Apply onto to This namespace only.
11. Select **Allow** for the desired permissions (for example, Remote Enable, Account Enable, and Execute Methods).
12. Click **OK** three times to get back to the WMI Control Properties Security page.

**Setting remote registry permissions**

The following article from Microsoft describes how to set remote registry permissions:

http://support.microsoft.com/kb/314837

The user or group must be given read access to the registry key described in this article. Alternatively, the user could be added to the **Backup Operators** group. However this group has a high level of access to the whole system.

**Granting user rights**

User rights can be granted either from gpedit.msc for local configuration, or using the Group Policy Management Console.

**UNIX and related operating systems**

This page shows the information categories discovered, the script used, and whether privileged access is required. Optional commands such as lsof are assumed to have been installed in all cases.

All methods which are marked with an asterisk (*) must succeed for a host to be created. For a method to succeed, it must return some useful data. Where multiple scripts are listed against such methods, one of the scripts must succeed. For simple methods such as getDeviceInfo and getHostInfo this means the result contains expected attributes such as hostname, OS information and so on. For more complex methods, such as getInterfaceList, one of the defined scripts must return at least one item, an IP address. Additional data such as speed or duplex is not required.
### AIX
#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHBAList</td>
<td>hbaInfo</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>lsIpp</td>
<td>Privileges</td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsOf-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable [ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable [ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>[ .1, .2, .3, .4, .5 ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ .1, .2, .5, .6 ]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable [ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ]</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ .1, .2, .3, .4, .5 ]</td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable [ udpLocalAddress, udpLocalPort ]</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ .1, .2 ]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable [ hrSWInstalledName ]</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ .2 ]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable [ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ]</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[ .1, .2, .4, .5 ]</td>
</tr>
</tbody>
</table>
### FreeBSD

**Shell scripts**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo’</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>getHostInfos</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList’</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>pkg_info</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>ls/of-i</td>
<td></td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo’</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo’</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList’</td>
<td>IP-MIB::ipAddrTable</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]</td>
<td>[ .1, .2, .3 ]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td>[ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>[ .1, .2, .5, .6 ]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>[ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ]</td>
<td>[ .1, .2, .3, .4, .5 ]</td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td>[ udpLocalAddress, udpLocalPort ]</td>
<td>[ .1 ]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWinStalledTable</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWinStalledName ]</td>
<td>[ .2 ]</td>
</tr>
</tbody>
</table>
### HPUX

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Privileges</td>
</tr>
<tr>
<td>getPackageList</td>
<td>swlist</td>
<td>Privileges</td>
</tr>
<tr>
<td>getPatchList</td>
<td>patch_list</td>
<td>Privileges</td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable [ ipAdEntAddr, ipAdEntIfIndex, ipAdEntIfNetMask ]</td>
<td>1.3.6.1.2.1.4.20.1 [.1,.2,.3]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable [ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>1.3.6.1.2.1.2.2.1 [.1,.2,.5,.6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable [ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ]</td>
<td>1.3.6.1.2.1.6.13.1 [.1,.2,.3,.4,.5]</td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable [ udpLocalAddress, udpLocalPort ]</td>
<td>1.3.6.1.2.1.7.5.1 [.1,.2]</td>
</tr>
</tbody>
</table>
### BMC Atrium Discovery 8.3

#### Configuration guide

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable</td>
<td>1.3.6.1.2.125.6.3.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWInstalledName ]</td>
<td>[.2]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable</td>
<td>1.3.6.1.2.125.4.2.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ]</td>
<td>[.1, .2, .4, .5]</td>
</tr>
</tbody>
</table>

#### IRIX

**Shell scripts**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td>file_content</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td></td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>showprods</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

#### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]</td>
<td>[.1, .2, .3]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td>[ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>[.1, .2, .5, .6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>[ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort,</td>
<td>[.1, .2, .3, .4, .5]</td>
</tr>
<tr>
<td></td>
<td>tcpConnRemAddress, tcpConnRemPort ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td>[ udpLocalAddress, udpLocalPort ]</td>
<td>[.1, .2]</td>
</tr>
</tbody>
</table>
Method | MIB Values | OID
--- | --- | ---
getPackageList | HOST-RESOURCES-MIB::hrSWInstalledTable [ hrSWInstalledName ] | 1.3.6.1.2.1.25.6.3.1 [.2 ]
getProcessList | HOST-RESOURCES-MIB::hrSWRunTable [ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ] | 1.3.6.1.2.1.25.4.2.1 [.1,.2,.4,.5 ]

Linux

Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo`</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td><code>file_metadata</code></td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td></td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHBAList</td>
<td>hba_sysfs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hba_procfs</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hba_hbacmd</td>
<td>Privileges</td>
</tr>
<tr>
<td></td>
<td>hba_lputil</td>
<td>Privileges</td>
</tr>
<tr>
<td>getHostInfo`</td>
<td>host_info</td>
<td>Privileges</td>
</tr>
<tr>
<td>getInterfaceList`</td>
<td>ip_addr</td>
<td>Privileges</td>
</tr>
<tr>
<td></td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td>Privileges</td>
</tr>
<tr>
<td>getPackageList</td>
<td>rpmx</td>
<td></td>
</tr>
<tr>
<td></td>
<td>rpm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>dpkg</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
</table>
getDeviceInfo`       | SNMPv2-MIB::sysDescr.0 | 1.3.6.1.2.1.1.1.0 |
                      | SNMPv2-MIB::sysName.0 | 1.3.6.1.2.1.1.5.0 |

getHostInfo`
<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>system_profiler-apps</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td></td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.5.0</td>
</tr>
<tr>
<td>Method</td>
<td>MIB Values</td>
<td>OID</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>getHostInfo'</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>IP-MIB::ipAddrTable [ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask]</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable [ifIndex, ifDescr, ifSpeed, iPhysAddress]</td>
<td>[.1, .2, .3]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[.1, .2, .5, .6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable [tcpConnState, tcpConnLocalAddress, tcpConnLocalPort,</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>tcpConnRemAddress, tcpConnRemPort]</td>
<td>[.1, .2, .3, .4, .5]</td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable [udpLocalAddress, udpLocalPort]</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[.1, .2]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable [hrSWInstalledName]</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[.2]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable [hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters]</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[.1, .2, .4, .5]</td>
</tr>
</tbody>
</table>

**NetBSD**

**Shell scripts**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo'</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHostInfo'</td>
<td>host_info</td>
<td>Privileges</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>pkg_info</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privileges</td>
</tr>
</tbody>
</table>

**SNMP**

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo'</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.5.0</td>
</tr>
</tbody>
</table>
### Method | MIB Values | OID
--- | --- | ---
getHostInfo | HOST-RESOURCES-MIB::hrSystemUptime.0  
HOST-RESOURCES-MIB::hrMemorySize.0 | 1.3.6.1.2.1.1.1.0  
1.3.6.1.2.1.1.1.2.0
getInterfaceList | IP-MIB::ipAddrTable  
IF-MIB::ifTable | 1.3.6.1.2.1.4.20.1  
[ .1, .2, .3 ]  
1.3.6.1.2.1.2.2.1  
[ .1, .2, .5, .6 ]
getNetworkConnectionList | TCP-MIB::tcpConnTable  
UDP-MIB::udpConnTable | 1.3.6.1.2.1.6.13.1  
[ .1, .2, .3, .4, .5 ]  
1.3.6.1.2.1.7.5.1  
[ .1, .2 ]
getPackageList | HOST-RESOURCES-MIB::hrSWInstalledTable  
[ hrSWInstalledName ] | 1.3.6.1.2.1.25.6.3.1  
[ .2 ]
getProcessList | HOST-RESOURCES-MIB::hrSWRunTable  
[ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ] | 1.3.6.1.2.1.25.4.2.1  
[ .1, .2, .4, .5 ]

### OpenBSD

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td>Privileges</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>pkg_info</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
</table>
| getDeviceInfo | SNMPv2-MIB::sysDescr.0  
SNMPv2-MIB::sysName.0 | 1.3.6.1.2.1.1.1.0  
1.3.6.1.2.1.1.1.5.0 |
### Configuration guide

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getHostInfo'</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0 HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.1.1.0 1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>IP-MIB::ipAddrTable [ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ] IF-MIB::ifTable [ ifIndex, iDescr, ifSpeed, ifPhysAddress ]</td>
<td>1.3.6.1.2.1.4.20.1 [.1,...,3] 1.3.6.1.2.1.2.2.1 [.1,...,5,6]</td>
</tr>
</tbody>
</table>
| getNetworkConnectionList | TCP-MIB::tcpConnTable [ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ] 
UDP-MIB::udpConnTable [ udpLocalAddress, udpLocalPort ] | 1.3.6.1.2.1.6.13.1 [.1,...,3,4,5] 1.3.6.1.2.1.7.5.1 [.1,...,2] |
| getPackageList        | HOST-RESOURCES-MIB::hrSWInstalledTable [ hrSWInstalledName ]                | 1.3.6.1.2.1.25.6.3.1 [.2] |
| getProcessList        | HOST-RESOURCES-MIB::hrSWRunTable [ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ] | 1.3.6.1.2.1.25.4.2.1 [.1,...,4,5] |

### OpenVMS

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo'</td>
<td>deviceinfo</td>
<td></td>
</tr>
<tr>
<td>getFileSystems</td>
<td>show-mount</td>
<td></td>
</tr>
<tr>
<td>getHostInfo'</td>
<td>hostinfo</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>iflist</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>show-network</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>show-product</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>show-system</td>
<td></td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo'</td>
<td>SNMPv2-MIB::sysDescr.0 SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo'</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0 HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.1.1.0 1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>IP-MIB::ipAddrTable [ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ] IF-MIB::ifTable [ ifIndex, iDescr, ifSpeed, ifPhysAddress ]</td>
<td>1.3.6.1.2.1.4.20.1 [.1,...,3] 1.3.6.1.2.1.2.2.1 [.1,...,5,6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Configuration guide

### BMC Atrium Discovery 8.3

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP-MIB::tcpConnTable</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>[ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort,</td>
<td>[.1, .2, .3, .4, .5]</td>
</tr>
<tr>
<td></td>
<td>tcpConnRemAddress, tcpConnRemPort ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td>[ udpLocalAddress, udpLocalPort ]</td>
<td>[.1, .2]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWInstalledName ]</td>
<td>[.2]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ]</td>
<td>[.1, .2, .4, .5]</td>
</tr>
</tbody>
</table>

### POWER HMC

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td>*</td>
</tr>
<tr>
<td>getFileSystem</td>
<td>monhmc-rdisk</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td>*</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>lshmc-n</td>
<td>*</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable</td>
<td>1.3.6.1.2.1.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]</td>
<td>[.1, .2, .3]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td></td>
<td>[ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>[.1, .2, .5, .6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable</td>
<td>1.3.6.1.2.1.6.13.1</td>
</tr>
<tr>
<td></td>
<td>[ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort,</td>
<td>[.1, .2, .3, .4, .5]</td>
</tr>
<tr>
<td></td>
<td>tcpConnRemAddress, tcpConnRemPort ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td></td>
<td>[ udpLocalAddress, udpLocalPort ]</td>
<td>[.1, .2]</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWInstalledName ]</td>
<td>[.2]</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
<tr>
<td></td>
<td>[ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ]</td>
<td>[.1, .2, .4, .5]</td>
</tr>
</tbody>
</table>

BMC Atrium Discovery 8.3

Page 306 of 399
Solaris
Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td></td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td></td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td></td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHBAList</td>
<td>hba_fcinfo</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hba_emlxadm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hba_hbacmd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>hba_lputil</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>pkginfo</td>
<td></td>
</tr>
<tr>
<td>getPatchList</td>
<td>patch_list</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pfiles</td>
<td></td>
</tr>
</tbody>
</table>

SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td></td>
<td>SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0</td>
<td>1.3.6.1.2.1.25.1.1.0</td>
</tr>
<tr>
<td></td>
<td>HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>IP-MIB::ipAddrTable</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]</td>
<td>[.1, .2, .3]</td>
</tr>
<tr>
<td></td>
<td>IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.4.20.1</td>
</tr>
<tr>
<td></td>
<td>[ ifIndex, ifDescr, ifSpeed, ifPhysAddress ]</td>
<td>[.1, .2, .5, .6]</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Method | MIB Values | OID
---|---|---
**TCP-MIB::tcpConnTable**<br> [ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ]
**UDP-MIB::udpConnTable**<br> [ udpLocalAddress, udpLocalPort ] | 1.3.6.1.2.1.6.13.1 [ .1, .2, .3, .4, .5 ]<br> 1.3.6.1.2.1.7.5.1 [ .1, .2 ] | **TCP-MIB::tcpConnTable** | 1.3.6.1.2.1.6.13.1 [ .1, .2, .3, .4, .5 ]
**UDP-MIB::udpConnTable** | 1.3.6.1.2.1.7.5.1 [ .1, .2 ] | **UDP-MIB::udpConnTable** | 1.3.6.1.2.1.7.5.1 [ .1, .2 ]

### Tru64

#### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td></td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td>Privileges</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>setld</td>
<td>Privileges</td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo</td>
<td>SNMPv2-MIB::sysDescr.0&lt;br&gt; SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.0&lt;br&gt; 1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0&lt;br&gt; HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.1.1.0&lt;br&gt; 1.3.6.1.2.1.25.2.2.0</td>
</tr>
</tbody>
</table>
### Method | MIB Values | OID
---|---|---
getInterfaceList | IP-MIB::ipAddrTable
[ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]
IF-MIB::ifTable
[ ifIndex, ifDescr, ifSpeed, ifPhysAddress ] | 1.3.6.1.2.1.4.20.1
[ .1, .2, .3 ]
1.3.6.1.2.1.2.2.1
[ .1, .2, .5, .6 ]

getNetworkConnectionList | TCP-MIB::tcpConnTable
[ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort ]
UDP-MIB::udpConnTable
[ udpLocalAddress, udpLocalPort ] | 1.3.6.1.2.1.6.13.1
[ .1, .2, .3, .4, .5 ]
1.3.6.1.2.1.7.5.1
[ .1, .2 ]

getPackageList | HOST-RESOURCES-MIB::hrSWInstalledTable
[ hrSWInstalledName ] | 1.3.6.1.2.1.25.6.3.1
[ .2 ]

getProcessList | HOST-RESOURCES-MIB::hrSWRunTable
[ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ] | 1.3.6.1.2.1.25.4.2.1
[ .1, .2, .4, .5 ]

### UnixWare

**Shell scripts**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
<tr>
<td>getDirectoryListing</td>
<td>ls</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileContent</td>
<td>file_content</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileInfo</td>
<td>Handled by the getFileMetadata and getFileContent calls.</td>
<td></td>
</tr>
<tr>
<td>getFileMetadata</td>
<td>file_metadata</td>
<td>Privileges</td>
</tr>
<tr>
<td>getFileSystems</td>
<td>df</td>
<td></td>
</tr>
<tr>
<td>getHostInfo</td>
<td>host_info</td>
<td></td>
</tr>
<tr>
<td>getInterfaceList</td>
<td>ifconfig</td>
<td></td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>netstat</td>
<td></td>
</tr>
<tr>
<td>getPackageList</td>
<td>pkginfo</td>
<td></td>
</tr>
<tr>
<td>getProcessList</td>
<td>ps</td>
<td></td>
</tr>
<tr>
<td>getProcessToConnectionMapping</td>
<td>lsof-i</td>
<td>Privileges</td>
</tr>
</tbody>
</table>

### SNMP

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
</table>
| getDeviceInfo | SNMPv2-MIB::sysDescr.0
SNMPv2-MIB::sysName.0 | 1.3.6.1.2.1.1.1.0
1.3.6.1.2.1.1.5.0 |
| getHostInfo | HOST-RESOURCES-MIB::hrSystemUptime.0
HOST-RESOURCES-MIB::hrMemorySize.0 | 1.3.6.1.2.1.25.1.1.0
1.3.6.1.2.1.25.2.2.0 |
Method | MIB Values | OID
--- | --- | ---
getInterfaceList | IP-MIB::ipAddrTable
  [ ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask ]
  IF-MIB::ifTable
  [ ifIndex, ifDescr, ifSpeed, ifPhysAddress ] | 1.3.6.1.2.1.4.20.1 [.1, .2, .3 ]
  1.3.6.1.2.1.2.2.1 [.1, .2, .5, .6 ]

getNetworkConnectionList | TCP-MIB::tcpConnTable
  [ tcpConnState, tcpConnLocalAddress, tcpConnLocalPort,
    tcpConnRemAddress, tcpConnRemPort ]
  UDP-MIB::udpConnTable
  [ udpLocalAddress, udpLocalPort ] | 1.3.6.1.2.1.6.13.1 [.1, .2, .3, .4, .5 ]
  1.3.6.1.2.1.7.5.1 [.1, .2 ]

getPackageList | HOST-RESOURCES-MIB::hrSWInstalledTable
  [ hrSWInstalledName ] | 1.3.6.1.2.1.25.6.3.1 [.2 ]

getAddressList | HOST-RESOURCES-MIB::hrSWRunTable
  [ hrSWRunIndex, hrSWRunName, hrSWRunPath, hrSWRunParameters ] | 1.3.6.1.2.1.25.4.2.1 [.1, .2, .4, .5 ]

VMware ESX

vSphere

Method | Managed Object Reference | Properties | Notes
--- | --- | --- | ---
getDeviceInfo | HostSystem | name | 
  ServiceInstance | content.about | 
getFileSystems | Datastore | summary.name | 
  summary.type | 
  summary.capacity | 
  summary.freeSpace | 
  summary.url | 
  info.vmfs.uuid | VMFS volumes only | 
  info.nas.remoteHost | NFS & CIFS volumes only | 
  info.nas.remotePath | NFS & CIFS volumes only | 
  info.nas.userName | CIFS volumes only | 
  info.path LOCAL volumes only | 
getHBAInfo | HostSystem | config.storageDevice.hostBusAdapter[].device | 
  config.storageDevice.hostBusAdapter[].nodeWorldWideName | 
  config.storageDevice.hostBusAdapter[].portWorldWideName | 
  config.storageDevice.hostBusAdapter[].model | 
  config.storageDevice.hostBusAdapter[].driver | 

getHostInfo | HostSystem | hardware.memorySize | 

<table>
<thead>
<tr>
<th>Method</th>
<th>Managed Object Reference</th>
<th>Properties</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.model</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.vendor</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.uuid</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.otherIdentifyingInfo[].identifierType.key</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.otherIdentifyingInfo[].identifierValue</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuPkg.threadId</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuPkg.numCpuCores</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuInfo.threadId</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.hyperThread.active</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.dnsConfig.dnsDomainName</td>
<td>Not used if unset</td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>HostSystem</td>
<td>config.network.pnic[].device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.pnic[].driver</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.pnic[].mac</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.pnic[].spec.ip.ipAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.pnic[].spec.ip.subnetMask</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.vnic[].device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.vnic[].spec.mac</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.vnic[].spec.ip.ipAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.vnic[].spec.ip.subnetMask</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.consoleVnic[].device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.consoleVnic[].spec.mac</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.consoleVnic[].spec.ip.ipAddress</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.network.consoleVnic[].spec.ip.subnetMask</td>
<td></td>
</tr>
<tr>
<td>getPatchList</td>
<td>HostSystem</td>
<td>configManager.patchManager</td>
<td>Uses queryHostPatch() task</td>
</tr>
<tr>
<td>getVirtualMachines</td>
<td>VirtualMachine</td>
<td>config.name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.uuid</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.guestFullName</td>
<td></td>
</tr>
</tbody>
</table>
## Method | Managed Object Reference | Properties | Notes
---|---|---|---
| | | config.guestId | 
| | | config.alternateGuestName | 
| | | name | Used if config.name is empty
| | | guest.guestId | 
| | | guest.guestFullName | 
| | | runtime.powerState | 

*indicates methods that must succeed for a Host to be created

### Shell scripts

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
<tr>
<td>getDeviceInfo</td>
<td>device_info</td>
<td></td>
</tr>
</tbody>
</table>
| getDirectoryListing | ls | Privileges
| getFileInfo |(file_content) | Privileges
| getFileInfo | Handled by the getFileMetadata and getFileContent calls. | 
| getFileMetadata | file_metadata | Privileges
| getFileSystem | df | Privileges
| getHBAList | hba_sysfs | hba_procfs
| | hba_hbacmd | Privileges
| | hba_lputil | Privileges
| getHostInfo | host_info | Privileges
| getInterfaceList | ip_addr | Privileges
| | ifconfig | Privileges
| getNetworkConnectionList | netstat | Privileges
| getPackageList | rpmx | rpm
| | rpm | 
| | dpkg | 
| getProcessList | ps | 
| getProcessToConnectionMapping | lsof-i | Privileges
### VMware ESXi

#### vSphere

<table>
<thead>
<tr>
<th>Method</th>
<th>Managed Object Reference</th>
<th>Properties</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>getDeviceInfo</code></td>
<td>HostSystem</td>
<td>name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ServiceInstance</td>
<td>content.about</td>
<td></td>
</tr>
<tr>
<td><code>getFileSystems</code></td>
<td>Datastore</td>
<td>summary.name</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary.type</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary.capacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary.freeSpace</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>summary.url</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>info.vmfs.uuid</td>
<td>VMFS volumes only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>info.nas.remoteHost</td>
<td>NFS &amp; CIFS volumes only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>info.nas.remotePath</td>
<td>NFS &amp; CIFS volumes only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>info.nas.userName</td>
<td>CIFS volumes only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>info.path</td>
<td>LOCAL volumes only</td>
</tr>
<tr>
<td><code>getHBAInfo</code></td>
<td>HostSystem</td>
<td>config.storageDevice.hostBusAdapter[].device</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.storageDevice.hostBusAdapter[].nodeWorldWideName</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.storageDevice.hostBusAdapter[].portWorldWideName</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.storageDevice.hostBusAdapter[].model</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.storageDevice.hostBusAdapter[].driver</td>
<td></td>
</tr>
<tr>
<td><code>getHostInfo</code></td>
<td>HostSystem</td>
<td>hardware.memorySize</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.model</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.vendor</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.uuid</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.otherIdentifyingInfo[].identifierType.key</td>
<td>Not used if unset</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.systemInfo.otherIdentifyingInfo[].identifierValue</td>
<td>Not used if unset or &quot;unknown&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuPkg.threadId</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuPkg.numCpuCores</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>hardware.cpuInfo.threadId</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>config.hyperThread.active</td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>Managed Object Reference</td>
<td>Properties</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>config.network.dnsConfig.dnsDomainName</td>
<td>config.network.dnsConfig.hostName</td>
<td>Not used if unset</td>
<td></td>
</tr>
<tr>
<td>config.network.dnsConfig.hostName</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>getInterfaceList'</td>
<td>HostSystem</td>
<td>config.network.pnic[].device</td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].driver</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].mac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].spec.ip.ipAddress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].spec.ip.subnetMask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].spec.linkSpeed.speedMb</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.pnic[].device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.vnic[].device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.vnic[].spec.mac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.vnic[].spec.ip.ipAddress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.vnic[].spec.ip.subnetMask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.consoleVnic[].device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.consoleVnic[].spec.mac</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.consoleVnic[].spec.ip.ipAddress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.network.consoleVnic[].spec.ip.subnetMask</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>getPatchList</td>
<td>HostSystem</td>
<td>configManager.patchManager</td>
<td>Uses queryHostPatch() task</td>
</tr>
<tr>
<td>getVirtualMachines</td>
<td>VirtualMachine</td>
<td>config.name</td>
<td></td>
</tr>
<tr>
<td>config.uuid</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.guestFullName</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.guestId</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>config.alternateGuestName</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td></td>
<td>Used if config.name is empty</td>
<td></td>
</tr>
<tr>
<td>guest.guestId</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guest.guestFullName</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>runtime.powerState</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Shell scripts**

<table>
<thead>
<tr>
<th>Method</th>
<th>Script</th>
<th>Privileges required</th>
</tr>
</thead>
<tbody>
<tr>
<td>initialise</td>
<td>init</td>
<td></td>
</tr>
</tbody>
</table>
### Mainframe

Some of the detail data that the z/OS Discovery Agent collects is dependent on additional MainView products being installed. The following table shows the MainView products used to obtain additional detail information. See the BMC Discovery for Z/OS documentation for further information.

<table>
<thead>
<tr>
<th>Method</th>
<th>Script Views</th>
</tr>
</thead>
<tbody>
<tr>
<td>getMainframeInfo</td>
<td>View Z</td>
</tr>
<tr>
<td>getMFPart</td>
<td>View Z</td>
</tr>
<tr>
<td>getApplication</td>
<td>Views 49Z, 4HZ and 4WZ (requested as View 49HWZ) — Requires MainView for WebSphere, Application Server, and MainView Transaction Analyzer products to be installed.</td>
</tr>
<tr>
<td>getCouplingFacility</td>
<td>View Z</td>
</tr>
<tr>
<td>getDatabase</td>
<td>Views 1IZ and 1XZ (requested as View 1IXZ) — Requires MainView for DB2 and MainView for IMS products to be installed.</td>
</tr>
<tr>
<td>getDatabaseDetail</td>
<td>Views 1IJZ, 1ILZ and 1IKZ (requested as View 1IJKLZ) — Requires MainView for DB2 product to be installed.</td>
</tr>
<tr>
<td>getDependency</td>
<td>View Z</td>
</tr>
<tr>
<td>getDiskDrive</td>
<td>View #-.</td>
</tr>
</tbody>
</table>
| getMQDetail          | **Version 8.3** — Views 5UZ, 5$Z and 5NZ (requested as View 5U$NZ)  
                        | **Version 8.3 SP2** — Views 5UZ, 5VZ and 5NZ (requested as View 5NUVZ) — Requires MainView for WebSphere MQ product to be installed. |
| getSoftware          | Views 0Z, 1Z, 2Z, 3Z, 4Z, 5Z, 6Z and 7Z (requested as View 01234567Z)          |
| getStorageSubsystem  | View -                                                                       |
| getSysplex           | View Z                                                                       |
| getTapeDrive         | View -@                                                                      |
| getTransaction       | View 0YZ — Requires MainView for CICS and MainView for IMS products to be installed. |
Method | Script Views
---|---
getTransactionProgram | Version 8.3 SP3 – View 0YZ — Requires MainView for CICS and MainView for IMS products to be installed.

*indicates methods that must succeed for a Mainframe to be created.

**IBM i**

IBM i (AS/400) discovery is undertaken using SNMP. SNMP discovery is supported for ALL devices with an accessible SNMP agent. Discovery supports SNMP v1, v2c and v3. For some older platforms (for example Netware) the use of SNMP v1 may be required. This is defined on a per credential basis. Note that only read (GET, GETNEXT, GETBULK) access is required.

This page shows the method used, MIB values, and OIDS used.

<table>
<thead>
<tr>
<th>Method</th>
<th>MIB Values</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>getDeviceInfo*</td>
<td>SNMPv2-MIB::sysDescr.0, SNMPv2-MIB::sysName.0</td>
<td>1.3.6.1.2.1.1.1.0, 1.3.6.1.2.1.1.5.0</td>
</tr>
<tr>
<td>getHostInfo*</td>
<td>HOST-RESOURCES-MIB::hrSystemUptime.0, HOST-RESOURCES-MIB::hrMemorySize.0</td>
<td>1.3.6.1.2.1.25.1.1.0, 1.3.6.1.2.1.25.2.2.0</td>
</tr>
<tr>
<td>getInterfaceList*</td>
<td>IP-MIB::ipAddrTable, IF-MIB::ifTable</td>
<td>1.3.6.1.2.1.4.20.1, 1.3.6.1.2.1.2.2.1</td>
</tr>
<tr>
<td>getNetworkConnectionList</td>
<td>TCP-MIB::tcpConnTable, UDP-MIB::udpConnTable</td>
<td>1.3.6.1.2.1.6.13.1, 1.3.6.1.2.1.7.5.1</td>
</tr>
<tr>
<td>getPackageList</td>
<td>HOST-RESOURCES-MIB::hrSWInstalledTable</td>
<td>1.3.6.1.2.1.25.6.3.1</td>
</tr>
<tr>
<td>getProcessList</td>
<td>HOST-RESOURCES-MIB::hrSWRunTable</td>
<td>1.3.6.1.2.1.25.4.2.1</td>
</tr>
</tbody>
</table>

**What is a Database Credential Group?**

A Database Credential Group is a container for information used to query databases. They contain one or more credentials and one or more queries.

- **Credential**: contains the information (for example, database credentials, driver, IP address) to create a connection from BMC Atrium Discovery to the target database.
- **Query**: the SQL query which is passed to the target database to extract the required information. The query is supplied by the pattern.

A Database Credential Group is created by the activation of a Database Pattern. A Database Pattern has its type defined as sql_discovery.
Deep database discovery

Any database driver listed on the JDBC management page can be used to create database connections for querying from patterns. The TKU shipped with BMC Atrium Discovery 8.3 provides patterns for deep discovery of the following databases:

- IBM DB2 – mainframe only
- IBM Information Management System (IMS) – mainframe only
- Microsoft SQL Server
- MySQL
- Oracle
- Sybase

Configuring a Database Credential Group

This procedure shows you how to configure a Database Credential Group. The only items requiring configuration through the UI for a Database Credential Group are the credentials (username, password, connection information). The database queries come from the database pattern.

The example used is for MySQL and uses the MySQL_AB.MySQL_RDBMS_Extended.DatabasesAndTables pattern.

This is the definitions section of the MySQL_AB.MySQL_RDBMS_Extended.DatabasesAndTables pattern. Additional comments explain various definitions.

definitions MySQLDetails 1.0
    """Queries for MySQL to recover detailed content information''"" // provides the description text for the Credential Group
    type := sql_discovery; // sql_discovery places the credential group
    group := "MySQL"; // tab with the heading MySQL. The group also
    // Name field.

define showDatabases // defines a query called showDatabases
    """Return a list of defined databases''"" // provides the description text for the showDatabases query
    // the query
    query := "SHOW DATABASES";
end define;
define showTables        // defines a query called showTables
    """Return a list of defined tables within the given database"""
    // provides the description text for the showTable query

    // the query
    query := "SELECT table_name FROM information_schema.tables WHERE t

    parameters := db_name;
    end define;
end definitions;

1. Ensure that the MySQL_AB.MySQL_RDBMS_Extended.DatabasesAndTables pattern is activated.
2. From the Discovery home page, click Credentials.
3. Click the Databases tab.
4. Click the MySQL credential group heading.
5. Click the Credentials tab.
7. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Credential, for example, ExtendedMySQL.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a free text description of the Credential.</td>
</tr>
<tr>
<td>Username</td>
<td>The username with which to log in to the target database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password corresponding to the username above.</td>
</tr>
<tr>
<td>Database Driver</td>
<td>Select an appropriate database driver from the drop down list. When one is selected, additional fields are added to the form depending on the driver selected.</td>
</tr>
<tr>
<td>Database IP Address</td>
<td>Enter a value to represent an IP address or range of IP addresses. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• an IP address (10.10.10.3)</td>
</tr>
<tr>
<td></td>
<td>• a range specification (10.10.10.* or 10.10.1-5.* or 10.10.0.0/24)</td>
</tr>
<tr>
<td></td>
<td>• a regular expression matching an IP address (.* or 10.10.10.(23</td>
</tr>
</tbody>
</table>

What level of credentials are required?
In order for BMC Atrium Discovery to retrieve the Database details, it will need to be able to access the Database as a legitimate user, with privileges sufficient to execute the SQL Queries below. These examples pertain to Oracle, for other databases, see the relevant Configipedia pages.

<table>
<thead>
<tr>
<th>Oracle Database Server SID</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtaining a list of Schemas for a SID</td>
<td>SELECT username FROM all_users ORDER BY username</td>
</tr>
<tr>
<td>Obtaining a list of Tables within a Schema</td>
<td>SELECT table_name FROM all_tables WHERE owner = %schema%</td>
</tr>
</tbody>
</table>
### Oracle Database Server SID

**Query**

- Obtaining a list of Tablespaces for a SID
  
  ```sql
  SELECT * FROM dba_tablespaces
  ```

- Obtaining a list of DataFiles within a Tablespace
  
  ```sql
  SELECT * FROM DBA_DATA_FILES WHERE TABLESPACE_NAME = %tablespace_name%
  ```

### Oracle Database Server service_name

**Query**

- Obtaining a list of Schemas
  
  ```sql
  SELECT username FROM all_users ORDER BY username
  ```

- Obtaining a list of Tables within a Schema
  
  ```sql
  SELECT table_name FROM all_tables WHERE owner = %schema%
  ```

- Obtaining a list of Tablespaces
  
  ```sql
  SELECT * FROM dba_tablespaces
  ```

- Obtaining a list of DataFiles within a Tablespace
  
  ```sql
  SELECT * FROM DBA_DATA_FILES WHERE TABLESPACE_NAME = %tablespace_name%
  ```

**The following table describes the additional fields:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>The database name. If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any database whose name is supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose name matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Database Name</td>
<td>The database name (Informix). If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any database whose name is supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose name matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Database Instance Name</td>
<td>The database instance name (Microsoft SQL Server). If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any database whose name is supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose name matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Server Name</td>
<td>The name of the Informix server as it appears in the sqlhosts file. If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any server name supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose name matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>System ID (SID)</td>
<td>The Oracle System ID, or instance running on the Oracle host. If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any database whose SID supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose SID matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Service name</td>
<td>The Oracle service name, an alias to an instance, or multiple instances in for example a clustered environment. If you leave the <strong>Match Regular Expression</strong> checkbox clear, the connection will be made to any database whose service name is supplied by the pattern. If the checkbox is selected, the connection will be made to any database whose service name matches the regular expression. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>The port number to use to connect to the database. If you leave the <strong>Match Regular Expression</strong> checkbox clear, any port supplied by the pattern will be used to connect to the database. If the checkbox is selected, any port supplied which matches the regular expression will be used to connect to the database. Select the default value checkbox and specify a value to be used if none is specified by a pattern.</td>
</tr>
<tr>
<td>Additional JDBC Parameters</td>
<td>Any additional JDBC parameters to use when making the connection. Select the default value checkbox and specify a value to be used if none is specified by a pattern. These are specified as <strong>key=value</strong> pairs in a semicolon separated list.</td>
</tr>
</tbody>
</table>

8. To save the details, click **Apply**.
9. Click the **Details** tab to return to the main summary page for the Credential Group.

**What is a Middleware Credential Group?**

A Middleware Credential Group is a container for information used to query middleware such as web and application servers and similar tools that support application development and delivery. They contain one or more credentials and one or more queries.

- **Credential**: contains the login credentials and IP address required to create a connection from BMC Atrium Discovery to the middleware target.
- **Query**: the query which is passed to the Expert Discovery Module (EDM). Only one query is supported by EDMs, that query is **scan** which triggers a discovery scan of the target.

A Middleware Credential Group is created by the activation of a Middleware Pattern. A Middleware Pattern has its type defined as one of the following:

- `tomcat_discovery`
- `weblogic_discovery`

**Configuring a Middleware Credential Group**

This procedure shows you how to configure a Middleware Credential Group. The only items requiring configuration through the UI for a Middleware Credential Group are the credentials (username, password, connection information). The query comes from the middleware pattern.

The example used is for Tomcat and uses the `Tomcat.ExtendedDiscovery.DiscoverTomcat` pattern.

There is more to configuring the discovery of middleware than configuring a Middleware Credential Group. For a full description of this, see the **Extended discovery of Tomcat** section.

**This is the definitions section of the Tomcat.ExtendedDiscovery.DiscoverTomcat pattern.** Additional comments explain various definitions.

```plaintext
// includes EDMRequest 1.0

""""Queries to recover detailed Tomcat information"

// provides the description text for the Credential Group
```
The page Discovering Tomcat does not exist.

Management system credentials

The management system credentials page is used for vCenter, vSphere, and mainframe credentials.

The configuration of the management system credentials is described in the following sections:

- Configuring Management System vCenter credentials
- Configuring Management System vSphere credentials
- Configuring mainframe credentials
- Testing mainframe credentials

Configuring management system vCenter credentials

The vCenter credentials tab is a holder for credentials provided by the vCenter DIP provider. These credentials are populated when patterns containing vSphere queries are activated.

From the Management System tab, you can manually add new vCenter credentials and update existing vCenter credentials. However, it is a lot simpler to add or update vCenter credentials from the Devices tab. When you edit a vCenter credential on the Devices tab, the same changes are reflected for that credential on the Management System tab.

⚠️ Typically, the recommended procedure to add or edit vCenter credentials is from the Devices tab. For more information about adding or editing vCenter credentials from the Devices tab, see Configuring vCenter credentials
Viewing vCenter credentials

To view the pattern-populated vCenter credentials, perform the following:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Management System**.
3. Click **vCenter**.
   The *vCenter Credentials* page displayed.

The vCenter credentials are checked in sequence, and the first matching entry is used. After a working vCenter credential is found, further credentials are not checked. The vCenter credentials are shown in color-coded boxes. The colors represent the level of login success achieved with that credential:

- Green: 100% success rate.
- Yellow: partial success.
- Blue: the credential has never been used.
- Red: 0% success rate.

The following table describes the fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the vCenter credential. This field is a link to the <strong>Details</strong> tab on the <strong>vCenter</strong> page which contains details about the vCenter credentials, associated patterns, and queries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of credential. The type is displayed as vCenter.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Displays the number of credentials. This field is a link to the <strong>Credentials</strong> tab on the <strong>vCenter</strong> page which contains details about the credential.</td>
</tr>
<tr>
<td>Queries</td>
<td>Displays the number of queries associated with the credential. This field is a link to the <strong>Queries</strong> tab on the <strong>vCenter</strong> page which contains details about the queries.</td>
</tr>
</tbody>
</table>
| Actions | A list with the following options:                                                                                           
  - View: Select this to view the details of the credential. For more information, see *Viewing vCenter credential details*.                                                                                           
  - Edit: You can select this to update existing vCenter credentials. However, the recommended procedure to edit vCenter credentials is from the **Devices** tab. For more information about editing vCenter credentials from the **Devices** tab, see *Configuring vCenter credentials*. 
  - Delete: This is a dimmed field.                                                                                           |

**Viewing vCenter credential details**

To view the vCenter credential details:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Management System**.
3. Click **vCenter**.
The **vCenter Credentials** page is displayed.

4. To view the vCenter credential details, do one of the following:
   a. Click on the corresponding credential name, or,
   b. From the **Actions** list, select **View**
      The **vCenter** page for that credential is displayed.

5. The **vCenter** page contains the following tabs:
   a. **Details**: Contains details about the vCenter credential, related patterns, and integration results.
   b. **Credentials**: Displays the available vCenter credentials. The tab also displays the available number of credentials in brackets.
   c. **Queries**: Displays the list of queries related to the patterns.

6. Click on a tab to see the details.

The following table describes the fields for each tab:

<table>
<thead>
<tr>
<th>Details</th>
<th>This tab has the following sections:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Details:</td>
</tr>
<tr>
<td></td>
<td>• Name: Name of the credential.</td>
</tr>
<tr>
<td></td>
<td>• Description: A description of</td>
</tr>
<tr>
<td></td>
<td>what the credential does and how.</td>
</tr>
<tr>
<td></td>
<td>(For example, *Queries for</td>
</tr>
<tr>
<td></td>
<td>getting licensing information for</td>
</tr>
<tr>
<td></td>
<td>ESX/ESXi hosts via vCenter.*)</td>
</tr>
<tr>
<td></td>
<td>• Type: The type of credential.</td>
</tr>
<tr>
<td></td>
<td>The type is displayed as vCenter.</td>
</tr>
<tr>
<td></td>
<td>• Connection setup: Describes</td>
</tr>
<tr>
<td></td>
<td>whether the connection setup is</td>
</tr>
<tr>
<td></td>
<td>dynamic or static.</td>
</tr>
<tr>
<td></td>
<td>• Related Patterns:</td>
</tr>
<tr>
<td></td>
<td>• Pattern: The list of related</td>
</tr>
<tr>
<td></td>
<td>patterns. Each listed pattern</td>
</tr>
<tr>
<td></td>
<td>links to the view pattern page.</td>
</tr>
<tr>
<td></td>
<td>• Details: The list of queries</td>
</tr>
<tr>
<td></td>
<td>related to the patterns. Each</td>
</tr>
<tr>
<td></td>
<td>listed query links to the view</td>
</tr>
<tr>
<td></td>
<td>query page.</td>
</tr>
<tr>
<td></td>
<td>• Related Integration Results by</td>
</tr>
<tr>
<td></td>
<td>Pattern: The pattern that</td>
</tr>
<tr>
<td></td>
<td>triggered this result. Each</td>
</tr>
<tr>
<td></td>
<td>listed pattern links to the</td>
</tr>
<tr>
<td></td>
<td>view pattern page. State:</td>
</tr>
<tr>
<td></td>
<td>Describes whether the pattern</td>
</tr>
<tr>
<td></td>
<td>is active or not. Results:</td>
</tr>
<tr>
<td></td>
<td>Displays the integration result</td>
</tr>
<tr>
<td></td>
<td>and links to the *Integration</td>
</tr>
<tr>
<td></td>
<td>Result* page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Credentials</th>
<th>Displays the name of the credentials. The credential name links to the credential details tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the pattern that triggered this result.</td>
</tr>
<tr>
<td>TPL</td>
<td>To create a new credential, you can select this option. The <em>Create New Credential</em> page is displayed. However, the recommended procedure to add a new vCenter credentials is from the <em>Devices</em> tab. For more information about adding vCenter credentials from the <em>Devices</em> tab, see Configuring vCenter credentials.</td>
</tr>
<tr>
<td>Create</td>
<td>This list contains the following options:</td>
</tr>
<tr>
<td></td>
<td>• Edit: You can select this to update existing vCenter credentials. However, the recommended</td>
</tr>
<tr>
<td></td>
<td>procedure to edit vCenter credentials is from the <em>Devices</em> tab. For more information about editing vCenter credentials from the <em>Devices</em> tab, see Configuring vCenter credentials.</td>
</tr>
<tr>
<td></td>
<td>• Test: Select this to test the credential. For more information, see #Testing vCenter credentials.</td>
</tr>
<tr>
<td></td>
<td>• Copy: If you want to copy the credential, select this option.</td>
</tr>
<tr>
<td></td>
<td>• Delete: To delete the credential, select this option.</td>
</tr>
</tbody>
</table>
### Adding vCenter credentials

The recommended procedure to add new vCenter credentials is from the Devices tab. For more information about adding vCenter credentials from the Devices tab, see Configuring vCenter credentials.

### Updating vCenter credentials

The recommended procedure to edit vCenter credentials is from the Devices tab. For more information about editing vCenter credentials from the Devices tab, see Configuring vCenter credentials.

### Testing vCenter credentials

To test a vCenter credential:

1. On the vCenter Credentials page, click the credential to test. The vCenter details page is displayed.
2. Click the Credentials tab.
3. From the Actions list, click Test. A dialog box is displayed with the the credential values, and a field in which you enter the IP address against which to test the credential.
4. Enter the target IP address to test.
5. Click Test. The page is refreshed to show that the test in progress and when complete, the results are shown on the Device Credentials page; this may take a few minutes.

### Configuring management system vSphere credentials

#### Unpatched VMware vSphere known problems

Unpatched versions of VMware vSphere have known problems when scanned by various tools. We strongly recommend that you apply the appropriate patches to affected systems. There is more information on this issue on the following Configipedia link.
The VMware vSphere API is used to discover VMware ESX and ESXi systems. Where the vSphere API cannot be accessed, discovery falls back to an ssh login to access the underlying Linux operating system.

⚠️ **vSphere credentials are not host credentials**

The vSphere credentials that you enter in this page are only used for the vSphere API. If this is not accessible and ssh discovery is attempted, a separate host login credential for the endpoint is required.

From the **Management System** tab, you can manually add new vSphere credentials and update existing vSphere credentials. However, it is a lot simpler to add or update vSphere credentials from the **Devices** tab. When you edit a vSphere credential on the **Devices** tab, the same changes are reflected for that credential on the **Management System** tab.

⚠️ **Typically, the recommended procedure to configure the vSphere credentials is from the Devices tab. For more information about configuring vSphere credentials from the Devices tab, see Configuring vSphere credentials**

### Viewing vSphere credentials

To view existing vSphere credentials:

1. From the secondary navigation bar on the **Discovery** tab, click **Credentials**.
2. Click **Management System**.
3. Click **vSphere**.

   The **vSphere Credentials** page is displayed.

The vSphere credentials are checked in sequence, and the first matching entry is used. After a working vSphere credential is found, further credentials are not checked. The vSphere credentials are shown in color-coded boxes. The colors represent the level of login success achieved with that credential:

- **Green**: 100% success rate.
- **Yellow**: partial success.
- **Blue**: the credential has never been used.
- **Red**: 0% success rate.

The following table describes the fields:
1. From the secondary navigation bar on the *Discovery* tab, click *Credentials*.
2. Click *Management System*.
3. Click *vSphere*.
   The *vSphere Credentials* page is displayed.
4. To view the vSphere credential details, do one of the following:
   a. Click on the corresponding credential name, or,
   b. From the *Actions* list, select *View*
      The vSphere page of that credential is displayed.

The vSphere page contains the following tabs:

- **Details**: Contains details about the vSphere credential, related patterns, and integration results.
- **Credentials**: Displays the available vSphere credentials. The tab also displays the available number of credentials in brackets.
- **Queries**: Displays the list of queries related to the patterns.

To see the vSphere credential details, click on a tab. The following table describes the fields for each tab:

<table>
<thead>
<tr>
<th>Details</th>
<th>This tab has the following sections:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Details:</td>
</tr>
<tr>
<td></td>
<td>• Name: Name of the credential.</td>
</tr>
<tr>
<td></td>
<td>• Description: A description of</td>
</tr>
<tr>
<td></td>
<td>what the credential does and</td>
</tr>
<tr>
<td></td>
<td>how. For example, <em>vSphere</em></td>
</tr>
<tr>
<td></td>
<td>queries for getting licensing</td>
</tr>
<tr>
<td></td>
<td>information from ESX/ESXi hosts.*</td>
</tr>
</tbody>
</table>

---

**Viewing vSphere credential details**

To view the pattern-populated vSphere credential details:

<table>
<thead>
<tr>
<th>Name</th>
<th>The name of the vSphere credential. This field is a link to the Details tab on the vSphere page which contains details about the vSphere credentials, associated patterns, and queries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of credential. The type is displayed as vSphere.</td>
</tr>
<tr>
<td>Credentials</td>
<td>Displays the number of credentials. This field is a link to the Credentials tab on the vSphere page which contains details about the credential.</td>
</tr>
<tr>
<td>Queries</td>
<td>Displays the number of queries associated with the credential. This field is a link to the Queries tab on the vSphere page which contains details about the queries.</td>
</tr>
<tr>
<td>Actions</td>
<td>A list with the following options:</td>
</tr>
<tr>
<td></td>
<td>• View: Select this to view the details of the credential. For more information, see #Viewing vSphere credential details.</td>
</tr>
<tr>
<td></td>
<td>• Edit: You can select this to update existing vSphere credentials. However, the recommended procedure to edit vSphere credentials is from the Devices tab. For more information about editing vSphere credentials from the Devices tab, see Configuring vSphere credentials.</td>
</tr>
<tr>
<td></td>
<td>• Delete: This is a dimmed field.</td>
</tr>
</tbody>
</table>
**Adding vSphere credentials**

The recommended procedure to add new vSphere credentials is from the **Devices** tab. For more information about adding vCenter credentials from the **Devices** tab, see Configuring vSphere credentials.
Updating vSphere credentials

The recommended procedure to edit existing vSphere credentials is from the Devices tab. For more information about editing vSphere credentials from the Devices tab, see Configuring vSphere credentials.

Testing vSphere credentials

To test a vSphere credential:

1. On the vSphere Credentials page, click the credential to test. The vSphere details page is displayed.
2. Click the Credentials tab.
3. From the Actions list, click Test. A dialog box is displayed with the the credential values, and a field in which you enter the IP address against which to test the credential.
4. Enter the target IP address to test.
5. Click Test. The page is refreshed to show that the test in progress and when complete, the results are shown on the Device Credentials page; this may take a few minutes.

Configuring mainframe credentials

The Mainframe credentials tab is a holder for the mainframe credentials. This tab enables you to view, edit, add, and test mainframe credentials.

Viewing mainframe credentials

To view the mainframe credentials, perform the following:

1. From the Discovery home page, click Credentials.
2. Click Management Systems.
3. Click Mainframe. The mainframe credentials page displays credentials checked in sequence, and the first matching entry is used. After a working mainframe credential is found, further credentials are not checked. To reorder mainframe credentials, drag the credential to the required position in the list.

The mainframe credentials are shown in color-coded boxes. The colors represent the level of login success achieved with that credential:
   a. Green: 100% success rate.
   b. Yellow: partial success.
   c. Blue: the credential has never been used.
   d. Red: 0% success rate.

The following information is shown for each credential:
### Editing mainframe credentials

To update an existing mainframe credential, perform the following:

1. From the mainframe credentials page, do one of the following for the credential:
   a. On the credentials list, click on the credential, or
   b. From the **Actions** list, click **Edit**

2. You can then update the mainframe credential as follows:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
</table>
   | IP Range   | Enter the IP range for which this credential will be used. This option can be one of the following:  
   |            | - IP address: for example, 10.10.10.3  
   |            | - Range of IP addresses: for example, 10.10.10.* or 10.10.1–5.* or 10.10.10.0/24  
   |            | - Regular expression: for example, .* or 10.10.10.23|25)  
   
   | Username   | Enter the z/OS username with which to log in to the mainframe computer. |
   
   | Set password | When updating a credential, the password is shown as a series of asterisks in this field and it cannot be edited. To enter a new password, select the checkbox. The password entry field is cleared. Enter the password into the password entry field; the password text is not echoed to the screen. |
   
   | Description | Enter a free text description of the credential. |
   
   | Custom Mainframe Host Server Port | The port to use to connect to the mainframe. By default this is 3940. To use a different port, select the **Enable custom mainview port?** check box and choose a port number from the list. The list is populated with port numbers specified on the **Discovery Configuration** page. |

3. To save the details, click **Apply**.
Adding mainframe credentials

To add a credential for a mainframe computer:

1. From the Discovery home page, click **Credentials**.
2. Click **Management Systems**.
3. Click **Mainframe**.
4. Click **Add**.
5. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| IP Range            | The IP range for which this credential will be used. This option can be one of the following:  
|                     | • an IP address (10.10.10.3)  
|                     | • a range specification (10.10.10.* or 10.10.1-5.* or 10.10.10.0/24)  
|                     | • a regular expression matching an IP address (.* or 10.10.10.(23|25))  
| Username            | The z/OS username with which to log in to the mainframe computer.          |
| Password            | The password corresponding to the username above.                          |
| Description         | Enter a free text description of the credential.                          |
| Custom Mainframe    | The port to use to connect to the mainframe. By default this is 3940. To use a different port, select the Enable custom mainview port? checkbox and choose a port number from the list. The list is populated with port numbers specified on the Discovery Configuration page. |
| Host Server Port    |                                                                             |

6. To save the details, click **Apply**.

### Testing mainframe credentials

**Recommendation**

You should confirm that the BMC Discovery for z/OS Agent is installed and functioning correctly with the credential testing tool before attempting discovery of the mainframe as the test includes a number of diagnostics. Problems with configuration are much simpler to resolve using this approach.

To test an existing mainframe credential:

1. From the mainframe credential list, select **Actions => Test**.
2. Enter the IP address for which you want to test credentials.
3. Click **Test**.
   
   The ***Management System Credentials*** page is displayed showing the test in progress.
4. When the test completes, the page is refreshed with the result.
   
   You are shown whether the test ultimately resulted in a success or a failure. By clicking through the state link you can view the results of the credential test in more detail.
This screen illustrates how to view more detailed results of the credential test.

The credential test result page shows the discovery methods enabled in BMC Atrium Discovery, whether corresponding views are detected in the Discovery for z/OS agent, and the z/OS agent version.

Testing mainframe credentials

The mainframe credential test page

You can test mainframe credentials using the mainframe credential tests page.

To test mainframe credentials:

1. Click on the Discovery tab.
2. Click Credentials.
3. Click Management System.
4. Click Mainframe Credential Tests.

The mainframe credential test page is displayed.

Mainframe Credentials Test page.

The mainframe credential test page displays the credential tests that are currently in progress and the tests run in the last ten minutes. You can delete completed tests, or run them again. However, you cannot cancel tests that are currently in progress. You can also test whether credentials exist for any IP address on your network.

- To delete a completed credential test, in the Actions column, click Delete.
- To run a credential test again, in the Actions column, click Retry.

Testing mainframe credentials for an arbitrary IP address

You can test whether BMC Atrium Discovery can access any mainframe IP address on your network. You do not need to have previously scanned the IP address. This way you can verify whether any of your existing mainframe credentials will allow you to access this IP.

To test mainframe credentials for an arbitrary IP Address, perform the following:
1. From the mainframe credential test page, click Test IP Access... at the bottom right corner of the page.
   The Test Management System Credentials dialog box is displayed.
2. Enter the IP address for which you want to test credentials.
3. Click Test.
   The mainframe credential test result page is displayed showing the test in progress.

When the test completes, the page is refreshed with the result. You are shown whether the test ultimately resulted in a success or a failure. You can view the results of the credential test in more detail by clicking through the success or failure links under State.

Managing the credential vault

BMC Atrium Discovery stores all passwords used to access customer devices in a secure credential vault. A secure credential vault is generated when the appliance is commissioned. The contents of the vault is encrypted, and can be secured using a passphrase.

The credential vault can be open or closed. If no passphrase is set, the vault is opened automatically when Discovery starts. If a passphrase has been set, you will be prompted to enter it before Discovery can begin. While the Vault is open, BMC Atrium Discovery can use the credentials stored in it to access devices.

When Discovery is stopped, the vault is automatically closed if a passphrase is set. You can close the Vault while Discovery is in progress. This will prevent access to further devices during the current Discovery runs.

When the state of the credential vault is changed, that is, when a passphrase is added or changed, or the vault is opened or closed, the system creates a backup copy. When adding a passphrase, the vault is protected, however, the backup copy of the vault is made before the passphrase is added, so is unprotected. Similarly when a passphrase is changed, the backup copy still has the old passphrase. You should delete or protect the backup copy in line with your organization's security procedures.

To manage the credential vault

From the Discovery section of the Administration tab, select Vault Management.
From this page you can open or close the credential vault and specify a passphrase to secure it. You can also change the passphrase or remove it.

Setting a passphrase

To set a passphrase:

1. Enter the new passphrase in the New Passphrase field.
2. Repeat it in the verify New Passphrase field.
3. Click Set Passphrase.
   The passphrase is now set.
Changing a passphrase

To change a passphrase:

1. Enter the new passphrase in the New Passphrase field.
2. Repeat it in the Verify New Passphrase field.
3. Click Change Passphrase.
   The passphrase is now changed.

⚠️ Setting or changing a passphrase does not change whether the vault is open or closed.

Clearing a passphrase

To clear a passphrase:

1. Enter the current passphrase in the Current Passphrase field.
2. Click Clear Passphrase.
   The passphrase is now cleared.

Opening the credential vault

To open a closed credential vault:
Enter the passphrase and click Open the Vault.
You are requested to confirm the operation.

You can also open the credential vault from the Discovery Status page. When Discovery is not running and the vault is closed, a Passphrase entry box is displayed above START LOCAL SCANS.

Closing the credential vault

To close the vault, it must be open and have the passphrase set:
Enter the passphrase and click Close the Vault.
You are requested to confirm the operation.

You can also close the vault from the Discovery Status page. When Discovery is running and a passphrase is set, stopping Discovery also closes the vault.

Monitoring credential usage

In previous versions of BMC Atrium Discovery, it was difficult to quickly obtain an overview of the currency of configured credentials. In this version, each tab on the Login Credentials, Windows proxy Management, and SNMP Credentials pages shows credentials in color coded boxes. The colors represent:

- **Green**: 100% success rate
- **Yellow**: partial success
• **Blue**: the credential has never been used
• **Red**: 0% success rate

Where a credential has been used successfully, a link showing the number of successful uses is displayed. If there is a single use then it links to the DiscoveryAccess page for that credential use. If there are multiple uses, it links to a list of DiscoveryAccess pages. Where a credential has failed periodically but has been used successfully, a link is provided to the last successful Discovery Access, and links are also provided to a list of Session Results for failure cases.

Where a credential has never been used successfully there is a link to the SessionResult page for that attempted access, as illustrated in the following figure:

This screen illustrates links to successful Discovery Access attempts.

**Credential Windows proxy note**

The Credential Windows proxy uses credentials defined on the Login Credentials page, so the usage statistics display in the Login Credentials page, rather than the Windows proxy Management page.

**DiscoveryAccess page**

A DiscoveryAccess is a single access to a Discovery Endpoint. When an endpoint is scanned, a DiscoveryAccess node is created which records information on the interaction that BMC Atrium Discovery has with that endpoint. When BMC Atrium Discovery is unable to access a host, the DiscoveryAccess is a good starting point for troubleshooting.

**To view a DiscoveryAccess page**

You can view DiscoveryAccesses from a number of places in the user interface.

**From a Host Node**

From the view page for a host node:

1. Scroll down to the Inference section
2. Click the main link in that section, for example: 172.17.3.116 SUCCESS 09/12/2008 10:48 - 09/12/2008 10:55
The Example DiscoveryAccess is shown.

From the Discovery Recent Runs page
From the Recent Runs tab of the Discovery Status page:

1. Click a discovery run.
2. Scroll down to the Endpoint field.
3. Click the DiscoveryAccess link. If it is a link to a single DiscoveryAccess, then that Example DiscoveryAccess is shown. If there are multiple DiscoveryAccesses, then a list page is displayed.
4. Click a DiscoveryAccess line to view the Example DiscoveryAccess.

Example DiscoveryAccess
The following screens show DiscoveryAccess pages for a Unix host, a Windows host, a network device, and a mainframe computer.

This screen illustrates a DiscoveryAccess page for a Unix host.
This screen illustrates a DiscoveryAccess page for a Windows host.

This screen illustrates a DiscoveryAccess page for a network device.

This screen illustrates a DiscoveryAccess page for a mainframe computer.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint Section</strong></td>
<td></td>
</tr>
<tr>
<td>Endpoint</td>
<td>The endpoint (IP address) scanned in this discovery access.</td>
</tr>
<tr>
<td>Start Time</td>
<td>The time at which the scan started.</td>
</tr>
<tr>
<td>End Time</td>
<td>The time at which the scan finished.</td>
</tr>
<tr>
<td>Total Duration</td>
<td>The time it took to discover and process the data, that is, the time between Start Time and End Time.</td>
</tr>
<tr>
<td>Discovery Run</td>
<td>A link to the Discovery Run that this DiscoveryAccess is part of.</td>
</tr>
<tr>
<td>Previous Discovery Access</td>
<td>A link to the previous DiscoveryAccess with the same endpoint. Not displayed if this is the first in a list.</td>
</tr>
<tr>
<td>Next Discovery Access</td>
<td>A link to the next DiscoveryAccess with the same endpoint. Not displayed if this is the last in a list.</td>
</tr>
<tr>
<td>Device Summary</td>
<td>An read-only summary showing the Host Type, Discovered OS Type, and Discovered OS Version. For example, Unix Server, Debian Linux, 4.0.</td>
</tr>
<tr>
<td>Host</td>
<td>A link to the host that was created or updated as part of the scan. Not displayed if no host was created or updated.</td>
</tr>
<tr>
<td><strong>Status Section</strong></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>The current state of the DiscoveryAccess. This may be Started or Finished.</td>
</tr>
<tr>
<td>End State</td>
<td>The end state of the discovery run. This may be one of the following:</td>
</tr>
<tr>
<td></td>
<td>Successful discovery results in GoodAccess; during processing you may see first DeviceIdentified and later HostInferred.</td>
</tr>
<tr>
<td></td>
<td>For optimised discovery, that is, started but stopped for a reason, you may see Opt1stScan, OptNotBestIP, OptRemote, OptAlreadyProcessing.</td>
</tr>
<tr>
<td></td>
<td>For unsuccessful discovery you may see NoResponse, UnsupportedDevice, NoAccess, Excluded, Error.</td>
</tr>
<tr>
<td>Result</td>
<td>The result of the DiscoveryAccess. This may be Skipped, NoResponse, Success, NoAccess, or Error.</td>
</tr>
<tr>
<td>Errors</td>
<td>If there were any errors detected by the ECA engine during discovery this will link to those errors. Examples are:</td>
</tr>
<tr>
<td></td>
<td>• Error detected by the ECA engine: This is typically an internal rule error or pattern error. Usually triggered when the data returned does not match what is expected.</td>
</tr>
<tr>
<td></td>
<td>• Unable to get the deviceInfo: ExecutionFailure:Discovery has attempted to run a command but a failure has been reported.</td>
</tr>
<tr>
<td></td>
<td>• Unable to get the deviceInfo: NoAccessMethod: No access method, this is frequently because it is not meaningful, such as getting patches on Linux.</td>
</tr>
<tr>
<td></td>
<td>• Unable to get the deviceInfo: NoSuchDevice: There is a NoResponse endstate. That is, nothing detected on the IP address.</td>
</tr>
<tr>
<td></td>
<td>• Unable to get the deviceInfo: TRANSIENT CallTimedout: Probably caused by the reasoning timeout; the call to discovery is taking too long to complete.</td>
</tr>
<tr>
<td></td>
<td>• Unable to get the deviceInfo: UNKNOWN: Some other CORBA error. Contact Customer Support.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Session Results</td>
<td>If there were any failures attempting to get a session on the endpoint this will link to a list of failures and successes. See below for details.</td>
</tr>
<tr>
<td>Discovery Details Section</td>
<td></td>
</tr>
<tr>
<td>Data Source</td>
<td>Does this Discovery Access originate from this appliance, come from a scanning file, or was it consolidated from a scanning appliance.</td>
</tr>
<tr>
<td>Credential Used</td>
<td>A link to the Windows proxy or Credential used to in this Discovery Access. The link name is a hash of details of the credential; it does not provide the credential itself. You are not shown the Credential pages if you do not have permissions to view them. This field is not displayed as a link on the consolidation appliance for scans which have been consolidated from a scanning appliance.</td>
</tr>
<tr>
<td>Discovery Start Time</td>
<td>The time at which discovery started on the scanning appliance. This field is only displayed on the consolidation appliance for scans which have been consolidated from a scanning appliance.</td>
</tr>
<tr>
<td>Discovery End Time</td>
<td>The time at which discovery completed on the scanning appliance. This field is only displayed on the consolidation appliance for scans which have been consolidated from a scanning appliance.</td>
</tr>
<tr>
<td>Session Establishment Duration</td>
<td>The time it took to establish the session, that is, to log onto the host.</td>
</tr>
<tr>
<td>Total Discovery Duration</td>
<td>The time taken to establish a session and run commands.</td>
</tr>
<tr>
<td>On Hold Since</td>
<td>If the discovery is currently paused, the time at which it was paused.</td>
</tr>
<tr>
<td>On Hold Duration</td>
<td>If the discovery has been paused, the elapsed time since it was paused.</td>
</tr>
<tr>
<td>Standard Discovery Method</td>
<td>The discovery method used. This is one of: getDeviceInfo, getHostInfo, getInterfaceList, getProcessList, getPackageList, getPatchList, getNetworkConnectionList, getHBAInfo, and getNames.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the discovery access for the method. This is OK or the failure reason.</td>
</tr>
<tr>
<td>Script</td>
<td>The name of the script used, if any.</td>
</tr>
<tr>
<td>Access</td>
<td>The access method used to connect to the endpoint (for example, ssh, telnet, rlogin, and so on.</td>
</tr>
<tr>
<td>Result</td>
<td>A link to the node or nodes created by this discovery method.</td>
</tr>
<tr>
<td>Additional Discovery Method</td>
<td>The additional discovery method used. These are discovery methods called by patterns, for example:</td>
</tr>
<tr>
<td></td>
<td>• getFileInfo</td>
</tr>
<tr>
<td></td>
<td>• getFileMetadata</td>
</tr>
<tr>
<td></td>
<td>• runCommand</td>
</tr>
<tr>
<td></td>
<td>• getDirectoryListing</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the discovery access for the method. This is OK or the failure reason summarised into links.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Script</td>
<td>The name of the script used.</td>
</tr>
<tr>
<td>Access</td>
<td>The access method used to connect to the endpoint. For example: ssh, telnet, rlogin, etc.</td>
</tr>
<tr>
<td>Result</td>
<td>A link to the node or nodes created by this discovery method.</td>
</tr>
</tbody>
</table>

**DiscoveryAccess state**

The following table shows the possible discovery scenarios and the resulting `end_state` and `result` attributes of the DiscoveryAccess node:

In addition to `end_state` and `result` attributes on the DiscoveryAccess there is also a `reason` attribute that contains further details. There is no fixed set of values for `reason`.

The following state diagram and table may be of use understanding the results of an attempted access.

**This screen illustrates the result of an attempted access of a DiscoveryAccess node.**

<table>
<thead>
<tr>
<th>Discovery Scenario</th>
<th>Resulting State of DiscoveryAccess</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Injected In Exclude list</td>
<td>end_state=Excluded result=Skipped</td>
</tr>
<tr>
<td><em>Example:</em> The user has requested a scan of an IP that is in an exclude range.</td>
<td></td>
</tr>
<tr>
<td>IP Injected Already Processing this IP</td>
<td>end_state=OptAlreadyProcessing result=Skipped</td>
</tr>
<tr>
<td><em>Example:</em> The user has requested a scan of an IP that is currently being processed as part of an earlier scan.</td>
<td></td>
</tr>
<tr>
<td>IP Injected Second Scan Optimization (Best IP)</td>
<td>end_state=OptNotBestIP result=Skipped</td>
</tr>
<tr>
<td><em>Example:</em> The user has requested a scan of an IP that is on a host that has already been scanned using another IP address that is considered to be the best IP to use to scan that host.</td>
<td></td>
</tr>
<tr>
<td>IP Injected No IP Response</td>
<td>end_state=NoResponse result=NoResponse</td>
</tr>
<tr>
<td><em>Example:</em> No response was received from the scanned IP address.</td>
<td></td>
</tr>
<tr>
<td>IP Injected IP Response</td>
<td>end_state=DeviceIdentified result=Success</td>
</tr>
<tr>
<td><em>Example:</em> After a sweep scan of an IP address, Discovery has received a response. No identification has taken place other than that there is a device of some description that has responded to the sweep scan. If the device is subsequently not recognised then the <code>end_state</code> is set to <code>UnsupportedDevice</code> as below.</td>
<td></td>
</tr>
<tr>
<td>IP Injected IP Response Device Type not supported</td>
<td>end_state=UnsupportedDevice result=Skipped</td>
</tr>
<tr>
<td>UnsupportedDevice is the default <code>end_state</code> for any device that we can detect but do not have any knowledge of in Reasoning to build an inferred node. We may still be able to identify what the device</td>
<td></td>
</tr>
</tbody>
</table>
Discovery Scenario | Resulting State of DiscoveryAccess
---|---
is and some key properties, or we may know nothing more than the fact it returned a ping. Example: Discovery has received a response from an endpoint but has not been able to identify the device further. This may mean that the OS is unrecognised, garbage has been returned or there is a shell error. This can be caused by a firewall. For more information, see the IP Fingerprinting information in the Base Device Discovery section.

| IP Injected | IP Response | No HostInfo recovered | end_state=NoAccess | result=NoAccess |
| IP Injected | IP Response | No InterfaceList recovered | end_state=NoAccess | result=NoAccess |
| IP Injected | IP Response | HostInfo and InterfaceList recovered | end_state=HostInferred | result=Success |
| IP Injected | IP Response | HostInfo and InterfaceList recovered First Scan Optimization | end_state=Opt1stScan | result=Skipped |
| IP Injected | IP Response | HostInfo and InterfaceList recovered First Scan Optimization not needed | end_state=GoodAccess | result=Success |
| IP Injected | Traceback captured | | end_state=Error | result=Error |
| IP Consolidated when originally optimized on Discovery Appliance | | | end_state=OptRemote | result=Skipped |

Troubleshooting using session results

There are three scenarios that are highlighted using Session Results:

- Initial scan and successful connection: a number of unsuccessful connection attempts followed by a successful connection shows BMC Atrium Discovery selecting credentials.
- Failure to connect: BMC Atrium Discovery was unable to connect. Typical problems could be failed credentials or poor network connectivity.
- Failure at start of scan before successful connection: this can occur when a credential fails (expiry) but a later credential is successful.

Checking credentials after a failure

1. From the Discovery Access, click the session results link.
2. Click the Connection timed out rows to display the SessionResult page for that specific login attempt.

This page shows information on the attempted login, including a credential link and a link to the DiscoveryAccess. The credential link is a hash of the credential name which links to that credential in the Login Credentials page only if you have sufficient permissions to view the credentials.
3. Click the test button. If the credential tests successfully, it is likely that a transient network problem caused the connection time-out. Alternatively, you can navigate back to the Discovery Access page and rescan from the Discovery Actions menu.

**Consolidation**

Consolidation refers to the centralization of discovery data from scheduled or snapshot scans on multiple *scanning* appliances to one or more *consolidation* appliances. You might want to use consolidation in the following scenarios:

- **Firewalled environments**: When an environment is divided by firewalls so that a single appliance is unable to reach all parts, a scanning appliance can be situated on each section of the network blocked by a firewall. The scanning appliances can all feed back data to a central consolidation appliance.
- **Restricted (policy) networks**: Certain lines of business might enforce policies on the control of IT infrastructure in their environments. Where such policies limit or prohibit access, scanning appliances can be deployed which all feed back data to a central consolidation appliance.
- **Restricted (time) scanning windows**: Where a discovery window is short, a single appliance may be unable to complete a scan of a large range of IP addresses during the permitted time. Sharing the IP addresses between multiple scanning appliances means each smaller scan can be completed in less time, and the results can be consolidated and viewed on the consolidation appliance.

In each of these situations, multiple scanning appliances can be deployed, and their data consolidated into a central consolidation appliance. The consolidation appliance is then used for reporting and provides a coherent view of the entire scanned network. A consolidation appliance must be set as one which accepts connections or feeds from scanning appliances. Scanning appliances must in turn register with a consolidation appliance.

**Consolidation Appliance**: The main purpose of the consolidation appliance is to report on data consolidated from a number of other scanning appliances. It can also perform normal/discovery, although this is not recommended.

**Scanning Appliance**: The scanning appliance also operates as a normal/standalone appliance. The only difference is that it constantly sends discovery data to the consolidation appliance. After setting up, this process is transparent to the user. A scanning appliance must request and be approved on a consolidation appliance before it can send any consolidation data to that appliance. This is described in Approving or rejecting a scanning appliance request.

On the consolidation appliance user interface, the **Discovery Currently Processing Runs** tab shows any local scans and any consolidation runs in progress. The **Discovery Currently Processing Runs** is described in The Discovery Status page. The tab is shown below:
This screen illustrates the discovery status page for a consolidating appliance.

What is consolidated?

The consolidated data is the BMC Atrium Discovery Directly Discovered Data (DDD) Nodes including the data collected by the patterns. The data inferred by the scanning appliances, for example, SoftwareInstance nodes, is not consolidated, but the consolidation appliance will infer it again (based on its pattern configuration).

⚠️ TKU release, patterns, CSV imports and consolidation

The TKU release package and custom patterns that are loaded on the scanning and consolidation appliances must be the same in order to infer the same data, for example, SoftwareInstance nodes. This is not enforced in any way by the system. The data imported via CSV in a scanning appliance will not be consolidated. It has to be imported in the consolidation appliance too.

Restrictions

BMC Atrium Discovery version 9.0 introduced major changes in the data model. As a result of these model changes, you cannot consolidate BMC Atrium Discovery version 9.0 appliances with any previous version. If you try to do so, warning messages are shown on the version 9.0 appliance UI. If, while using an earlier version, you attempt to register with a version 9.0 appliance, the attempt fails with an authentication error shown in the earlier version's UI.

For pre-version 9.0 consolidating systems, the consolidator version should be at least the same version as the scanning appliances. This is not enforced by the system.

Integration points and consolidation

A consolidation appliance is capable of performing discovery although this is not recommended. The one situation in which a consolidation appliance does perform discovery is where an integration point request fails on the scanning appliance. In this case, the consolidation appliance will attempt to perform the integration point request on the discovery target.

Configuring consolidation

Configuring consolidation is a two step procedure. Initially the appliance which is to be the consolidation appliance must be set as a consolidation appliance, and then one or more scanning appliances register with the appliance. To configure consolidation you need the permissions detailed in Consolidation Permissions.
Firewalls and consolidation

Consolidated appliances use port 25032 to communicate. The scanning appliance must be able to connect to port 25032 on the consolidation appliance. You must configure any firewalls between scanning appliances and consolidation appliances to allow this traffic.

Consolidation appliances communicate using port 25032, and the port is open whether or not an appliance is configured as a consolidation appliance. Therefore you cannot, for example, telnet to the appliance IP address and port 25032 to determine whether it is a consolidation appliance.

To set an appliance as a consolidation appliance

1. From the Discovery section of the Administration tab, select Discovery Consolidation. The Consolidation page is displayed. You cannot use consolidation if the appliance is named Discovery_Appliance. A warning is displayed including a link to where you can change the appliance name.
2. In the Consolidation page, click Set as Consolidation Appliance. The appliance is now configured as a consolidation appliance.

To set an appliance as a scanning appliance

1. From the Discovery section of the Administration tab, select Discovery Consolidation.
2. In the Consolidation page, click Set as Scanning Appliance.

This dialog enables you to specify a Consolidation target. Enter or edit the following information in the dialog:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the scanning appliance. Names must be unique in the consolidation network and you cannot consolidate a scanning appliance with the default name, Discovery_Appliance. The name is taken from the Administration =&gt; Appliance Configuration =&gt; Identification page. See Initial configuration. A change link is provided which displays the Identification page. In the identification page you can change the name of the appliance. You can only consolidate appliances which have unique names.</td>
</tr>
<tr>
<td>Consolidation Appliance</td>
<td>The IP address or the hostname of the target consolidation appliance.</td>
</tr>
</tbody>
</table>

⚠️ You can supply credentials for the consolidation appliance in this dialog. If you supply valid credentials here, the scanning appliance is approved automatically.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user name for a user on the consolidation appliance. This user must have appropriate permissions to approve the connection of the scanning appliance to the consolidation appliance.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user on the consolidation appliance.</td>
</tr>
</tbody>
</table>

If you supplied valid credentials for automatic approval on the consolidation appliance, then the scanning appliance is now configured and working as a scanning appliance.
This screen illustrates a successful working scanning appliance.

**Approving or rejecting a scanning appliance request**

After a request (without automatic approval) has been made from a scanning appliance, it requires approval on the consolidation appliance.

To approve or reject a pending scanning appliance request:

1. From the Administration tab on the consolidation appliance, select **Discovery Consolidation** from the Discovery section.

   In the following example, the "Tideway05" appliance has requested to become a scanning appliance.

   ![Diagram](image)

   **This screen illustrates the Tideway05 appliance has requested to become a scanning appliance.**
   - To accept the appliance connection, click **Approve**.
   - To reject the request, click **Reject**. When you do this, the connection is deleted from the consolidation appliance and when no connections remain the scanning appliance reverts back to a non-consolidated appliance.

**When consolidation is running**

Once consolidation has been set up, whatever scanning takes place on the scanning appliance is automatically sent to the consolidation appliance as soon as possible after the scan of an endpoint is complete. On the consolidation appliance, runs are displayed that are marked specifically as consolidation runs and can be viewed from the **Discovery Status page**.

Discovery must be running on the consolidation appliance for consolidation to take place. If Discovery is not running, the consolidation appliance will refuse to accept data from the scanning appliance. The scanning appliance will attempt to resend data later. Also, if Discovery is stopped on the consolidation appliance, it will stop consolidating any data it has already received.

**Canceling consolidating discovery runs**

You can cancel a consolidating discovery run from the scanning appliance or from the consolidation appliance. Where possible you should always cancel the discovery run on the scanning appliance. This is done by selecting the discovery run on the **Discovery Status page** of the scanning appliance and clicking **Cancel Runs**.
Canceling the discovery run at the scanning appliance enables the consolidation appliance to receive data from the scanning appliance. This stops the scan rather than the consolidation so that the two appliances' data remains consistent.

**Warning:** Canceling a consolidation run on the consolidation appliance stops the consolidation though the scan continues on the scanning appliance. This leads to inconsistencies between the data on the two appliances. Where possible you should always stop the scan on the scanning appliance and allow the consolidation to run to completion.

If you must cancel a consolidation run from the consolidation appliance, you can do so by selecting the discovery run on the Discovery Status page of the consolidation appliance and clicking **Cancel Runs**.

### Using appliance snapshot with consolidated appliances

When an appliance is part of a consolidation network, you can use appliance snapshot to backup the appliance datastore and configuration files as normal. This feature can be used for both consolidation and scanning appliances.

#### Scanning appliance

When you take a snapshot of a scanning appliance, the following steps take place:

1. Maintenance mode
2. Snapshot invoked
3. Transmission of any unsent consolidation data is halted
4. Snapshot takes place
5. Transmission of unsent consolidation data restarts

#### Consolidation appliance

When you take a snapshot of a consolidation appliance, the following steps take place:

1. Maintenance mode
2. Snapshot invoked
3. Incoming consolidation data and requests for approval of scanning appliances is rejected until the snapshot is complete. The scanning appliances continue to attempt to send data, but the connection times out on each attempt, and the data is resent
4. Snapshot takes place
5. Incoming consolidation data and requests for approval of scanning appliances are now accepted
6. The scanning appliances send consolidation data until the data queue is clear
Replacing an appliance

When an appliance has been replaced after a hardware failure, you can restore a snapshot of the appliance datastore and configuration files as normal. However, if the snapshot was taken during consolidation activity, there may be part completed consolidation runs and unsent data on the systems.

- Use the same IP address and identifier for the replacement appliance as the failed appliance was using.
- On the consolidation appliance, cancel any in progress consolidation runs.
- Test the connections.

If you had to change the IP address or identifier:
On the consolidation appliance:

- Cancel any in progress consolidation runs.

On the scanning appliance:

- Stop any discovery runs.

Pattern management

The Pattern Management UI enables you to upload patterns to the appliance, activate or deactivate patterns on the appliance, and to delete patterns which are no longer required. You can also download a zip archive of all patterns that are on the appliance. The following terms are used in the Pattern Management UI:

- **Pattern**: a sequence of commands written in the Pattern Language (TPL), which contain instructions that identify scanned entities which are then used to create the BMC Atrium Discovery data model.
- **Package**: a text file written in TPL which contains one or more patterns, or a zip archive of TPL files which contain one or more patterns.
- **Module**: the logical grouping to which patterns belong. For example, the following patterns are all in the **VMWareVM module**:
  - VMware
  - VMwareConsolidateFromSI
  - VMwareConsolidateFromVirtualHost

This is an example package name: **VMWareVM. VMwareConsolidateFromSI**
Activating a pattern means that it is loaded and from then will be used to identify software instances. You cannot activate a pattern with a lower version number than one that has previously been activated. Delete the pattern with the higher version number first. All patterns specify the TPL version number that they use. If a pattern uses TPL language features which are from a later TPL version than specified, you cannot activate that pattern.

This page describes the management of packages through the UI. Configuring and editing the actual packages and patterns is described in Pattern configuration and editing.

**Viewing details of all installed packages**

All currently installed patterns can be viewed from this page in read-only format. To access the Installed Knowledge Updates page; from the Discovery tab, select Pattern Management.

The Upload New Package and Pattern Template headings are controls which hide additional sections of the page. Click these to display sections which enable you to:

- Upload a New Package: see Uploading a TPL package to the appliance.
- Manage Pattern Templates: see Using pattern templates.

The following links are provided:

- Download all Patterns (Zip): enables you to download a zip file of all patterns on the appliance.
- View Configuration of all Patterns: links to the All Pattern Module Configurations page which lists all patterns with configurable items.

For each installed pattern, the following columns are displayed:

- **Name**: the name of the package. This is the name specified when the package was uploaded.
- **Description**: brief description of the package. This is the description entered when the package was uploaded.
- **State**: whether the pattern is Active or Inactive. If a pattern is Active, it is in use and will create data in the BMC Atrium Discovery model when triggered. If a pattern is Inactive, it is not in use and will not run.
- **Pattern Modules**: shows the number of modules contained in the package. If any pattern modules have been disabled, then this is shown in brackets after the total.

**Uploading a TPL package to the appliance**

A TPL package can be a zip archive of pattern files, or a single TPL file containing one or more patterns.
TKU packages contain multiple components, not simple a zip archive of TPL patterns. These should be uploaded and activated using the Knowledge Update page.

1. To upload a package, click **Upload New Package**.
2. Enter the pattern filename into the **Upload New Package** dialog box, or click **Browse** to locate a file. The **Name** field is automatically populated with the file name without the .tpl suffix. You can enter a description of the pattern into the **Description** field, this description is displayed in the UI.
3. To upload the file to the appliance, click **Upload**.
4. The pattern is uploaded to the appliance and is placed in the Inactive state. Before you can use the pattern you will need to Activate it.

**Uploading and activating a TPL package**

You can also upload and activate a package simultaneously. You may prefer to use this method when testing patterns. To do this, enter the package details as above and click **Upload & Activate**. The window is refreshed and the newly uploaded package is shown as Active.

**Using pattern templates**

Pattern templates are supplied with BMC Atrium Discovery to provide a starting point from which to model Software Instances and applications.

1. To view the pattern templates that are available, click **Pattern Templates**.
2. In the Pattern Templates window is a table with each row corresponding to a template pattern. For each pattern the following information or link is displayed:
   - **Name**: the name of the pattern. This is a link to the View Pattern template window. This is described in The View Pattern Template Window.
   - **Description**: a read only description of the pattern.
   - **Options**: a Download link. Clicking this enables you to download a copy of a particular pattern to your local filesystem.
     There is also a Download All Patterns (Zip) link which enables you to download a zip archive of all of the template patterns.

**Viewing pattern template window**

The View Pattern Template Window shows a read only version of the pattern with syntax highlighting where TPL keywords and variables are displayed in different colors to the other text. The Turn Line Numbering On/Turn Line Numbering Off button toggles line numbering can be used to ease copying and pasting text from one of the templates. A button to close the window is also provided.

**Managing packages on the appliance**

You can activate, deactivate, and delete packages which are on the appliance.
Activating a TPL package

To activate a package:

1. Select an Inactive package from the package list, using the selection checkbox on the left of the row containing the package. You can select multiple patterns, or by selecting the checkbox in the table heading, you can select all patterns.
2. Click **Activate**.
   The window is refreshed to show an Items Marked for Action pane.
3. You can validate the pattern to ensure that there are no problems with the pattern. To do this, click **Validate All Listed Changes**.
4. If no problems are found with the pattern, the pane is refreshed with a The Requested Changes were Successfully Validated message.
5. To complete the activation of the package, click **Commit All Listed Changes**.

Deactivating a TPL package

To deactivate a package:

1. Select an Active package from the package list, using the selection checkbox on the left of the row containing the package. You can select multiple patterns, or by selecting the checkbox in the table heading, you can select all patterns.
2. Click **Deactivate**.
3. The window is refreshed to show an Items Marked for Action pane.
   You can validate the pattern to ensure that there are no problems with deactivate the pattern. To do this, click **Validate All Listed Changes**.
4. If no problems are found, the pane is refreshed with a The Requested Changes were Successfully Validated message.
5. To complete the deactivation of the package, click **Commit All Listed Changes**.

Deleting a TPL package

To delete a package:

1. Select a package from the package list, using the selection checkbox on the left of the row containing the package. You can select multiple patterns, or by selecting the checkbox in the table heading, you can select all patterns.
   If you select an active pattern for deletion, it is deactivated and deleted when you commit the changes.
2. Click **Delete**.
   You can validate the operation to ensure that there are no problems with the deletion. To do this, click **Validate All Listed Changes**.
3. If no problems are found, the pane is refreshed with a The Requested Changes were Successfully Validated message.
4. To complete the deletion of the package, click **Commit All Listed Changes**.
**Downloading all TPL packages**

To download all of the packages that are installed on the appliance, click **Download All Patterns (Zip)** above the package list. A Save As dialog box is displayed for you to enter a location to save the file.

**Pattern configuration and editing**

You can make **configuration changes** to patterns and you can **edit** the entire pattern source from the user interface. Installing and managing patterns is described in **Pattern management**.

The packages that are installed on the appliance are shown in the Pattern Management Window, illustrated in the following screen.

![Pattern Management Window](image)

**This screen illustrates the packages selected for installation on the appliance.**

To view one of the packages, click the corresponding row in the Package table. The following buttons are provided on the Package Information page.

- **Deactivate**: deactivates the package.
- **History**: shows a history comparison of the package. The comparison UI is the same as the node comparison which is described in **Comparing the history of nodes**.

The Package Information page shows the following information on the package:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>The name of the package.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether the package is active or inactive. This is shown by a Yes or No.</td>
</tr>
<tr>
<td>Submitting user</td>
<td>The user name of the person submitting the package.</td>
</tr>
<tr>
<td>Submission date</td>
<td>The date that the package was submitted.</td>
</tr>
<tr>
<td>Pattern Module</td>
<td>A link showing the number of modules which links to a page showing all of the modules included in the package.</td>
</tr>
</tbody>
</table>

Click **Pattern Module**. The Pattern Module List window, which lists the pattern modules in the package, is displayed.

Each row in the table is a link to the Pattern Module Source window where you can view the pattern module source. If only one pattern module is in the package, the Pattern Module link leads to the Pattern Module Source window.
**Viewing the pattern module**

To view the pattern module information, configuration options, and source, click the corresponding pattern module row in the table.

If you have sufficient permissions, such as members of the appmodel group, or users with the reasoning/pattern/edit permission, you can edit pattern modules through the Pattern Module window. This is primarily intended for application modeling where repeated editing in a text editor, uploading, activating and so forth may become cumbersome and time consuming. However, when editing through the user interface, the pattern falls outside any change control procedures and becomes tied to a single appliance. For these reasons, it is recommended that the edit function in the user interface is only used for pattern development, rather than maintenance in the field.

**Pattern module information**

The first section of the Pattern Module window shows the following information on the pattern:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>The name of the module. For example, AppServer.Tomcat.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether the pattern module is enabled or disabled. This is shown by a Yes or No.</td>
</tr>
<tr>
<td>Submitting User</td>
<td>The user name of the person submitting the pattern module.</td>
</tr>
<tr>
<td>Submission Date</td>
<td>The date that the pattern module was uploaded to the appliance.</td>
</tr>
<tr>
<td>Activation Date</td>
<td>The date and time that the pattern module was activated.</td>
</tr>
<tr>
<td>Pattern Package</td>
<td>A link to a page showing basic information on the package. This is the page shown in #Package Information Window.</td>
</tr>
<tr>
<td>Pattern</td>
<td>A link to a page showing basic information on the pattern. This is the page shown in #Pattern Management Window.</td>
</tr>
</tbody>
</table>

**Pattern configuration**

Patterns can have configuration blocks defined in the TPL source. This provides a number of items that can be configured through the user interface. For information on TPL configuration blocks, see Pattern Configuration.

Pattern Configuration is shown on the Pattern Module page for modules that contain configuration. The Pattern Configuration section provides a table with the following columns:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The description of the configuration item that can be edited in this row. For example, Default Port.</td>
</tr>
<tr>
<td>Value</td>
<td>The current value of the configuration item that can be edited in this row.</td>
</tr>
<tr>
<td>Default</td>
<td>The default value for the configuration item.</td>
</tr>
<tr>
<td>Pattern Variable</td>
<td>The name of the variable in the TPL pattern that the configuration item controls.</td>
</tr>
</tbody>
</table>

The Pattern Configuration section provides the following buttons:
• **Reset Configuration**: resets the configuration items in the pattern to the default values specified in the pattern.

• **Edit Configuration**: shows the values of configuration items in editable fields. Depending on the variable type being edited, radio buttons, text input fields, or multiple selection boxes are provided.

**To edit a pattern configuration**

To edit a pattern configuration:

1. Click *Edit Configuration*.
2. Make the required changes to the editable fields.
3. Click *Apply* to apply the changes.

You can also edit configurable items in Pattern Modules using the All Pattern Module Configurations page, described in the following section.

**View and edit configuration of all patterns**

You can view all pattern configuration in a central place by clicking the *Discovery* tab, clicking the *Pattern Management* subtab, and then clicking the *View Configuration of all Patterns* link. There is also a link to this page in the Pattern Configuration section of the pattern module page.

Each Pattern Module on the View All page has a brief text description and notes on usage of the configurable items in the Pattern Module. A link to the Pattern Module page is provided to the right of the main heading.

Click the main heading of a Pattern Configuration block to reveal an information table on the configurable items.

To edit a pattern configuration, click *Edit Configuration*.

**Editing a pattern module source**

To edit a pattern module source:

1. Click *Edit* in the Pattern Module Source Window.
   
   The page is refreshed and the source pane becomes an edit pane.

2. Make any required changes to the pattern module, and click *Apply* to apply the changes.

   If the changes are applied successfully, a success message is displayed and the Browse Packages window is displayed.

   The changed pattern module is contained in a package with the suffix _editn applied to the original name. The number n is incremented on further edits. The package and pattern module that you edited is noted in the description column. For example:

   ```
   Replacement for package 'My Patterns_edit4'. Contains the replacement for module 'AppServer.Tomcat'.
   ```
The replacement package is made active if the one you edited was active.

What is Configipedia?
Configipedia is BMC’s community website that facilitates knowledge sharing around TPL patterns, how they function and the real world issues they help address. Configipedia also provides visibility of the Technology Knowledge Update release schedule and contents.

A link to Configipedia is provided for the Pattern Module lists in the Pattern Management section of the Discovery Page. There is also a link to Configipedia provided from the Software Instance nodes and Business Application Instance nodes that are maintained by TPL software patterns. See Managing your IT infrastructure and Managing your business applications for more information.

Manual pattern execution
Patterns are generally triggered on specific events or changes that occur in the course of a discovery run. Sometimes you may want to run a pattern outside a discovery run, for example, you may be developing patterns against already scanned hosts. This can be achieved by running a pattern against the nodes contained in a Group.

When you run a pattern manually, it is not the same as triggering it as a result of scanning. Discovery calls may be made from the pattern, but it does not undertake full discovery. If you have changed your discovery credentials or configuration, you should rescan before running patterns manually.

Selecting hosts or other nodes
You can select hosts or other nodes by adding them to a group.

1. Either:
   - From a view node (including host) page: from the Actions list, select Groups and add the node to a group.
   - From a report or other search result: select the required items, then from the Actions list, select Groups and add the nodes to a group.

Node types against which patterns can be run
You should add nodes to your group of the kind that the pattern triggers on (for example, if the pattern triggers on a DiscoveredProcess, then you should add DiscoveredProcess nodes).

However, the system is able to expand host nodes in an intelligent fashion such that it is possible, for example, to simply add a host even though the pattern requires a DiscoveredProcess.

The following table defines the complete set of traversals used to expand from host nodes to other node kinds. Where more than one traversal is shown, the traversal steps are followed one after the other.

<table>
<thead>
<tr>
<th>Required</th>
<th>Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscoveredProcess</td>
<td></td>
</tr>
</tbody>
</table>
### Required Traversal(s)

<table>
<thead>
<tr>
<th></th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• InferredElement:Inference: Primary:DeviceInfo</td>
</tr>
<tr>
<td></td>
<td>• DiscoveryResult:DiscoveryAccessResult: DiscoveryAccess:</td>
</tr>
<tr>
<td></td>
<td>DiscoveryAccess</td>
</tr>
<tr>
<td></td>
<td>• DiscoveryAccess:DiscoveryAccessResult: DiscoveryResult:</td>
</tr>
<tr>
<td></td>
<td>ProcessList</td>
</tr>
<tr>
<td></td>
<td>• List:List:Member:DiscoveredProcess</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DiscoveredListeningPort</td>
<td>• InferredElement:Inference: Primary:DeviceInfo</td>
</tr>
<tr>
<td></td>
<td>• DiscoveryResult:DiscoveryAccessResult: DiscoveryAccess:</td>
</tr>
<tr>
<td></td>
<td>DiscoveryAccess</td>
</tr>
<tr>
<td></td>
<td>• DiscoveryAccess:DiscoveryAccessResult: DiscoveryResult:</td>
</tr>
<tr>
<td></td>
<td>NetworkConnectionList</td>
</tr>
<tr>
<td></td>
<td>• List:List:Member:DiscoveredListeningPort</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SoftwareInstance</td>
<td>• Host:HostedSoftware: RunningSoftware:SoftwareInstance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BusinessApplicationInstance</th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Host:HostedSoftware: RunningSoftware:BusinessApplicationInstance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DeviceInfo</th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• InferredElement:Inference: Primary:DeviceInfo</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HostInfo</th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• InferredElement:Inference: Primary:HostInfo</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ContainedHost:HostContainment: HostContainer:Cluster</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HostContainer</th>
<th>Required Traversal(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• ContainedHost:HostContainment: HostContainer:HostContainer</td>
</tr>
</tbody>
</table>

### Running patterns

To run a pattern against a group, navigate to the View Pattern page of the pattern you wish to run.

To do this:

1. From the **Discovery** tab, click **Pattern Management**.
2. Click the Package containing the pattern you want to run from the package list.
3. Click the Pattern Modules link.
4. Select the Pattern Module containing the pattern that you want to run.
5. From this page you can edit the pattern source or configuration if necessary. Editing the pattern is described in **Pattern configuration and editing**.
   a. Once the pattern is edited, you are returned to the Pattern Management: Browse Packages page.
   b. Select the Package containing the pattern you want to run from the package list.
   c. Click the Pattern Modules link.
   d. Click the Pattern Package link.
6. Click the Pattern link in the heading table.

7. From the **Actions** list, select **Run Pattern**.

Select the Group that you want to run the pattern against using the Run against Group list. Then choose the settings for the pattern run. Set Expand, Execution Logging, and Additional Discovery. The settings are described in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run against Group</td>
<td>Provides the list to select the group to run the pattern against.</td>
</tr>
<tr>
<td>• Only show Working Set:</td>
<td>If you do not have any Working Sets, this check box is disabled. If you have at least one working set, clearing this check box enables you to choose Groups that are not in your working set.</td>
</tr>
<tr>
<td>• Expand:</td>
<td>Selecting this check box checks the host for additional nodes that match the pattern's trigger. This depends on what nodes are in the group and what node kind the pattern triggers on. The text displayed under the Run against Group menu shows the number of nodes in the group that are the correct node kind to match the pattern’s trigger. If the group contains a host node, select this check box. For example, the ApacheBasedWebserver pattern triggers on DiscoveredProcess nodes. If the group contains one DiscoveredProcess node and one host node (containing 162 DiscoveredProcess nodes) this field shows 1 Discovered Process node if Expand is not checked and 163 Discovered Process nodes (including 162 via 1 Host node) if it is checked. As another example, if you have DiscoveredProcess nodes in your group and you trigger on DiscoveredProcess, then you do not select this check box.</td>
</tr>
<tr>
<td>Execution Logging</td>
<td>Select the logging level for this pattern run. This is one of Debug, Info, Warning, Error, or Critical.</td>
</tr>
<tr>
<td>Additional Discovery</td>
<td>Choose whether discovery commands that perform additional discovery should perform live discovery of the host. For example, the runCommand method performs additional discovery by calling remote commands from patterns. • Do not get extra data: Use any existing data that is available on the appliance. • Get data as needed: Use any existing data that is available on the appliance. If additional data is required, perform discovery on the target to obtain it. Get data as needed will only make a request if that request has not been made before. • Get all new discovery data: Always perform a new discovery. Do not use any previously discovered data.</td>
</tr>
</tbody>
</table>

While the pattern is running, the results page is displayed.

**Template patterns**

BMC Atrium Discovery includes patterns that model commonly deployed software. Through monthly Technology Knowledge Updates (TKUs), the Technology Knowledge Network team updates and creates new patterns to increase coverage of the leading products running in global 2000 data centers. Additionally, many template patterns are supplied with BMC Atrium Discovery. They are available from the Pattern Templates section of the Pattern Management page.

The following patterns are included:

- **template_simple_si**: Maintain a simple Software Instance based on identifying a process.
- **template_si_instances**: Maintain an identifiable Software Instance triggered on a process with its identity in its command line.
- **template_si_version_path**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found in the path.
- **template_si_version_path_table**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found in the path and looked up in a table.
- **template_si_version_command**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found by running a command.
- **template_si_version_registry**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found in the Windows registry.
- **template_si_version_xml_file**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found in an XML file.
- **template_si_version_package**: Maintain a grouped Software Instance triggered on a process, with the Software Instance version found in package information.
- **template_si_collect_children**: Maintain a Software Instance based on identifying a process, which collects the process' children into a single SI.
- **template_bai_search**: Maintain a Business Application Instance based on identifying a Software Instance and searching for some other components.
- **template_bai_add**: Maintain a Business Application Instance based on identifying each of several Software Instances that contribute to it.
- **template_host_location**: Maintain relationships linking Hosts to Locations based on hostname.
- **template_sql_asset_integration**: Use business contextual information stored in a SQL database to annotate Hosts with ownership and location information.
- **template_sql_deep_discovery**: Issue SQL queries to a discovered database to extract further information about it or other software.
- **template_mainframe_mq**: Maintain an identifiable Mainframe MQDetail and relationships to the parent Message Server SoftwareInstance.
- **template_mainframe_storage**: Maintain an identifiable item of Mainframe Storage based on a TapeDrive or DASDDrive and relationships to the containing StorageCollection and MFPParts.
- **template_mainframe_transaction**: Maintain an identifiable Mainframe Transaction and relationships to the parent Transaction Server Software Instance.
- **template_cmdb_cs_augment**: Augment BMC_ComputerSystem CIs synchronized to the CMDB with additional information taken from the BMC Atrium Discovery Host node.
- **template_cmdb_hostname_override**: Override the HostName attribute of BMC_ComputerSystem in the CMDB so it takes only the first component of compound dot-separated hostnames.
- **template_cmdb_location**: Relate BMC_ComputerSystem CIs to BMC_PhysicalLocation CIs in the CMDB.
- **template_cmdb_ss_augment**: Augment BMC_SoftwareServer CIs synchronized to the CMDB with additional attributes taken from the BMC Atrium Discovery SoftwareInstance node.
- **template_cmdb_ss_cti**: Override the default Category, Type, and Item values for BMC_SoftwareServer CIs mapped from particular BMC Atrium Discovery SoftwareInstance nodes.
Technology Knowledge Update (TKU)

Technology Knowledge Update (TKU) is the method used by BMC Atrium Discovery to distribute TPL patterns that you can install. Software identification and versioning is provided by the TKU patterns. Technology Knowledge Update is released on a regular basis and provides the following benefits:

- More recent patterns verified against known customer data.
- Greater number of software products supported by BMC Atrium Discovery.
- Certain existing customer patterns for off-the-shelf software can be removed or created as standard content as part of the update.
- Updates can be applied without requiring a BMC Atrium Discovery upgrade.

Technology Knowledge Update patterns are distributed as a zip file which is uploaded to the appliance. See Uploading and activating a TKU for more information.

Uploading and activating a TKU

You can upload and activate a TKU package in a single operation. Before you can do this, the appliance must be in Maintenance mode, and Discovery stopped. If not, a warning to this effect is displayed when you attempt to display the Knowledge Update page.

⚠️ Changes in the pattern configuration block revision number may reset the pattern configuration changes to the default values

If you install a Technology Knowledge Update (TKU) which contains an update to a pattern configuration block that requires its major revision number to be incremented, any end-user configuration changes to that pattern (made through the pattern configuration block) are lost and the default pattern values are restored.

A TKU release contains the following components. You may download one or both of these depending on your license agreement:

- Technology-Knowledge-Update-YYYY-MM-N-RELEASE.zip
  - Core – Patterns that model various software products.
  - Extended Database discovery – Patterns that extend some of the core database patterns to obtain additional detailed information about certain databases.
  - Middleware discovery – Patterns that obtain detailed information about certain J2EE Application Servers and Web servers
  - Network Device Integration Module with associated Network Device definition files (compatible with BMC Atrium Discovery 8.2.01 and above)* and Printer definition files (compatible with BMC Atrium Discovery 8.3 and above).
• System – Patterns that detect configuration issues and populate Discovery Conditions and patterns used by the CMDB sync system

• Extended-Data-Pack-YYYY-MM-N-RELEASE.zip
• Product Lifecycle – Patterns that populate BMC Atrium Discovery with information about End-of-Life, End-of-Support, and End-of-Extended-Support for versions of certain host Operating Systems as well as versions of certain software products.
• Hardware Reference Data – Patterns and data import CSV file that populate BMC Atrium Discovery with power and heat consumption figures for various hosts.

Where an upgrade makes changes to syncmapping files (see Default CDM Mapping and Syncmapping block), the initial CMDB syncs after upgrade may result in longer reconciliation times. Examples of such changes are key changes or attribute changes on a CMDB CI.

⚠️ Hardware Reference Data

This page uploads hardware reference data using the Create and Update option available when importing using the Import Hardware Reference Data page.

⚠️ Lifecycle reports

The Extended Data Pack provides a means of populating many of the Lifecycle reports that are shown in the OS Product Lifecycle Analysis dashboard.

These supplied zip archives can be uploaded and their content activated without any further processing by following the procedure below.

To upload and activate a TKU package

1. Ensure that the appliance is in Maintenance mode, and Discovery is stopped.
2. From the Model section of the Administration tab, select Knowledge Update.

The result of the last update is displayed on the Knowledge Update page unless it has been cleared, or no updates have taken place since the appliance was started.

This screen illustrates the result of the Knowledge Update.
3. Click **New Update** to display the Knowledge Update dialogs.
4. Enter the filename into the **File To Upload** dialog box, or click **Browse...** to locate a file.
5. To upload and perform the update, click **Apply**.
   - This task may take a long time. You can navigate away from this page while the task is running.
   - When the task is finished, the page is updated with the results which remain until cleared.

### Updating a TKU

When updating a TKU, follow the same procedure for **uploading** a TKU. The patterns in the previous TKU are automatically deactivated. Where the major version of TKU patterns changes, the new patterns do not become the maintainer of the inferred model created by the patterns from the previous TKU. Where this happens the inferred model created by the previous TKU and that by the new TKU may coexist in parallel until the older one is aged out. You can avoid this by deleting the previous TKU, and consequently removing the inferred model created by its patterns.

### Integration points

#### What is an integration point?

An **integration point** is the container for information used to query centralized databases containing information relating to many hosts in the network. For each host, the integration point can query the database and extract useful information to populate attributes on the host node in the BMC Atrium Discovery model. For example, the name and contact details of people responsible for a particular server is valuable data, but is not generally held on that server. BMC Atrium Discovery enables you to extract such data from a central database by means of integration points.

An integration point contains one or more of each of the following components:

- **Connection**: provides the information (for example, database credentials, driver, IP address) to create a connection from BMC Atrium Discovery to the target database.
- **Query**: the SQL query which is passed to the target database to extract the required information. The query is specified in the pattern used to query the target database.

Integration points and queries are created automatically when a pattern that defines them is uploaded. The two are matched up by the integration point name and the name attribute of a Pattern Definitions block. See the Pattern Language Guide for details of Pattern Definitions. Once an integration point is created, you must populate it with at least one connection and one query before it can be used.

#### Viewing integration points

You view integration points from the Discovery page.

1. From the Discovery page, click the **Integration Points** tab
2. Click the name of an integration point to view it.
   The Details tab on the Integration Point window contains the following sections:
   - **Details**: basic description of the integration point
   - **Related Patterns**: lists any patterns on the appliance that use this integration point.
   - **Results**: lists results for each pattern.
   The Connections tab on the Integration Point window shows a list of connections configured for this integration point.
   The Queries tab on the Integration Point window shows a list of queries configured for this integration point.

**Row colors in integration points**

The rows have colored backgrounds according to the status of the integration point. The following scheme is used:

- **green**: all successful outcomes each time the integration point is called from a pattern.
- **amber**: some successful outcomes and some failures when the integration point is called from a pattern.
- **red**: all failures each time the integration point is called from a pattern.
- **blue**: the integration point has not yet been called from a pattern.

This color scheme is used for connections and queries too.

**Viewing a connection**

The Connections tab on the Integration Point window shows a list of connections configured for this integration point.

To view a connection:

1. From the Connections tab on the Integration Point window, click the connection name.

**Viewing a query**

The Queries tab on the Integration Point window shows a list of queries configured for this integration point.

To view a query, click the query name.

The Query window is displayed:

1. From the Query tab on the Integration Point window, click the query name.

**Creating a connection**

An SQL discovery connection provides the information to create a connection from BMC Atrium Discovery to the target database. Once a connection has been made, the database can be queried.

A connection can be represented as a URL which should be immediately familiar to a database administrator. This is shown in the preview section of the window. An example TPL call using the connection is also shown.

To Create a connection in an integration point:
1. Click the **Connections** tab on the Integration Point screen.

2. Click **Create** at the top right hand side of the Integration Point screen.

   Enter details of the connection.

   Which fields are displayed and whether they are required depends on the database driver selected.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the connection. You can only use numbers, letters, or the underscore character (_). This name is used in TPL to call the connection. An example TPL call using the connection name is shown in the Useful Information section.</td>
</tr>
<tr>
<td>Description</td>
<td>A free text description of the connection.</td>
</tr>
<tr>
<td>Username</td>
<td>The database user name which will be used to connect to the database server.</td>
</tr>
<tr>
<td>Password</td>
<td>The password corresponding to the database user name.</td>
</tr>
<tr>
<td>Database Driver</td>
<td>The driver to use to connect to the database server. Select the appropriate driver from the drop down list. BMC Atrium Discovery ships with a limited number of database drivers due to licensing restrictions. See adding new drivers for details of how to add further drivers.</td>
</tr>
<tr>
<td>Database IP Address</td>
<td>The IP address of the database server.</td>
</tr>
<tr>
<td>Port</td>
<td>The port to use to connect to the database server.</td>
</tr>
<tr>
<td>Database</td>
<td>The database to connect to in the database server.</td>
</tr>
</tbody>
</table>
   | Additional Parameters | Any additional parameters that you want to supply to the database driver. These are specified as key=value pairs in a semicolon separated list. For example, you may want to specify that a driver which supports it should connect using SSL and with a non-default timeout:
   ```
   useSSL=true;timeout=60
   ```
   For information about the parameters that can be specified for each driver, you should consult the driver documentation on the internet. Links are provided on the JDBC drivers page. |

3. To save the connection, click **Apply**.

   The Connection window is displayed showing the details of the connection including the example URL and TPL call, and an empty result section. The results section is updated when the connection is used.

   **Testing a connection**

   Once you have created a connection, you should test it. To test a connection:

   1. From the Connection window, click **Test**.
   2. The screen is refreshed to show a Test Results section below the Connection Details section.

   The following screenshot shows a success:

   **This screen illustrates a successful connection.**

   The following screenshot shows a failure:
Testing a query
Once you have created a query, you should test it. To test a query:

1. From the Query window, click **Test**.
2. From the Test Query dialog select a connection from the list to use to test the query.
3. Click **Next**.
4. Enter the parameters to be passed with the query.
   The example above shows a query requiring the hostname parameter.
5. To perform the test, click **Test**.
   The screen is refreshed to show a Test Results section below the Query Details section.

Adding new JDBC drivers
BMC Atrium Discovery ships with the JTDS driver which can connect to MS SQL Server and Sybase. To connect to other databases you must download and install JDBC drivers for the databases that you want to use.

If you wish to connect to a database from the list below, then all you need to do is download the driver from the appropriate web site (the URL is available from Uploading new JDBC drivers) and upload it using the Uploading new JDBC drivers page. However, before you can use a new driver that is not in the list below, you must provide a properties file for it. The properties file determines how the JDBC URL is constructed. The following properties files are shipped with BMC Atrium Discovery and are located in the `$TIDEWAY/data/installed.jdbcdrivers` directory:

- Informix
- Ingres
- Microsoft SQL Server
- MySQL
- Oracle
- PostgreSQL
- Sybase
- JTDS

⚠️ **Additional driver support**

While it is possible to add new JDBC drivers not specified on the preceding list, these will not have been tested by BMC, and as such no guarantees can be made that they will work with BMC Atrium Discovery as expected. For further information, please contact BMC Support.
The $TIDEWAY/data/custom/jdbcdrivers and $TIDEWAY/data/installed/jdbcdrivers directories are both checked for properties files.

When you save a driver to the $TIDEWAY/data/custom/jdbcdrivers directory, you can create a new properties file in the same directory, or you can edit one of the supplied properties files in the $TIDEWAY/data/installed/jdbcdrivers directory.

Writing a properties file

1. Create a text file called name.properties where name **must** be the same as the name of the driver that the properties file relates to. For example, mysql-connector-java-5.0.7.properties is the properties file for mysql-connector-java-5.0.7.jar.
2. The following table describes the entries that you must put in the properties file and also the additional optional entries:

<table>
<thead>
<tr>
<th>Mandatory Entries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entry Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>driver.name</td>
<td>The name of the driver. This is the field that is displayed throughout the BMC Atrium Discovery UI to identify this driver.</td>
</tr>
<tr>
<td>driver.class</td>
<td>The main class that will be loaded from the relevant jar file in custom/jdbcdrivers. The user will need to get this from the documentation provided by the database/JDBC vendor. For example, driver.class=com.mysql.jdbc.Driver</td>
</tr>
<tr>
<td>driver.url</td>
<td>The format of the connection URL that this driver uses. There is no standard URL for the JDBC URL so every driver has its own format. BMC Atrium Discovery passes the assembled URL to each registered driver and the driver responds whether it recognises the URL or not. The URL is made up of several parts that are dealt with in the next section.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional Entries</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entry Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>driver.default=true</td>
<td>Specifies that this driver is the default driver and will be displayed first in lists when creating objects that use JDBC drivers, for example, SQLIntegrationConnections. If no default is specified across all the drivers then the order in which they are displayed is random. If more than one driver is specified as the default then the last driver to be loaded will be marked as the default.</td>
</tr>
<tr>
<td>driver.exceptionProcessor</td>
<td>Specifies a Java class that can format SQL exceptions (java.sql.SQLException) that bubble up from the JDBC driver. This class must implement the ExceptionProcessorIF interface. When an SQL exception occurs, the specified class will be called and then the result of that call will be published to the relevant source, which may be a log file or to the UI. For example, driver.exceptionProcessor=com.tideway.integrations.service.servants.MySqlExceptionProcessor</td>
</tr>
<tr>
<td>translation.variablename</td>
<td>Translates a variable that is specified in the JDBC URL to a user visible label. See the table below for a list of variable names. (e.g. translation.extra_parameters=Additional Parameters)</td>
</tr>
<tr>
<td>validationregex.variablename</td>
<td></td>
</tr>
</tbody>
</table>


**Mandatory Entries**

*Used only with Integration Points and Software Credential Groups.* Validates a given variable specified in the JDBC URL. When the user tries to save a connection, each of the properties is checked to see if it has an associated validation regex. If so, and if the *Match on this* checkbox is *NOT* selected, or the connection is static, then the value entered by the user is matched against the value specified here. If they do not match, the user is prompted to re-enter the value. Endpoint is always validated, for static credentials, to ensure that it is a valid IPv4 address.

The following table shows the parameters used by each driver:

<table>
<thead>
<tr>
<th>Field</th>
<th>Informix</th>
<th>MySQL</th>
<th>Postgres</th>
<th>Oracle (service)</th>
<th>Oracle (SID)</th>
<th>Ingres</th>
<th>Sybase</th>
<th>MS SQL Server</th>
<th>JTDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>serverType</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>endpoint</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
<td>Req</td>
</tr>
<tr>
<td>database</td>
<td>Req</td>
<td>Opt</td>
<td>Req</td>
<td></td>
<td>Req</td>
<td>Opt</td>
<td></td>
<td></td>
<td>Opt</td>
</tr>
<tr>
<td>INFORMIXSERVER</td>
<td>Req</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>instance_name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Opt</td>
</tr>
<tr>
<td>service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Req</td>
</tr>
<tr>
<td>sid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Req</td>
</tr>
</tbody>
</table>

When you have added a new driver and written a properties file for it, you must restart the Tideway services. To do this, enter the following command:

```
$ sudo /sbin/service tideway restart
```

**Multiple drivers using the same JAR (Oracle)**

There are two methods of connecting to Oracle, OracleService and OracleSID. These methods use the same driver JAR file, but need two properties files to build the different connection URLs used. Rather than copying and renaming the JAR file, a better method is to use symbolic links.

The driver file is called `ojdbc14.jar` for Oracle to 10g. For Oracle 11g the driver file is called `ojdbc15.jar` which requires JRE 1.5 or later.

```
cd ~/data/installed/jdbcdrivers
ln -s ojdbc14.jar oracleService.jar
ln -s ojdbc14.jar oracleSID.jar
```
This creates a symbolic link called `oracleService.jar` for the `oracleService.properties` properties file and one called `oracleSID.jar` for the `oracleSID.properties` properties file.

### Uploading new JDBC drivers

A JDBC driver is shipped in the form of a single file with an extension of `.jar` (Java ARchive). The JAR file contains a compiled java implementation of the client code to remotely talk to the database. Database vendors usually make their JDBC drivers available for free download from their websites.

Due to licensing issues we cannot ship the drivers for all of the databases that we support. They are available from the vendors' websites for download. We supply the URLs to access these jar files on the JDBC Drivers page. To access this, in the Administration page, Appliance section, click **JDBC Drivers**.

After you have downloaded the JDBC driver for the database you wish to communicate with, upload it to the appliance using the correct upload link in the table. The file will be uploaded and verified. If the required Java class is not found in the jar, or if the jar is corrupt (or not a jar at all) then an appropriate message will be displayed in the Status column. Simply re-upload the correct driver to correct the issue should one arise.

The available statuses for the drivers are:

- No JAR Uploaded
- Jar Uploaded (Deactivated)
- Activated and in use. This means the driver is being used by an SQL credential.
- Activated but not in use
- Error.

BMC Atrium Discovery is shipped with a default set of properties files which define the databases that you can connect to. If you want to connect to a different database, you must write a properties file and download an appropriate driver. This is described in **Adding new JDBC drivers**.

### JDBC drivers

The following table provides an example JDBC URL for database targets. It also provides documentation and download URLs where available. When selecting the appropriate driver, note that BMC Atrium Discovery uses JDK 1.6. Consult the database vendor's documentation for further information.

<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC URL</th>
<th>Internet site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informix</td>
<td><code>jdbc:informix-sqli://host[:port]/database;INFORMIXSERVER=servername</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>[;property=value]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Database JDBC URL

The following example URL connects to an Informix server running on a host on IP address 192.168.0.100, port 1533, database name ADDM_IMPORT, INFORMIXSERVER ADDMserver, user fred, and password password.

```java
jdbc:informix-sqli://192.168.0.100:1533/ADDM_IMPORT:INFOMIXSERVER=ADDMserver; user=fred;password=password
```

**Download and documentation** [See the IBM website.](http://www.ibm.com)

### MySQL

```java
jdbc:mysql://host,[failoverhost...][:port]/[database]
[property=value][;property=value]
```

The following example URL connects to a MySQL server running on a host on IP address 192.168.0.100, port 3306, database name ADDM_IMPORT, user fred, and password password.

```java
jdbc:mysql://192.168.0.100:3306/ADDM_IMPORT?user=fred&password=password
```

**Download:** [http://www.mysql.com/products/connector/](http://www.mysql.com/products/connector/)


### Postgres

```java
jdbc:postgresql://host:[port]/database
[property1=value1][&property2=value2]
```

The following example URL connects to a Postgres server running on a host on IP address 192.168.0.100, port 5432, and database name ADDMdatabase.

```java
jdbc:postgresql://192.168.0.100:5432/ADDMdatabase
```

**Download:** [http://jdbc.postgresql.org/download.html](http://jdbc.postgresql.org/download.html)

**Documentation:** [http://jdbc.postgresql.org/documentation/83/connect.html](http://jdbc.postgresql.org/documentation/83/connect.html)

### Oracle

For Oracle there are two possible connection styles:

**Connection using service**

```java
jdbc:oracle:<driver type>:[username/password]://host:[port]/service
```

The following example URL connects, using a thin driver, to an Oracle server running on a host on IP address 192.168.0.100, port 1521, and service ADDM_DB.

```java
jdbc:oracle:thin:@/192.168.0.100:1521/ADDM_DB
```

**Connection using SID**

```java
jdbc:oracle:<driver type>:@host:[port]:SID
```

The following example URL connects, using a thin driver, to an Oracle server running on a host on IP address 192.168.0.100, port 1521, and SID ADDM100.

```java
jdbc:oracle:thin:[username/password]@192.168.0.100:1521:ADDM100
```
<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ingres</strong></td>
<td><code>jdbc:ingres://host:[port]/database</code></td>
</tr>
<tr>
<td></td>
<td><code>[;property=value][;property=value]</code></td>
</tr>
<tr>
<td><strong>Sybase</strong></td>
<td><code>jdbc:sybase:Tds:host:[port]/databasename</code></td>
</tr>
<tr>
<td><strong>MS SQL</strong></td>
<td><code>jdbc:sqlserver://servername[\instanceName][:portNumber]</code></td>
</tr>
<tr>
<td></td>
<td><code>[;property=value][;property=value]</code></td>
</tr>
<tr>
<td><strong>JTDS</strong></td>
<td><code>jdbc:jtds:server\d:\port&quot;[\database]</code></td>
</tr>
<tr>
<td></td>
<td><code>[;property=value][;property=value]</code></td>
</tr>
</tbody>
</table>

**Download:** http://www.oracle.com/technetwork/database/features/jdbc/index-091264.html


See [here](http://community.ingres.com/wiki/JDBC_Driver) for more information on setting up both styles in BMC Atrium Discovery.

The following example URL connects to an Ingres server running on a host on IP address 192.168.0.100, port mnemonic II7, database name ADDMdatabase, user fred, and password password.

```
jdbc:ingres://192.168.0.100:II7/ADDMdatabase;user=fred;password=password
```

**Download:** http://community.ingres.com/wiki/JDBC_Driver

**Documentation:** [Ingres_JDBC_URL_Connection_Information](http://community.ingres.com/wiki/Open_Office_How_To#)

The following example URL connects to a Sybase server running on a host on IP address 192.168.0.100, port 6689, and database name ADDM_DB.

```
jdbc:sybase:Tds:192.168.0.100:6689/ADDM_DB
```

**Download:** [http://www.sybase.com/detail?id=1009876#sec2q2](http://www.sybase.com/detail?id=1009876#sec2q2)

The following example URL connects to an instance of MS SQL server called TDA running on a host on IP address 192.168.0.100, port 1433, user fred, and password password. The username and password correspond to a user configured on the database rather than a Windows AD user. See this [Microsoft article](http://msdn.microsoft.com/en-us/library/ms378428.aspx) for more information.

```
jdbc:sqlserver://192.168.0.100\TDA:1433;User=fred;Password=password
```


The downloaded file (a gzipped tar archive, current version `sqljdbc_3.0.1301.101_enu.tar.gz`) contains two JAR files. Use the `sqljdbc4.jar` the other does not work.

The following example URL connects using JTDS to an MS SQL server server running on a host on IP address 192.168.0.100, port 1433, database name ADDM_IMPORT, instance TDA, user fred, and password password.

```
jdbc:jtds:sqlserver://192.168.0.100:1433/ADDM_IMPORT;instance=TDA;user=fred;password=password
```
<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet site</td>
<td>When using a domain credential (Windows Authentication) of the form <code>DOMAINNAME\username</code> enter the username in the URL described, and the domain information in the Additional JDBC parameters dialog box in the following form: <code>domain=&quot;DOMAINNAME&quot;</code>. Also, if the domain controller requires NTLM v2 add the parameter: <code>useNtlMv2=true</code></td>
</tr>
</tbody>
</table>

The following example URL connects using JTDS to an MS SQL server server running on a host on IP address 192.168.0.100, port 1433, database name `ADDM_IMPORT`, instance `TDA`, Windows user `fred` in the domain `DOM1`, and password `password`.

```
instance=TDA;domain=DOM1;useNtlMv2=true;user=fred;password=password
```

Importing data

This section describes how to import data into BMC Atrium Discovery.

- Importing network device data
- Importing Hardware Reference Data
- Importing CSV data

Importing network device data

The CiscoWorks import tool creates network device entries in the datastore. The import tool creates and updates the following node types:

- NetworkDevice
- PortInterface

Entries in the datastore for a network device and its ports are overwritten if a network device in the input data has the same name.

A limitation of the importer is that a network device already in the datastore for which a matching name cannot be found in the input data will not be removed. Therefore if a network device has been renamed since a previous import, it will appear in the datastore as a second network device.

Use of imported data and direct discovery is not supported

If you use the CiscoWorks import tool to import network devices, and also scan the same network devices, this will potentially generate duplicate network devices. BMC recommends that you use either direct discovery or import, not both.

Importing data from CiscoWorks

The CiscoWorks importer loads the data file exported from CiscoWorks LMS using the Campus Manager User Tracking tool, and loads any existing network device data from the BMC Atrium Discovery datastore. It then compares the sets of data. The supported versions are Campus Manager 3.x and 4.x (UT CLI 1.0, 1.1, and 1.1.1).

The network device name is used as the index. Therefore, if two network devices have the same name, they are treated as the same network device.

- If a new network device is found in the exported file, it is added to the BMC Atrium Discovery datastore. The name of the network device is used as its primary key. See the note below regarding deletion of network devices.
The ports on each network device are updated. These are indexed by IP address (the primary key). Port attributes that are updated include speed, duplex, and IP address. New ports (identified by IP address) are added, and any ports removed from the CiscoWorks data are removed from the datastore.

Importing a CiscoWorks data file

To import a CiscoWorks Data File:

1. From the Discovery section of the **Administration** tab, select **CiscoWorks Import**.

   The options on this page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>File To Upload</td>
<td>The file to upload. Click <strong>Browse...</strong> to display a file browser window. Select the file to import and click <strong>Open</strong>.</td>
</tr>
<tr>
<td>File Type</td>
<td>Choose the type of file to import. Choose either XML or delimited from the File Type list. If you select XML, the lists for <strong>File Delimiter</strong> and <strong>File Has Header Line</strong> are dimmed.</td>
</tr>
<tr>
<td>File Delimiter</td>
<td>For a delimited file only, select the delimiter type from the File Delimiter list. This may be one of Comma, Tab, or Space.</td>
</tr>
<tr>
<td>File Has Header Line</td>
<td>Choose Yes or No from the File Has Header Line list depending on whether the delimited file has a heading line.</td>
</tr>
<tr>
<td>Remove existing NetworkDevices</td>
<td>Do you want to remove existing network devices from the BMC Atrium Discovery datastore that are not present in the file you are importing? Choose Yes or No from the Remove existing NetworkDevices list.</td>
</tr>
<tr>
<td>Logging Level</td>
<td>Choose the logging level from the Logging Level list. This may be Debug, Info, Warning, Error, or Critical.</td>
</tr>
</tbody>
</table>

2. To import the CiscoWorks data file, click **Apply**.

There is also a command line utility available for importing CiscoWorks data. It is described in `tw_imp_ciscoworks`.

Generating CiscoWorks data

To export data from CiscoWorks in a layout which the importer can use, you must create a custom layout. To do this:

1. From the CiscoWorks LMS Portal, select **Reports**.
2. Select **Custom Layouts**.
3. Click **Create**.
4. In the Add Layout dialog box, select **End Host**.
5. Select the columns that you want displayed in the report from the Available Sources list and click **Add** to add them to the Selected Sources list.
6. Arrange these into the required order using the up and down arrows.

   The import file must be in the following order otherwise data will be imported into the wrong attribute, and the import will fail. More or fewer columns will also cause the import to fail:
6. a. Specify the name of the layout as StandardTideway and enter a description.
   b. To create the StandardTideway layout, click Add.

As of 7.2, you can populate an optional field of Port Negotitation (with values of "AUTO" or "FORCED")

⚠️ The full instructions are available on the Cisco Systems website.

The following methods of generating the CiscoWorks data are supported.

**Generating CSV files**

Generating CSV files on the CiscoWorks server:

```
C:\Program Files\CSCOpx\campus\bin\ut -cli -query all
   -layout StandardTideway -export c:\data.csv
   -u user -p password
```

This command produces a Java stack trace. This is a known issue and can be ignored.

The file that is produced can be imported by running the following command on the BMC Atrium Discovery appliance:
$TIDEWAY/bin/tw_imp_ciscoworks --delimiter=',’ --username name --password password --file ~/tmp/data.csv

Generating XML import files
Generating XML files on the CiscoWorks server:

C:\Program Files\CSCOpx\campus\bin\cmexport ut -u userid -p password -host -layout StandardTideway

The file is written into the following directory:
C:\PROGRAM FILES\CSCOpx\files\cmexport\ut

The file that is produced can be imported with the following command on the BMC Atrium Discovery appliance:

$TIDEWAY/bin/tw_imp_ciscoworks --xml --username name --password password --file ~/tmp/2006516154526ut.xml

The following attributes are imported into the data store, where they exist in the input file:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Example</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacAddress</td>
<td>MAC address of port on connected device</td>
<td>01-23-45-67-89-ab</td>
<td>Must be a valid MAC address</td>
</tr>
<tr>
<td>IPAddress</td>
<td>IP address of port on connected device</td>
<td>192.168.0.1</td>
<td>Must be a valid IP address</td>
</tr>
<tr>
<td>DeviceName</td>
<td>Name of network device</td>
<td>switchl.tideway.com</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port name</td>
<td>3/19</td>
<td></td>
</tr>
<tr>
<td>PortDuplex</td>
<td>Duplex setting of port</td>
<td>full-duplex</td>
<td></td>
</tr>
<tr>
<td>PortSpeed</td>
<td>Speed setting of port</td>
<td>100M</td>
<td>Must be a power of ten with K/M/G suffix</td>
</tr>
<tr>
<td>VTPDomain</td>
<td>VLAN Trunking Protocol (VTP) domain name.</td>
<td>Somedomain</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>The name of the VLAN.</td>
<td>Somelan</td>
<td></td>
</tr>
<tr>
<td>VLANId</td>
<td>The VLAN identifier.</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td>VLANType</td>
<td>The type of VLAN.</td>
<td>Ethernet</td>
<td></td>
</tr>
<tr>
<td>PortNegotiation</td>
<td>Negotiation setting of the Port.</td>
<td>AUTO</td>
<td>Must be AUTO or FORCED</td>
</tr>
</tbody>
</table>
Importing Hardware Reference Data

Hardware Reference Data (HRD) provides the following vendor specification data:

- Rack Unit size
- Power W
- Power VA
- Heat Output BTU

Import of HRD into BMC Atrium Discovery will enable customers to associate discovered systems with physical assets and report on both directly from BMC Atrium Discovery.

Importing a Hardware Reference Data file

To import a HRD file:

1. From the Model section of the Administration tab, click HRD Import.
   The options on the Import Hardware Reference Data page are described in the following table.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>File To Upload</td>
<td>The file to upload. Click Browse... to display a file browser window. Select the file to import and click Open. See File Format for details on the format of HRD files.</td>
</tr>
<tr>
<td>Action</td>
<td>Do you want update, create or delete existing HRD?</td>
</tr>
<tr>
<td></td>
<td>Create and Update will perform both actions as described below.</td>
</tr>
<tr>
<td></td>
<td>Create will import records that do not already exist, but will not change any records already imported.</td>
</tr>
<tr>
<td></td>
<td>Update is used ONLY when non-key fields in an existing record need to be updated. Key fields are vendor, model, and config_num_processors. Update will find all imported records that match existing data and update with the imported values. New records in the imported data will NOT be created. If you need to change a key field, you must first delete the existing records and then create the new records.</td>
</tr>
<tr>
<td></td>
<td>Delete is used to delete records selectively. All records imported that match an existing record will cause that existing record to be removed. Existing records that do not appear in the import set will not be deleted.</td>
</tr>
<tr>
<td></td>
<td>The HRD patterns automatically recreate the HRD nodes; you do not have to rescan the hosts.</td>
</tr>
<tr>
<td>Logging Level</td>
<td>Choose Create And Update, Create, Update or Delete from the list.</td>
</tr>
<tr>
<td></td>
<td>Logging Level</td>
</tr>
<tr>
<td></td>
<td>Choose the logging level from the list. This may be Debug, Info, Warning, Error, or Critical.</td>
</tr>
</tbody>
</table>

2. Click Apply.

File format

You can import csv files which must have a heading row specifying the HRD node attributes. For example:

```
vendor,model,known_model_names,config_num_processors,processor_type,max_ram,u_size,power_v
Sun Microsystems,Sun Fire V440,'[Sun Fire V440','SUNW,Sun Fire V440']',4,UltraSPARC-IIIi,4,32768,4,908,636,2172,227,159,543
Sun Microsystems,Sun Fire 280R,'[Sun Fire 280R]',2,UltraSPARC-III+,4096,4,454,318,1086,114
```
Importing CSV data

It is often very easy to extract information from applications and devices and store it as CSV data. Data can be exported from BMC Atrium Discovery in this format. For more information, see CSV API. You can also import CSV data into BMC Atrium Discovery (for example, you might have information on a number of hosts that you want to import).

You can import a CSV file using the Import CSV Data page described in the following section. You can choose delimiters other than commas when importing data using the Import CSV Data page. Alternatively, if you have command line access, you can use the `tw_imp_csv` utility.

**Incorrect usage may result in data loss**

Before using the Import CSV Data page you should fully understand the system taxonomy and the changes that you are going to make to your data. Using Import CSV Data incorrectly can cause irreparable damage to your data. The data you submit using this tool is applied directly to the production data without any validation.

*Always* back up your datastore before using this tool.

**Do not import the following node kinds**

- You *must not* import DDD nodes.
- You should avoid importing Host nodes and other system maintained nodes. If in doubt, contact Customer Support.

Importing a CSV file

To import a CSV data file:

1. From the Model section of the Administration tab, click **CSV Import**.

   The following screen illustrates the Import CSV Data page with the Host Container node kind selected.
This screen illustrates the Import CSV Data page with the Host Container node kind selected.

The options on this page are described below:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>File To Upload</td>
<td>The file to upload. Click <strong>Browse...</strong> to display a file browser window. Select the file to import and click <strong>Open</strong>.</td>
</tr>
<tr>
<td>Update Mode</td>
<td>Select the mode to use for updates. Choose one of the following from the list:</td>
</tr>
<tr>
<td></td>
<td>• Create And Update: nodes are created and updated as required.</td>
</tr>
<tr>
<td></td>
<td>• Create Only: new nodes are created, existing nodes are not updated.</td>
</tr>
<tr>
<td></td>
<td>• Update Only: new nodes are NOT created, existing nodes are updated.</td>
</tr>
<tr>
<td></td>
<td>• Delete Only: nodes with match are deleted. No other nodes will be created or updated.</td>
</tr>
<tr>
<td>Node Kind</td>
<td>Choose the type of node to import from the list. This may be one of any node kind defined in the taxonomy. Changing the node kind updates the Keys field dynamically.</td>
</tr>
<tr>
<td>Keys</td>
<td>Choose the key or keys for each entry. You must select at least one key. The taxonomy defined keys are marked with a red asterisk * . Use the checkboxes if you want to use other keys. The following quick selection links are provided at the top of the keys field:</td>
</tr>
<tr>
<td></td>
<td>• Key Attributes: selects just the taxonomy defined keys.</td>
</tr>
<tr>
<td></td>
<td>• None: clears any selection.</td>
</tr>
</tbody>
</table>

**Note**

The behavior differs from the **tw_imp_csv** utility, which uses the first column of the input file as the key unless others are specified. When controlling an import using the UI Import page, only the keys that are selected are used.

<table>
<thead>
<tr>
<th>Delimiter</th>
<th>Choose the required delimiter from the list. This may be Comma, Semicolon, or Tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Level</td>
<td>Choose the logging level from the list. This may be Debug, Info, Warning, Error, or Critical.</td>
</tr>
</tbody>
</table>

2. To import the CSV file, click **Apply**.

See [CSV import examples](#) for example of using the CSV importer.
Notes on the CSV importer

File format

The CSV file represents a two dimensional table with rows separated by newlines, and columns separated by commas. Commas may be included in that data but must be enclosed between double quote characters.

Column names that do not begin with a hash character (#) are treated as names of attributes on the node.

Column names that begin with a hash character are treated as key expressions. Key expressions are used to create or update a relationship to another node. See Relationships for more information.

Keys

The CSV importer searches the datastore for nodes of a specified kind which have a key or keys matching rows in the supplied CSV data. Where the keys match, the node is updated, or deleted and recreated depending on the options selected. The first attribute column is used as a key by default. This can be overridden with the Keys option described in the table above.

Relationships

Relationship columns describe a relationship between the node being modified and one or more other nodes. Relationships are defined using a full key expression. The first example shows a link to a single node:

```
#role:relationship:role:kind.attribute
```

This example shows a link to multiple target nodes. Notice that you will need to surround the relationship definition and data in double quotes so that the subsequent attributes do not get treated as local nodes:

```
"#role:relationship:role:kind.attribute,attribute,attribute"
```

The first role part is the kind of the role that the node being created or updated plays in the relationship. The relationship part is the kind of the relationship being created. The second role part is the kind of role that the other node plays in the relationship. The kind part is the node kind of the other node. Finally, the attribute or attribute list is the name of the attribute used to find the other node. See the Node Lifecycle Document for information on relationships.

Only a single traversal is supported.
**Type conversion**

By default, the CSV importer attempts to convert attribute values to the type defined in the taxonomy. If an attribute is not defined, it is left as a string. If a conversion fails, it is also left as a string.

**Note:**

For list types, the value in the CSV file must be in Python list syntax.

When the `tw_imp_csv` utility is used with the `--force` option, all attributes are left as strings.

**CSV import examples**

**Example 1**

To free up rack space for other applications, some hosts have been moved from the *Campus* data centre to the newly acquired *Firehouse* data centre. Discovery and Reasoning have handled the IP address and subnet changes but the Host nodes are still linked to the wrong location. Here is the CSV file to process, called *firehouse_move.csv*:

```plaintext
name, #ElementInLocation:Location:Location:Location.name
egan, Firehouse
ray, Firehouse
peter, Firehouse
```

We process the CSV file with the following command line:

```
$ tw_imp_csv --username=system --password=system --kind=Host firehouse_move.csv
```

The script reads the file called `firehouse_move.csv` line by line. It uses the first line to name the columns. The first column is called `name`, which does not begin with a `#` character so it is treated as an attribute name. The second column does begin with a `#` character so it is treated as a specification for some relationships.

No explicit key has been specified so the first (and in this case, only) attribute name is taken to be the key.

Now the script reads the second line. The first field, `egan`, is in the `name` column which was selected as the key earlier. So the script uses the search service to find a node of kind *Host* (from the `--kind` command line option) that has a `name` attribute equal to `egan`. It finds exactly one
node matching that search. If it had not found that node, it would have been created. If it had found multiple nodes, an error would have been reported and processing would continue with the next line, NO nodes would have been updated.

Having found the node, it updates it using the other fields on the row. Were there any other attribute columns in the file, the script would have used these to update the node before looking at the relationships.

The file has only one relationship column. The name is #ElementInLocation:Location:Location:Location.name. The script searches for a Location node with a name attribute equal to Firehouse, this row's value for the column. Having found the Location node, the script creates a HostLocation relationship to it with the Host node playing the HostInLocation role and the Location playing the LocationOfHost role.

The script then processes the second and third data rows, updating the ray and peter nodes with the new location.

**Example 2**

A new host has been installed in the Firehouse data centre. Due to pressure from the organisation's E-services Protection Adviser, there is now a firewall preventing discovery of hosts on that site. Until a remote Windows proxy can be installed, the Firehouse sysadmins have been sending us spreadsheets with the changes.

Here is a CSV file, called new_host.csv:

<table>
<thead>
<tr>
<th>name, fqdn, #ElementInLocation:Location:Location:Location.name, #OwnedItem:Ownership:ITOwner:Person.name, ip_addrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>winston, winston.example.com, Firehouse, &quot;Melnitz, J&quot;, &quot;[10.3.4.1', '192.168.101.45']&quot;</td>
</tr>
</tbody>
</table>

We process the CSV file with the following command line:

```
$ tw_imp_csv --username=system --password=system --kind=Host --create new_host.csv
```

The command line is nearly the same as in Example 1. The differences are that the filename has changed because we are processing a different file and we are using Create Only mode.

As in Example 1, the script searches for Host nodes with a name attribute equal to winston. This time, because it is in create mode, the script checks that there are no matching nodes. If there were, the script would report an error and skip the row.

Now the script creates a new node. It populates the attributes of the node from the non-relationship fields in the data. The ip_addrs field is a list and the value starts with a '[' character so it is converted into a list. The new node has attributes:
- name = 'winston'
- fqdn = 'winston.example.com'
- ip_addrs = ['10.3.4.1', '192.168.101.45']

Then the script adds the relationships. The location relationship column is processed in the same way as in Example 1. The column called #OwnedItem:Ownership:ITOwner:Person.name creates an OwnedItem:Ownership:ITOwner relationship to a Person node with a name equal to Melnitz,J. The quotes around that field are needed because the field contains a comma.
Context-sensitive reporting and linking

This section explains how to create context-sensitive reports and links with BMC Atrium Discovery.

- Configuring additional links
- Custom reporting

Configuring additional links

The external links feature provides links from objects modelled in BMC Atrium Discovery, to other web-based systems where additional information is stored. It is also used to create links to reports or charts specified for individual nodes or sets of nodes (result sets).

For example, if you are viewing a host in the BMC Atrium Discovery UI, you may see a link to that host in a change management application such as Remedy. See Dynamic Toolbox. Search queries are used to construct the links. See Search and Reporting Service for more information.

The following link types are provided:

- Links to external systems
- Report for individual nodes
- Chart for individual nodes
- Report for result sets
- Chart for result sets

Configuration files

Additional link configuration has changed in version 7.3 to become a form of Custom reporting. The xml configuration files are held in the following directories:

1. /usr/tideway/data/installed/reports/
2. /usr/tideway/data/custom/reports/

The directories are parsed in the order given (installed before custom), and the files contained in these directories are parsed in alphabetical order, with numbers before letters. This order is important as later definitions for a named link override those loaded earlier. The standard additional links are contained in /usr/tideway/data/installed/reports/00additional_links.xml.

Upgrades from previous versions remove /usr/tideway/data/default/additional_links.xml and add the following new file:
/usr/tideway/data/installed/reports/00additional_links.xml
If you are upgrading, you must copy /usr/tideway/data/customer/additional_links.xml to /usr/tideway/data/custom/reports/00additional_links.xml and manually convert the file to the new format which is described on this page.

Links configured in the installed subdirectory are displayed beneath the default links, those from the custom subdirectory follow them. However, if a custom link overrides an installed link it will appear in place of the installed link.

Notes:

1. The link must be specified in valid XML. The XML equivalents of certain characters must be used (for example, &amp; instead of &, &gt; instead of >, and &lt; instead of <).
2. The XML files are read when the Application server starts. Usually you would restart the whole tideway service.
3. Parse errors in the XML do not prevent the Application server starting but may cause one or all external link definitions to be ignored.
4. Failure to return a value for a requested attribute will be caught, resulting in the link being discarded for this particular node, on this request. For future requests an attempt to build the link will be made again.
5. You can substitute any attribute in a tag. Use %(attribute_name)s to do this. If the attribute contains a list value there will also be a string representation containing a comma separated list of values in %(comma_separated_attribute_name)s.
6. The following keys are provided:
   - id: the node ID as set in the URL, for example nodeID=%(id)s
   - kind: the node kind.
   - uiModule: the UI module that normally handles display of the node kind.
   - urlPrefix: the URL prefix of the appserver. This is usually ui.
7. In addition <link> with <attribute> entries contain:
   - translated: the locale translated attribute name.
   - otherNodeID: if the attribute represents a link then the node ID of the related node.

Link tags

The link tag specifies the type of link that is being created. These may be one of the following:

- **Normal Link**: specified with a <link> tag.
  
  A report that is run against a single node and the link should be visible when viewing a node of the correct node kind.
- **Chart Link**: specified with a <node-chart> tag.
  
  A chart that is run against a single node. The link should be visible when viewing a node of the correct node kind.
- **Set Report Link**: specified with a `<refine-report>` tag.
  A report that is run against a nodeset and the link should be visible when viewing a set of nodes of the correct node kind.

- **Set Chart Link**: specified with a `<refine-chart>` tag.
  A chart that is run against a nodeset and the link should be visible when viewing a set of nodes of the correct node kind.

Each tag must specify a name using the `name` attribute. Note that each link tag is in a distinct namespace.

**Tags available**

The following XML tags are available in all form of links:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Provides the main page title for the link. This tag is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Populates the title attribute of the HTML link. Presented as a tool tip. Also shown as a subtitle below the main page title. This tag is mandatory.</td>
</tr>
<tr>
<td>Kind</td>
<td>Link will be shown against this node kind. This tag is mandatory.</td>
</tr>
<tr>
<td>Image</td>
<td>Specifies an image to display. The image should already exist on the appliance as the specification is from the appliance image root <code>{{http://appliance/styles/default/images/image_name}}</code>). This tag is mandatory.</td>
</tr>
<tr>
<td>Permissions</td>
<td>Specifies a list of permissions that the user must possess in order to display the link. <code>&lt;permissions&gt;</code> contains a list of <code>&lt;permission&gt;</code> entries, one per required permission.</td>
</tr>
</tbody>
</table>

The following XML tags are available in `<link>`:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The URL that the link points to. This tag is mandatory.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Displays a link in the UI next to the attribute if the attribute is not displayed, or not present on the node, then the link is not displayed.</td>
</tr>
<tr>
<td>Target</td>
<td>Populates the HTML anchor for the link. Points to the named window or frame that the results of this query will be displayed in. Frequently this will be <code>_new</code> so that the link will open in a new window.</td>
</tr>
</tbody>
</table>
The following XML tags are available in the remaining link types:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lookup</td>
<td>Supported in <code>&lt;node-chart&gt;</code> and <code>&lt;node-report&gt;</code>, Indicates if the query is relative to the node. Defaults to true which will generate a search of the form <code>LOOKUP 'id' = %id%</code>. If you need a general search then use this tag to override the behaviour. <code>&lt;lookup&gt;False&lt;/lookup&gt;</code></td>
</tr>
<tr>
<td>Flags</td>
<td>Any flags to include in the search query. <code>&lt;flags&gt;include_destroyed&lt;/flags&gt;</code></td>
</tr>
<tr>
<td>With</td>
<td>Any with functions to evaluate in the search query. <code>&lt;with&gt;value(NODECOUNT(TRAVERSE Host:HostedSoftware:RunningSoftware:SoftwareInstance)) AS si_count&lt;/with&gt;</code></td>
</tr>
<tr>
<td>Where</td>
<td>Any conditions in the search query. This tag takes an optional keyword attribute which, when given value <code>False</code>, prevents the addition of the WHERE keyword when constructing the query. For example, <code>TRAVERSE ::::Host must not be prefixed by WHERE.</code> <code>&lt;where&gt;version = ''&lt;/where&gt;</code></td>
</tr>
<tr>
<td>Order-by</td>
<td>Sort results of query by specified order. <code>&lt;order-by&gt;name&lt;/order-by&gt;</code></td>
</tr>
<tr>
<td>Show</td>
<td>List of attributes to display. For <code>&lt;node-chart&gt;</code> and <code>&lt;refine-chart&gt;</code> this represents the list of attributes shown when clicking through the chart. <code>&lt;show&gt;SUMMARY&lt;/show&gt;</code></td>
</tr>
<tr>
<td>Split</td>
<td>Supported in <code>&lt;node-chart&gt;</code> and <code>&lt;refine-chart&gt;</code>, Indicates the column to chart. This tag takes an optional columns attribute which specifies the number of columns generated by the split. For example <code>&lt;split columns=&quot;2&quot;&gt;endtime PROCESSWITH bucket(3600, 3, 48)&lt;/split&gt;</code> retrieves the endtime and puts the values into a list of buckets producing 2 columns, the time and the count. The title of the column is used as the axis title. A maximum of 2 <code>&lt;split&gt;</code> tags may be defined, the first for the x-axis, the second the y-axis. <code>&lt;split&gt;os AS 'Detailed OS'&lt;/split&gt;</code></td>
</tr>
<tr>
<td>Y-axis-title</td>
<td>Supported in <code>&lt;node-chart&gt;</code> and <code>&lt;refine-chart&gt;</code>, Indicates the title of the y axis column. This will default to 'Count' unless the <code>&lt;split&gt;</code> provides a second column. <code>&lt;y-axis-title&gt;Hosts&lt;/y-axis-title&gt;</code></td>
</tr>
</tbody>
</table>

The default type of chart can be specified by adding the `default` attribute to `<node-chart>` or `<refine-chart>`. Supported charts depend upon the number of columns specified by `<split>`.

For single columns the supported charts are:

- pie (default)
- bar
- column

For two columns the supported charts are:

- line (default)
- column
Example 00additional_links.xml file

An example XML file is broken down and its constituent parts are described below:
All files start with an XML declaration and an <reports> tag.

```xml
<?xml version="1.0"?>
<reports version="2.0">

The reports version must be 2.0.

External links

Each external link is defined under a <link> tag.

The following example shows a label populated with the text View trouble ticket for hostname, Where hostname is the name of the current host.
The URL in the example is to a trouble-ticketing system with a web interface. This assumes that there is a host attribute called ticketNum which contains the trouble ticket number.

```xml
<link name="Link.Host.Ticket">
  <title>View trouble ticket for %(hostname)s</title>
  <description>Browse trouble ticket system for this host.</description>
  <kind>Host</kind>
  <image>kind/gif/Location_16.gif</image>
  <url>http://tickets.tideway.com/tickets/%(ticketNum)s.cgi</url>
</link>
```

Report links

Each report link is defined under a <node-report> tag.

The following examples retrieves a list of hosts with the same operating system type as the currently viewed host.

```xml
<node-report name="Node.Report.Host.SameOS">
  <title>Hosts with the same OS type</title>
  <description>List of hosts with the same OS type</description>
  <kind>Host</kind>
  <image>system/gif/report_16.gif</image>
  <lookup>False</lookup>
  <where>os_type = %(os_type)r</where>
</node-report>
```
Chart links

Each chart link is defined under a `<node-chart>` tag.

A chart showing access methods for this host node.

```
<node-chart name="Node.Chart.Host.AccessMethod" default="column">
  <title>Host Login Summary Chart</title>
  <description>Host Login Methods on a column chart</description>
  <kind>Host</kind>
  <image>system/gif/column_chart_16.gif</image>
  <where keyword="False">TRAVERSE :::DeviceInfo</where>
  <split>last_access_method as '_|Method|_' </split>
  <show>SUMMARY</show>
</node-chart>
```

SetReport links

Each set report link is defined under a `<refine-report>` tag.

Show the number of hosts per software package on which the currently viewed set of packages are installed.

```
  <title>Package Host Density</title>
  <description>How many Hosts are these Packages installed on</description>
  <kind>Host</kind>
  <image>system/gif/report_16.gif</image>
  <show>
    name,
    version,
    NODECOUNT(TRAVERSE InstalledSoftware:HostedSoftware:Host:Host)
    AS '_|Number of Hosts|_'
  </show>
</refine-report>
```

SetChart links

Each set chart link is defined under a `<refine-chart>` tag.

Summarise the currently viewed set of Software Instance nodes in a pie chart segmented by type.

```
<refine-chart name="Refine.Chart.Host.SISummary" default="pie">
  <title>Software Instance Type Summary</title>
  <description>Show a Summary of the Software Instance Types</description>
  <kind>Host</kind>
</refine-chart>
```
Completion

Finally, the XML file is completed with the closing tag.

```xml
</reports>
```

Custom reporting

The custom reporting feature enables you to perform customization of the reports and channels on the appliance.

Configuration files

The reporting facilities and selection of UI channels shown on each page are configured using xml configuration files which are held in the following directories:

1. `/usr/tideway/data/installed/reports/`
2. `/usr/tideway/data/custom/reports/`

The directories are parsed in the order given (installed before custom), and the files contained in these directories are parsed in alphabetical order, with numbers before letters. This order is important as later definitions for a named report override those loaded earlier. The standard reports are contained in `/usr/tideway/data/installed/reports/00reports.xml`.

The format of the xml file changed in Tideway Foundation 7.3. Upgrades from previous versions convert from the old to new file format. If you add a file in the old format, the system will attempt to automatically convert the file format on start up. You can also use the `tw_convert_reports` tool to convert reports manually. This is described in `tw_convert_reports`.

The configuration is read when the UI process starts. Changes to the report configuration files require a UI restart. Errors in the configuration files do not prevent the Application server from starting but may cause various reports and channels to be missing.

⚠️ You cannot add context sensitive reports to the discovery status page.
The root element of each reports.xml file must be `<reports version="2.0">`. The `<reports>` element can have several types of elements:

- **Standard reports:**
  - `<chart>`: a chart. See `<chart elements>`.

- **Channels:**
  - `<chart-channel>`: a simple chart channel. See `<chart-channel> elements`.
  - `<chart-multi-channel>`: a chart channel with multiple values per column. See `<chart-multi-channel> elements`.
  - `<report-channel>`: a channel containing a list of charts and reports. See `<report-channel> elements`.
  - `<rss-channel>`: a rss feed channel. See `<rss-channel> elements`.
  - `<summary-channel>`: a channel containing node kind counts. See `<summary-channel> elements`.
  - `<time-series-channel>`: a chart channel containing values over time. See `<time-series-channel> elements`.
  - `<video-channel>`: a video channel. See `<video-channel> elements`.
  - `<web-channel>`: a channel containing a web feed. See `<web-channel> elements`.

- **Page information:**
  - `<page>`: the selection of channels on one page. See `<page> elements`.

**<report> elements**

The `<report>` element was extended in version 7.3 by merging in functionality from `<extrareport>` which no longer exists. A `<report>` element requires a `name` attribute giving a unique name to the report.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Provides the main page title for the report. This tag is mandatory. <code>&lt;title&gt;Hosts ordered by Host Owner&lt;/title&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>Populates the title attribute of the HTML link. Presented as a tool tip. Also shown as a subtitle below the main page title. This tag is mandatory. <code>&lt;description&gt;Shows a list of all Discovery Hosts, ordered by their Owner&lt;/description&gt;</code></td>
</tr>
<tr>
<td>Kind</td>
<td>Kind to use in search. Multiple kinds can be specified in a comma separated list or by using the <code>*</code> wildcard. <code>&lt;kind&gt;Host&lt;/kind&gt;</code></td>
</tr>
<tr>
<td>Flags</td>
<td>Any flags to include in the search query. This tag takes an optional <code>keyword</code> attribute which, when given value False, prevents the addition of the <code>FLAGS{ prefix and } postfix</code>. The attribute is normally used if parameters are used control the flags. <code>&lt;flags&gt;include_destroyed&lt;/flags&gt;</code></td>
</tr>
<tr>
<td>With</td>
<td>Any with functions to evaluate in the search query. <code>&lt;with&gt;value(NODECOUNT(TRAVERSE Host:HostedSoftware:RunningSoftware:SoftwareInstance)) AS si_count&lt;/with&gt;</code></td>
</tr>
</tbody>
</table>
Configuration guide

Tag | Details
---|---
Where | Any conditions in the search query. This tag takes a couple of options attributes:
| - **keyword** which, when given value False, prevents the addition of the WHERE keyword when constructing the query. For example, TRAVERSE ::Host must not be prefixed by WHERE.
| - **start** which, when given value False, places the parameter conditions at the start of the query rather than the end. Normally parameter queries are added after the <where> text. However, if there is a need to perform tests before a traversal then they can be placed at the beginning.

```xml
<where>version = ''</where>
```

Order-by | Sort results of query by specified order.

```xml
<order-by>name</order-by>
```

Show | List of attributes to display. This tag takes an optional **keyword** attribute which, when given value False, prevents the addition of the SHOW keyword.

```xml
<show>name, os, #InferredElement:Inference:Primary:HostInfo.hostid</show>
```

Url | Redirect browser when report is selected.

```xml
<url>NetworkMismatchSummaryReport</url>
```

Imports | List of `<import>` each of which contains a Python module to import. These are used by the `<parameters>` for `<convert>`, `<default>` and `<eval>` described below.

```xml
<imports><import>common.timeutil</import></imports>
```

Parameters | List of `<parameter>` each of which contains an interactive parameter filled in by the user. These are described in detail below.

**<parameter> element**

Interactive parameters are defined using `<parameter>` elements. They must have a **name**, representing the name of the parameter, that is unique in the report.

Tag | Details
---|---
Title | Label of the parameter shown when it is rendered in a form. This tag is mandatory.

```xml
<title>Start date</title>
```

Type | Type of control widget to use for the parameter in the form and is detailed below. This tag is mandatory.

```xml
<type>
```

Key | References a replacement construct in the constructed query.

```xml
?key>from</key>
```

Where | Query fragment to add to where clause of the parent element's search string. The reports system inserts the value of the parameter using string substitution with a key of **value**.

```xml
<where>name HAS SUBSTRING %{(value)r}</where>
```

When the query is built from parameters all the parameters are evaluated as specified by `<type>`. If a parameter has a where clause it is substituted into the where clause with a key of **value**. All parameters without a key are then joined together using AND and inserted either at the beginning (<where start="True"> specified) or end of the where clause in the report. The complete query is then constructed. If there are any parameters with a key the completed query has those parameters inserted using string substitution with the specified key of the parameter.
The `<type>` tag must have a `name` attribute which specifies the type of the parameter. It should have one of the following values:

- **TextField**: a text entry field.
- **SelectField**: a list.
- **RelationshipSearchField**: a popover node-selection field.
- **DateTimeField**: a time field.

The tags that can be used with `<type>` depend upon these values.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>If type is SelectField add an <code>All</code> option to the select list (the default). When given value False prevents the addition of the 'All' option. <code>&lt;all&gt;False&lt;/all&gt;</code></td>
</tr>
<tr>
<td>Convert</td>
<td>Function used to convert the default value and user-typed value for use in query. For example, the function could be <code>common.timeutil.convertFromUnix</code>. This will convert the value to Unix form, which can then be added to the query. Referenced functions should be fully specified, and the packages and modules required should appear in <code>&lt;imports&gt;</code> elements, described above. Note that functions are referenced rather than called so do not need parentheses. The function can also be a lambda function taking one parameter. <code>&lt;convert&gt;common.timeutil.convertFromUnix&lt;/convert&gt;</code></td>
</tr>
<tr>
<td>Default</td>
<td>Expression that defines a default value for the parameter. Referenced functions should be fully specified, and the packages and modules required should appear in <code>&lt;imports&gt;</code> elements, described above. <code>&lt;default&gt;common.timeutil.convertToUnix(common.timeutil.currentTime())&lt;/default&gt;</code></td>
</tr>
<tr>
<td>Escape</td>
<td>Escape string value. By default string values are escaped. When given value False prevents the escaping. <code>&lt;escape&gt;False&lt;/escape&gt;</code></td>
</tr>
<tr>
<td>Kind</td>
<td>If type is RelationshipSearchField is used to determine which source kind when finding a list of relationships defined in taxonomy. <code>&lt;kind&gt;Host&lt;/kind&gt;</code></td>
</tr>
<tr>
<td>Size</td>
<td>If type is TextField specifies the size of the text field otherwise specifies the number of visible options in the list. <code>&lt;size&gt;2&lt;/size&gt;</code></td>
</tr>
</tbody>
</table>
| Options | If type is SelectField then there are several ways to specify the selection options:
  - `eval` which evaluates the expression. Referenced functions should be fully specified, and the packages and modules required should appear in `<imports>` elements, described above. `<eval>api.audit.getEvents()</eval>`
  - `option` which contains the option text. The `<option>` takes an optional `value` attribute which is used when the option is selected. If no `value` attribute is present the option text is used. Multiple `<option>` values can be provided. `<option value="21">FTP</option>`
  - `query` which performs a search query the first column of which is used as selection values. `<query>SEARCH Location SHOW name</query>`

Only one of the selection option forms may be specified.

<table>
<thead>
<tr>
<th>Validate</th>
<th>How to validate the parameter. Currently supports:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• integer: value is an integer</td>
</tr>
<tr>
<td></td>
<td>• number: value is a number</td>
</tr>
<tr>
<td></td>
<td>• boolean: value is a boolean</td>
</tr>
</tbody>
</table>
### Tag Details

- **NotEmpty**: value is not empty

  If the value does not validate the form will present an error to the user.

  ```xml
  <validate>NotEmpty</validate>
  ```

---

Bringing all this together, the following element defines a parameter which appears in the UI labelled **Type** as a list with three specified values and no **All** entry. The **<where>** tag means that should the user choose **Host** then `kind(#)=Host` will be added to the report query.

```xml
<parameter name="DQ_Report_Global_type">
  <title>Type</title>
  <type name="SelectField">
    <all>False</all>
    <options>
      <option value="Host">Host</option>
      <option value="SoftwareProductVersion">Software Product Version</option>
      <option value="BusinessApplicationInstance">Application Instance</option>
    </options>
  </type>
  <where>kind(#)="%(value)s"</where>
</parameter>
```

The following report will count the number of instances of software instances on host optionally limiting the software instances to a particular type chosen by the user from a list.

```xml
<report name="Software_Report_InstanceSummary">
  <title>Software Inventory</title>
  <description>Shows summary of distribution of a piece of software</description>
  <kind>SoftwareInstance</kind>
  <show>
    type AS "__Type__",
    product_version AS "__Product Version__"
    PROCESS WITH
    countUnique(1,0)
  </show>
  <parameters>
    <parameter name="Software_Report_InstanceSummary_type">
      <title>Product type</title>
      <type name="SelectField">
        <query>
          SEARCH SoftwareInstance
          ORDER BY type
          SHOW type
          PROCESS WITH unique()
        </query>
      </type>
    </parameter>
  </parameters>
</report>
```
<options>
</options>
</type>
<where>type = %{value}s</where>
</parameter>
</parameters>
</report>

<chart> elements

The <chart> element is fundamentally the same as the <report> element with the following changes:

- the default type of chart can be specified by adding the default attribute to <chart>,
- the <show> tag is used to determine the click through columns of the chart.

Additional tags are:

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Split</td>
<td>Indicates the column to chart. This tag takes an optional columns attribute which specifies the number of columns generated by the split. For example, <code>&lt;split columns=&quot;2&quot;&gt;endtime PROCESSWITH bucket(3600, 3, 48)&lt;/split&gt;</code> retrieves the endtime and puts the values into a list of buckets producing 2 columns, the time and the count. The title of the column is used as the axis title. A maximum of 2 <code>&lt;split&gt;</code> tags may be defined, the first for the x-axis, the second the y-axis. <code>&lt;split&gt;os AS 'Detailed OS'&lt;/split&gt;</code></td>
</tr>
<tr>
<td>Y-axis-title</td>
<td>Indicates the title of the y axis column. This will default to Count unless the <code>&lt;split&gt;</code> provides a second column. <code>&lt;y-axis-title&gt;Hosts&lt;/y-axis-title&gt;</code></td>
</tr>
</tbody>
</table>

For single columns the supported charts are:

- pie (default)
- bar
- column

For two columns the supported charts are:

- line (default)
- column

The following chart will show a count of different OS classifications. By default a pie chart will be shown and when clicked through a summary report for the appropriate hosts. When displaying bar and column charts the y-axis will be labelled Hosts.

<chart name="Infrastructure.Chart.OSClassification" default="pie">
<title>Host OS Classification</title>
<description>Show count of Hosts for each OS Classification</description>
The `<chart-channel>` element requires a `name` attribute giving a unique name to the chart channel. An optional `default` attribute gives the initial chart type.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory. <code>&lt;title&gt;Operating Systems&lt;/title&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory. <code>&lt;description&gt;Operating System Reports and Charts&lt;/description&gt;</code></td>
</tr>
<tr>
<td>Kind</td>
<td>Kind to use in search. Multiple kinds can be specified in a comma separated list or by using the <code>*</code> wildcard. <code>&lt;kind&gt;Host&lt;/kind&gt;</code></td>
</tr>
<tr>
<td>With</td>
<td>Any with functions to evaluate in the search query. <code>&lt;with&gt;value(NODECOUNT(TRAVERSE Host:HostedSoftware:RunningSoftware:SoftwareInstance)) AS si_count&lt;/with&gt;</code></td>
</tr>
<tr>
<td>Where</td>
<td>Any conditions in the search query. <code>&lt;where&gt;version = ''&lt;/where&gt;</code></td>
</tr>
<tr>
<td>Order-by</td>
<td>Sort results of query by specified order. <code>&lt;order-by&gt;name&lt;/order-by&gt;</code></td>
</tr>
<tr>
<td>Split</td>
<td>Indicates the column to chart. The title of the column is used as the axis title. <code>&lt;split&gt;os AS 'Detailed OS'&lt;/split&gt;</code></td>
</tr>
<tr>
<td>Show</td>
<td>List of attributes to display when click through chart. <code>&lt;show&gt;name, os, #InferredElement:Inference:Primary:HostInfo.hostid&lt;/show&gt;</code></td>
</tr>
</tbody>
</table>

The following channel shows a pie chart of software product categories:

```xml
<chart-channel name="Channel.SWCategory" default="pie">
    <title>Software Products By Category</title>
    <description>Shows a list of the Software by Category</description>
    <split>explode(#Element:Maintainer:Pattern:Pattern.categories) AS 'Software Category'</split>
    <kind>SoftwareInstance</kind>
    <show>
        summary,
        #Element:Maintainer:Pattern:Pattern.categories AS 'Software Category'
    </show>
</chart-channel>
```
<chart-multi-channel> elements

The `<chart-multi-channel>` element requires a `name` attribute giving a unique name to the chart multi channel. An optional `default` attribute gives the initial chart type.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory.&lt;title&gt;Operating Systems&lt;/title&gt;</td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory.&lt;description&gt;Operating System Reports and Charts&lt;/description&gt;</td>
</tr>
<tr>
<td>Kind</td>
<td>Kind to use in search. Multiple kinds can be specified in a comma separated list or by using the * wildcard.&lt;kind&gt;Host&lt;/kind&gt;</td>
</tr>
<tr>
<td>With</td>
<td>Any with functions to evaluate in the search query.&lt;with&gt;value(NODECOUNT(TRAVERSE Host:HostedSoftware:RunningSoftware:SoftwareInstance)) AS si_count&lt;/with&gt;</td>
</tr>
<tr>
<td>Where</td>
<td>Any conditions in the search query.&lt;where&gt;version = ''&lt;/where&gt;</td>
</tr>
<tr>
<td>Order-by</td>
<td>Sort results of query by specified order.&lt;order-by&gt;name&lt;/order-by&gt;</td>
</tr>
<tr>
<td>Split</td>
<td>Indicates the column to chart. The title of the column is used as the axis title. There must be 2 <code>&lt;split&gt;</code> tags.&lt;split&gt;os AS 'Detailed OS'&lt;/split&gt;</td>
</tr>
<tr>
<td>Show</td>
<td>List of attributes to display when click through chart.&lt;show&gt;name, os, #InferredElement:Inference:Primary:HostInfo.hostid&lt;/show&gt;</td>
</tr>
</tbody>
</table>

The following channel shows a column chart of database versions with a column for each product type. Each column contains a list of found versions.

```xml
<chart-multi-channel name="Channel.SWDBVersion" default="column_nolegend">
    <title>Database versions</title>
    <description>Number and version of all the Database instances</description>
    <split>type</split>
    <split>(product_version or 'Unknown')</split>
    <kind>Pattern</kind>
    <where>
        'Relational Database Management Systems' in categories
        TRAVERSE Pattern:Maintainer:Element:SoftwareInstance
    </where>
    <show>SUMMARY</show>
</chart-multi-channel>
```

<report-channel> elements

The `<report-channel>` element requires a `name` attribute giving a unique name to the report channel.
The following channel contains a link to a report and chart.

```xml
<report-channel name="Infrastructure.Channel.NetworkPolicy">
    <title>Network Policies</title>
    <description>Shows a list of Network Infrastructure Reports</description>
    <chart>Infrastructure.Chart.IPAddressDistribution</chart>
</report-channel>
```

### <rss-channel> elements

The `<rss-channel>` element requires a `name` attribute giving a unique name to the rss channel.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory.</td>
</tr>
<tr>
<td>Render-description</td>
<td>Flag if to show RSS feed description, defaults to False.</td>
</tr>
<tr>
<td>Url</td>
<td>URL for RSS feed. This tag is mandatory.</td>
</tr>
</tbody>
</table>

The following channel shows an RSS feed for VMware.

```xml
<rss-channel name="Channel.RSS.VMware">
    <title>VMware Feed</title>
    <description>Shows the latest info from VMware</description>
    <url>http://vmware.simplefeed.net/rss/?f=2fe7e950-01de-11de-3b40-003048605010</url>
</rss-channel>
```
<summary-channel> elements

The `<summary-channel>` element requires a `name` attribute giving a unique name to the summary channel.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;title&gt;Operating Systems&lt;/title&gt;</code></td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;description&gt;Operating System Reports and Charts&lt;/description&gt;</code></td>
</tr>
<tr>
<td>Image</td>
<td>Image to show for channel.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;image&gt;discovery&lt;/image&gt;</code></td>
</tr>
<tr>
<td>Kind-count</td>
<td>Node kind for which to show count. Multiple <code>&lt;kind-count&gt;</code> entries can be specified.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;kind-count&gt;Host&lt;/kind-count&gt;</code></td>
</tr>
</tbody>
</table>

The following channel shows the number of `BusinessApplicationInstance` and `SoftwareInstance` nodes.

```xml
<summary-channel name="Applications.Channel.Summary">
  <title>Application Summary</title>
  <description>Shows a summary of Applications</description>
  <image>applications</image>
  <kind-count>BusinessApplicationInstance</kind-count>
  <kind-count>SoftwareInstance</kind-count>
</summary-channel>
```

<time-series-channel> elements

The `<time-series-channel>` element requires a `name` attribute giving a unique name to the time series channel.

This is identical to `<chart-channel>` with two exceptions:

- It performs a historical search and partition the result into a number of buckets. By default, this is 5 but can be overridden by specifying the `time-series` attribute on the `<time-series-channel>` element.
- `<split>` is optional and if not present the chart will be based on the number of the specified node kind rather than the value of the specified attribute.

The following channel shows the number of Hosts for each Unix OS over time.

```xml
<time-series-channel name="Applications.Channel.Summary">
  <title>Application Summary</title>
  <description>Shows a summary of Applications</description>
  <image>applications</image>
  <kind-count>Host</kind-count>
</time-series-channel>
```
<time-series-channel name="Channel.OSUNIX" time-series="7" default="line">
  <title>UNIX Operating Systems</title>
  <description>Shows a count of Hosts for each UNIX OS</description>
  <split>os_type as "OS Version"</split>
  <kind>Host</kind>
  <where>os_class = "UNIX"</where>
  <order-by>os_type</order-by>
  <show>SUMMARY</show>
</time-series-channel>

<video-channel> elements

The <video-channel> element requires a name attribute giving a unique name to the video channel.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory.</td>
</tr>
<tr>
<td>Image</td>
<td>Image to show for channel.</td>
</tr>
<tr>
<td>Src</td>
<td>Video source. This tag is mandatory.</td>
</tr>
</tbody>
</table>

The following channel shows an video feed for creating host profiles.

<video-channel name="Channel.Video.HostProfiles">
  <title>Feature Tutorial: Host Profiles</title>
  <description>Video Tutorial that explains the Host Profiles feature</description>
  <src>/videos/HostProfiles.swf</src>
</video-channel>

<web-channel> elements

The <web-channel> element requires a name attribute giving a unique name to the web channel.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Channel title. This tag is mandatory.</td>
</tr>
<tr>
<td>Description</td>
<td>Shown when editing the channels. This tag is mandatory.</td>
</tr>
<tr>
<td>URL</td>
<td>URL for the web feed. This tag is mandatory.</td>
</tr>
</tbody>
</table>

{{<url>http://www.google.com</url>}}
The following channel shows a web feed for the BMC Atrium Discovery Community forum.

```xml
<web-channel name="Channel.Web.Community">
  <title>Tideway Community Update</title>
  <description>Shows the Tideway Community update.</description>
  <url>http://www.tideway.com/widgets/foundation-forum/</url>
</web-channel>
```

**<page> elements**

The `<page>` element requires a `name` attribute giving a unique name to the page.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Reference a previously defined channel. There is an optional <code>builtin</code> attribute which must be specified if the channel is <code>builtin</code>. Multiple channel tags can be specified. The order in which the channels appear on a page is governed by the order of the <code>&lt;channel&gt;</code> tags.</td>
</tr>
<tr>
<td></td>
<td><code>&lt;chart builtin=&quot;True&quot;&gt;Discovery.Channel.Status&lt;/chart&gt;</code></td>
</tr>
</tbody>
</table>

**Built-in channels**

The following built-in channels are defined:

<table>
<thead>
<tr>
<th>Built-In Channel Name</th>
<th>Description</th>
</tr>
</thead>
</table>

**Built-in page names**

The following are the identifiers for pages with configurable content:

<table>
<thead>
<tr>
<th>Built-in Page Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApplicationHome</td>
<td>The front page of the applications module.</td>
</tr>
<tr>
<td>DiscoveryReports</td>
<td>Reports in the discovery module.</td>
</tr>
<tr>
<td>Home</td>
<td>The appliance home page.</td>
</tr>
<tr>
<td>InfrastructureHome</td>
<td>The front page of the infrastructure module.</td>
</tr>
<tr>
<td>Reports</td>
<td>The front page of the reports module.</td>
</tr>
</tbody>
</table>