**Contacting BMC Software**

You can access the BMC Software website at [http://www.bmc.com](http://www.bmc.com). From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

**United States and Canada**

<table>
<thead>
<tr>
<th>Address</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC SOFTWARE INC</td>
<td>713 918 8800</td>
<td>713 918 8000</td>
</tr>
<tr>
<td>2103 CITYWEST BLVD</td>
<td>800 841 2031</td>
<td></td>
</tr>
<tr>
<td>HOUSTON TX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>77042-2827</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Outside United States and Canada**

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>(01) 713 918 8800</td>
<td>(01) 713 918 8000</td>
</tr>
</tbody>
</table>

© Copyright 1999-2018 BMC Software, Inc.

Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of BMC Software, Inc.

BMC, BMC Software, the BMC logo, the BMC Software logo, and other BMC marks, and the tagline “Bring IT to Life” are the exclusive properties of BMC Software, Inc., or its affiliates or subsidiaries and are registered or may be registered with the U.S. Patent and Trademark Office and in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

For BMC Control-M Products that are licensed on the “per CPU - Full Capacity” unit of measurement and installed in an Amazon Web Services (“AWS”), Microsoft Azure (“Azure”), or Google Cloud Platform (“GCP”) cloud environment, a license is required for the total number of CPUs in each AWS, Azure, or GCP instance upon which the Product is installed or which the Product manages, either remotely or locally. For AWS and GCP, one CPU is equivalent to one vCPU, as defined by AWS. For Azure, one CPU is equivalent to up to four Virtual Cores (as defined by Azure), rounded up to the closest multiple of four.

**Server Endpoint Licensing**

All machines upon which any Control-M component is installed or upon which Control-M managed workload runs must be licensed. This includes Control-M Agent/Agentless platforms onto which one or more application plug-ins are installed but also includes Control-M Agent/Agentless platforms where no application plug-ins are installed. Control-M Agent/Agentless platforms on which jobs are ordered are counted regardless of whether those jobs execute or not. All Server Endpoints are counted, including development, staging, QA, pre-production, test, and production environments.

The licensing guidelines for application plug-ins are as follows:
- ERP and BI/DI: The application server(s) upon which Control-M managed processes are executed should be licensed in addition to the Control-M Agent machine(s) (in some cases, this may be the same machine).
- Databases: Each database server upon which Control-M managed database related processes are being executed should be counted in addition to the Control-M Agent machine(s).
- AFT and MFT: Only the machine(s) upon which the AFT or MFT plug-in is installed should be licensed.
- Web Services, Java & Messaging: only the Control-M Agent machine(s) upon which the plug-in is installed should be licensed.
- Backup: The Control-M Agent machine(s) where the Backup plug-in is installed and also the hosts which are running the backup server software should be licensed (note that this excludes the client machines for which the Backup Server software is managing actual backup processes except where a backup takes place of the backup server machine itself).
- Cloud: only the Control-M Agent machine(s) upon which the plug-in is installed should be licensed.
- Hadoop: All machines in each managed Hadoop Cluster should be licensed.

IBM® Tivoli® Business Service Manager, IBM Tivoli Workload Scheduler, IBM Cognos, IBM InfoSphere DataStage, IBM i (AS/400), IBM Websphere, and AIX® are the trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

UNIX® is the registered trademark of The Open Group in the US and other countries.

Linux is the registered trademark of Linus Torvalds.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

SAP® R/2 and SAP R/3, SAP Business Objects, and SAP NetWeaver are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

**Restricted rights legend**

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Field 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.

**Customer support**

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

**Support website**

You can obtain technical support from BMC 24 hours a day, 7 days a week at (http://www.bmc.com/support). From this website, you can:
• Read overviews about support services and programs that BMC offers
• Find the most current information about BMC products
• Search a database for issues similar to yours and possible solutions
• Order or download product documentation
• Download products and maintenance
• Report an issue or ask a question
• Subscribe to receive proactive e-mail alerts when new product notices are released
• Find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by telephone or e-mail
In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC
Have the following information available so that Customer Support can begin working on your issue immediately:

• Product information
  • Product name
  • Product version (release number)
  • License number and password (trial or permanent)
• Operating system and environment information
  • Machine type
  • Operating system type, version, and service pack or other maintenance level such as PUT or PTF
  • System hardware configuration
  • Serial numbers
  • Related software (database, application, and communication) including type, version, and service pack or maintenance level
• Sequence of events leading to the issue
• Commands and options that you used
• Messages received (and the time and date that you received them)
  • Product error messages
  • Messages from the operating system, such as file system full
  • Messages from related software

License key and password information
If you have questions about your license key or password, contact BMC as follows:

- **(USA or Canada)** Contact the Order Services Password Team at 800 841 2031, or send an e-mail message to ContractsPasswordAdministration@bmc.com.
- **(Europe, the Middle East, and Africa)** Fax your questions to EMEA Contracts Administration at +31 20 354 8702, or send an e-mail message to password@bmc.com.
- **(Asia-Pacific)** Contact your BMC sales representative or your local BMC office.

**Third party Software**

For the provisions described in the BMC License Agreement and Order related to third party products or technologies included in the BMC Product, see [https://docs.bmc.com/docs/display/workloadautomation/Control-M+Workload+Automation+Documentation](https://docs.bmc.com/docs/display/workloadautomation/Control-M+Workload+Automation+Documentation) and click **Third-party software (TPS).**
## Contents

**Introduction to SSL** ............................................................................................................. 8

**Zone 1 SSL configuration** .................................................................................................. 10
- Configuring the SSL Control-M/EM Web Server in HTTPS ...................................................... 10
- Managing connectors ........................................................................................................................ 11
- Testing SSL on the Control-M Web Server ................................................................................. 11
- Configuring ciphers for the Control-M Web Server ........................................................................ 12
- Reverting back to the HTTP connector ........................................................................................... 13
- Disabling SSL for the Control-M Web Server ................................................................................... 13

**Zone 2 and 3 SSL configuration** ............................................................................................. 14
- Deploying SSL in zone 2 and 3 .......................................................................................................... 14
- Enabling SSL in zone 2 and 3 ........................................................................................................... 15
- Enabling SSL on specific Control-M/Agents ................................................................................... 16
- Configuring protocols and ciphers for zones 2 and 3 ...................................................................... 16
- Testing SSL on zones 2 and 3 ............................................................................................................ 17
- Disabling SSL on Control-M/EM ........................................................................................................ 18
- Disabling SSL on Control-M/Server ................................................................................................... 18
- Disabling SSL on Control-M/Agents ................................................................................................. 19
- Modifying SSL configuration between Control-M/Agent and Remote hosts .................................. 19

**LDAP SSL configuration** ....................................................................................................... 21
- Configuring communication with LDAP or Active Directory servers using SSL ........................... 21
- Obtaining a certificate file from the Windows Active Directory server ........................................... 22

**Additional SSL configurations** ............................................................................................... 23
- Enabling SSL for Control-M/EM Add-ons ....................................................................................... 23
- Disabling SSL for Control-M/EM Add-ons ....................................................................................... 23
- Configuring SSL in EMAPI and EMAPI_CLI ................................................................................... 24
- Configuring SSL for CORBA ............................................................................................................ 25
- Using your own encrypted password ............................................................................................... 26
- Replacing CORBA Certificates ....................................................................................................... 26
- Disabling SSL for CORBA ............................................................................................................... 28
Introduction to SSL

Control-M works with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, ensuring secure communication between the various Control-M components.

SSL for Control-M authenticates and secures communications between one or more of the following:

- Control-M/EM server and its clients (see **Zone 1 SSL configuration** (on page 10))
- Control-M Web server (see **Zone 1 SSL configuration** (on page 10))
- Control-M/EM Server and Control-M/Servers (see **Zone 2 and 3 SSL configuration** (on page 14))
- Control-M/Server and Control-M/Agents (see **Zone 2 and 3 SSL configuration** (on page 14))
- Control-M/EM and the LDAP Server (see **LDAP SSL configuration** (on page 21))

Depending on your setup, you can enable security for the following components:

- Control-M Self Service and Control-M Workload Change Manager (WCM) web apps (see **Zone 1 SSL configuration** (on page 10))
- Control-M Workload Archiving server, Batch Impact Manager, and Control-M/Forecast (see **Additional SSL configurations** (on page 23))

To configure SSL in your environment, you must do the following:

- **Get Signed Certificates**: Signed certificates are required for enabling secured communication using SSL protocols. You need to request a recognized Certificate Authority (CA) with a Certificate Signing Request file, to get a signed certificate from that CA. The signed certificate also contains your public key. In many cases, you need to receive a certificate chain from the CA, which allows a client to trust a server. If the server’s certificate was issued by an intermediate CA, which has a certificate trusted by a root CA (directly or by a chain).

BMC recommends that you replace the existing certificates using one of the following methods:

- Bringing your own certificate (signed by an external recognized certified CA).
- Generate new certificates using the Control-M Configuration Manager. Use this method when you are using the site CA provided by BMC (different per customer). The site CA is stored in the Control-M/EM Server machine, and is used to sign the certificates for Control-M/EM, Control-M/Server, and Control-M/Agent. How to use this method is specified in "Enabling SSL for Control-M components using BMC self-signed Certificates". Using this method, it is also possible to configure SSL for each of the zones in the diagram below.
- **Deploy SSL**: To create an SSL policy, you must deploy the keystore, which contains the private key, and the certificate to the relevant Control-M components.

- **Enable SSL**: Enable SSL for relevant Control-M components.

The following diagram shows the multiple ways you can configure SSL in environment based on zones:
Zone 1 SSL configuration

Zone 1 SSL configuration allows you to configure SSL between Control-M/EM Web Server and Control-M client applications.

The following procedures describe how to configure SSL in zone 1.

- Configuring the SSL Control-M/EM Web Server in HTTPS (on page 10)
- Managing connectors (on page 11)
- Testing SSL on the Control-M Web Server (on page 11)
- Configuring ciphers for the Control-M Web Server (on page 12)
- Reverting back to the HTTP connector (on page 13)
- Disabling SSL for the Control-M Web Server (on page 13)

Configuring the SSL Control-M/EM Web Server in HTTPS

This procedure describes how to configure SSL between Control-M client applications and the Control-M/EM Web Server in HTTPS. This SSL configuration occurs in zone 1.

**NOTE:** If you are working in a Control-M/EM Distributed environment with multiple Control-M Web Servers, or in a high availability environment, you must provide a different keystore for each server. If you are working in a high availability environment with SSL, run the following command on both the primary and secondary hosts: `em restore_host_config -interface_name -name <FQDN>`

**NOTE:** BMC recommends that you bring your own certificate for the usage of the Web Server. BMC provided demo certificates are supported in the Web Server with limited conditions (see “Using Web Server certificates that comes with Control-M/EM Server installation”). If you generated a new certificate using Manage SSL in the CCM, HTTPS cannot be used and you cannot log in to Control-M client using SSL.

➢ To configure SSL for Control-M/EM Web Server in HTTPS:

1. Navigate to one of the following directories:
   - UNIX: `<Product Home Directory>/data/SSL/config directory`
   - Windows: `<Product Home Directory>\Data\SSL\config directory`
2. Edit the fields in the `csr_params.cfg`.
3. Create the private key and certificate signing request file by running the following:
   
   ```
   <ctmkeytool location>/ctmkeytool -create_csr -password <private key password>
   ```

   **NOTE:** For more information, see `ctmkeytool` (on page 29).
4. Use the Certificate Signing Request (CSR) file to obtain the certificate file, and possibly the certificate chain file, from an external recognized CA. All certificates must be valid X509 certificates.
5. Create the `tomcat.p12` keystore file by running the following command:
openssl pkcs12 -in <certificate pem file name> -inkey <private key file name> -export -passout pass:<keystore password> -passin pass:<private key password> -CAfile <certificate chain pem file name> -chain -out tomcat.p12 -name <keystore friendly name> -caname <ca friendly name>


7. Turn on SSL mode, by doing the following:
   a. Type the following command:
      ```
      manage_webserver
      ```
   b. Press 1 to display the Tomcat configuration
   c. Press 4 to display SSL mode.
   d. Set the current configuration for using SSL to [true]

8. In the CCM, recycle the Web Server, as described in

Managing connectors

This procedure describes how to add, change, or delete connectors. By default, the installation includes a secure and non-secure connector. If you want add, change, or delete, use this procedure.

➢ To manage connectors:
1. Type the following command:
   ```
   manage_webserver
   ```
2. Press 1 to display the Tomcat configuration.
3. Press 3 to display Secure Connector Configuration.
4. Do one of the following:
   • To add a new connector, do the following:
     a. Press 2.
     b. Provide the name of the keystore this connector will use.
   • To delete a connector, do the following:
     d. Choose the connector you want to delete from the list.

Testing SSL on the Control-M Web Server

This procedure describes how to test the SSL connector on the Control-M Web Server.

➢ To test SSL on the Control-M Web Server:
1. Verify that the Web Server certificate is installed on the Control-M client computer.
If it is not installed, copy the p12 keystore file that contains the certificate to the Control-M client computer and run the installation.

2. Verify the hostname and port which are used by the relevant connector, by doing the following:
   a. Type the following command:
      
      ```
      manage_webserver
      ```
   b. Press 1 to display the Tomcat configuration
   c. Press 3 to display the secure connector configuration
   d. Press 1 to display the list of secure connectors

3. From the web browser on the Control-M client computer, type the URL as follows:
   
   ```
   https://<web server's fqdn>:<web server's port>
   ```

   The Control-M Welcome Page appears.

### Configuring ciphers for the Control-M Web Server

This procedure describes how to configure ciphers for the Control-M Web Server in zone 1. The Control-M Web Server only supports the TLSv1.2 SSL protocol. The available ciphers for Zone 1 are defined in `<EM Home Directory>/ini/ssl_tomcat_ciphers.xml`. If you want to use a cipher that is not listed in the file or limit the listed ciphers perform this procedure.

➢ To configure ciphers for the Control-M Web Server:

1. From the Web Server computer, run the following command and verify that this cipher exists in the output of the command.

   ```
   em openssl ciphers -V
   ```


3. Add the ciphers to the relevant secured connector, as follows:
   a. Type the following command:

      ```
      manage_webserver
      ```
   b. Press 1 to display the Tomcat configuration.
   c. Press 3 to display Secure Connector Configuration.
   d. Press 3 to edit the SSL Connector.
   e. Select the connector you want to edit.

4. Select 1 and insert the list containing all the cipher names this connector must support, as they appear in the `<EM Home Directory>/ini/ssl_tomcat_ciphers.xml` file.

5. From the CCM, recycle the Control-M Web Server.
Reverting back to the HTTP connector

This procedure describes how to revert back to an HTTP connector if you deleted it.

➢ To revert back to the HTTP connector:

1. Do one of the following:
   - To replace the server.xml file if the delete action was the last action in the manage_webserver utility, do the following:
     a. Navigate to the following directory:
        
        UNIX: %EM_HOME%/etc/emweb/tomcat/conf/  
        Windows: %EM_HOME%\emweb\tomcat\conf
     b. Delete the server.xml file
     c. Rename the server.xml.backup file to server.xml.
   - To edit the server.xml file add the http connector:
     
     <Connector port="18080" protocol="HTTP/1.1"
     connectionTimeout="20000"
     redirectPort="8443" />

2. From the CCM, recycle the Web Server.

Disabling SSL for the Control-M Web Server

This procedure describes how to disable SSL for the Control-M Web Server in zone 1.

➢ To turn off SSL mode on the Web Server:

1. Type the following command:

   manage_webserver

2. Press 1 to display the Tomcat configuration.

3. Press 4 to display SSL mode.

   If current configuration for using SSL is set to [true], press Y to change the configuration.

4. Press N to stop using SSL.

5. From the CCM, recycle the Control-M Web Server.
Zone 2 and 3 SSL configuration

Zone 2 allows you to configure SSL between Control-M/EM server and Control-M/Server. Zone 3 allows you to configure SSL between Control-M/Server and Control-M/Agent.

When SSL is configured on the Control-M/Server, Control-M/EM and all Control-M/Agents that are connected to this Control-M/Server must also be configured with SSL. Control-M/EM, Control-M/Server and all Control-M/Agents must use certificates that are signed by the same root Certificate Authority.

The following procedures describe how to configure SSL in zone 2 and 3:

- Deploying SSL in zone 2 and 3 (on page 14)
- Enabling SSL in zone 2 and 3 (on page 15)
- Enabling SSL on specific Control-M/Agents (on page 16)
- Configuring protocols and ciphers for zones 2 and 3 (on page 16)
- Testing SSL on zones 2 and 3 (on page 17)
- Disabling SSL on Control-M/EM (on page 18)
- Disabling SSL on Control-M/Server (on page 18)
- Disabling SSL on Control-M/Agents (on page 19)
- Modifying SSL configuration between Control-M/Agent and Remote hosts (on page 19)

Deploying SSL in zone 2 and 3

This procedure describes how to deploy SSL from Control-M/Server to Control-M/EM server or to Control-M/Agents.

➢ To deploy SSL in zone 2 and 3:

1. Navigate to one of the following directories:
   - UNIX: <Product Home Directory>/data/SSL/config directory
   - Windows: <Product Home Directory>\Data\SSL\config directory

2. Edit the fields in the <csr_params.cfg>.

3. Create the private key and certificate signing request file by running the following:

   <ctmkeytool location>/ctmkeytool -create_csr -password <private key password>

   **NOTE**: For more information, see ctmkeytool (on page 29).

4. Use the Certificate Signing Request (CSR) file to obtain the certificate file, and possibly the certificate chain file, from an external recognized CA. All certificates must be valid X509 certificates.

5. Create the <tomcat.p12> keystore file on each component by running the following command:
openssl pkcs12 -in <certificate pem file name> -inkey <private key file name> -export
    -passout pass:<keystore password> -passin pass:<private key password> -CAfile
    <certificate chain pem file name|certificate authority pem file name> -chain -out
    <keystore p12 name>

6. Deploy SSL on each component:
<ctmkeytool location>/ctmkeytool -keystore <p12 keystore file with its full path>
    -password <keystore password> -passwkey <name of file containing the password
    encryption key, with its full path>

7. Update the supported protocols and ciphers in your environment, as described in Configuring
    protocols and ciphers for zones 2 and 3 (on page 16).

Enabling SSL in zone 2 and 3

This procedure describes how to enable SSL in zone 2 and 3.

➢ To enable SSL in zone 2 and 3:

1. Enable SSL on the CMS and Gateway components by doing the following:
   a. From the CCM, change the value of the CmsCommMode system parameter to AUTO or to SSL,
      as described in .
   b. Restart the Control-M/EM Configuration Agent, Naming Service, and CMS.
   c. Recycle the Gateway(s) that are connected to the Control-M/Servers where SSL is configured.

2. Enable SSL on Control-M/Server by doing the following:
   a. Run the ctm.sys utility.
   b. Press 2 - System Parameters.
   c. Press n to move to the next page of parameters.
   d. Set option 9 Secure Sockets Layer to ENABLED.
      All connected Control-M/Agents are now configured with SSL. For more information, see SSL
      communication parameters.
   e. Restart the Control-M/Server Configuration Agent and the Control-M/Server component.

3. Enable SSL on each Control-M/Agent by doing the following:
   a. From the CCM, right-click the required Control-M/Agent and select Properties and then click the
      Communication.
   b. From the Secure Socket Layer drop-down list, select Default.
      This inherits the value from the Control-M/Server configuration.
   c. Click Test.
   d. After the test has validated the settings, click OK.
      If you deployed a new certificate for the Control-M/Agent, as described in Deploying SSL in zone
      2 and 3 (on page 14), you need to restart the Control-M/Agent. Control-M/Agents that are not
      enabled with SSL cannot connect to an SSL enabled Control-M/Server.
Enabling SSL on specific Control-M/Agents

This procedure describes how to enable SSL on specific Control-M/Agents when Control-M/Server is not enabled with SSL.

**NOTE:** In these Control-M/Agents, you must deploy SSL configuration using a certificate signed by the same root CA as Control-M/Server, as described in Deploying SSL in zone 2 and 3 (on page 14).

To enable SSL on specific Control-M/Agents:

1. From the CCM, right-click the required Control-M/Agent and select **Properties** and then click the **Communication**.
2. From the **Secure Socket Layer** drop-down list, select **Default**.
3. Click **Test**.
4. After the test has validated the settings, click **OK**.

Configuring protocols and ciphers for zones 2 and 3

This procedure describes how to configure SSL connections for zones 2 and 3 to work with specific protocols and ciphers.

To use more than one cipher, use a space to separate them.

To configure protocols and ciphers for zones 2 and 3:

1. On both the client and server computers, run the following command:
   
   ```bash
   openssl ciphers -V
   
   ``

   The ciphers that appear on both computers can be used for the connection.

2. Filter for the allowed ciphers according to the secured protocol, by running the following commands:
   
   ```bash
   openssl ciphers -V -ssl3
   openssl ciphers -V -tls1
   
   ``

3. Write the ciphers in the SSL configuration exactly as they appear in the available ciphers list.

4. Do one of the following:
   
   - **UNIX:** Edit the relevant policy file, as described in **UNIX environment** (on page 40).
   - **Windows:** Edit the relevant policy file, as described in **Microsoft Windows environment** (on page 43).

5. Edit the provider_options field, as follows:

   a. **SSLProtocol=<desired protocol>**, where **<desired protocol>** can be one or more of the following protocols:
      
      - **SSLv3**
      - **TLS1**
      - **TLS1_2**

   b. After the last specified protocol, add a comma (,), and then the cipher suite specifier.
For SSLv3 and TLS1 protocols, the cipher suite specifier is `SSLV3CipherSuite=`, and for TLS1_2 protocol, the cipher suite specifier is `TLSCipherSuite=`. Then, specify the list of ciphers from the above list.

The cipher suite specifier and list of ciphers must be specified for each specified protocol.

6. Restart the relevant component.

**EXAMPLE:**

- **SSLv3 protocol:**
  ```
  provider_options=SSLProtocol=SSLv3,SSLV3CipherSuite=DHE-RSA-AES256-SHA
  AES256-SHA DHE-RSA-AES128-SHA
  ```

- **TLS1 protocol:**
  ```
  provider_options=SSLProtocol=TLS1,SSLV3CipherSuite=DHE-RSA-AES256-SHA
  AES256-SHA DHE-RSA-AES128-SHA
  ```

- **TLS1_2 protocol:**
  ```
  provider_options=SSLProtocol=TLS1_2,TLSCipherSuite=DHE-RSA-AES256-SHA
  AES256-SHA DHE-RSA-AES128-SHA
  ```

**NOTE:**

- Several protocols and cipher suites can be configured in the server section, while only one protocol and cipher suite can be configured in the client section.
- Before defining the client side for the connection between Control-M/Agent and remote hosts, see Modifying SSL configuration between Control-M/Agent and Remote hosts (on page 19).
- All ciphers with SHA256 can be used only with TLS1_2 protocol.
- If you work on a Control-M/Server installed on AIX and you plan to use Advanced Encryption Standard (AES) ciphers, you must configure the system to work with the TLS1 SSL protocol.
- If you plan to configure Control-M/Server to use the SSLv3 protocol with ciphers DHE-RSA-AES128-SHA AES128-SHA or DHE-RSA-AES256-SHA AES256-SHA, the Control-M/Agents must be version 8.0.00.300 and above.

## Testing SSL on zones 2 and 3

This procedure describes how to test SSL on zones 2 and 3.

1. **To test the SSL on zones 2 and 3:**
   ```
   <ctmkeytool location>/ctmkeytool -status -host <Control-M/Server name as displayed in CCM> -keystore_pass <password of the local keystore on EM> -key_pass <password of the private key in the keystore>
   ```
   For more information, see ctmkeytool (on page 29).

2. Verify that all operations between Control-M/EM and Control-M/Server, such as job ordering, are working.
3. From the CCM, verify that all Control-M/Servers and Control-M/Agents are Up.
4. Test the connection between Control-M/Server and Control-M-Agent by running the following commands:
   • ag_diag_comm
   • ctm_diag_comm

Disabling SSL on Control-M/EM

This procedure describes how to disable SSL on Control-M/EM in zone 2 and 3.

➢ To disable SSL on Control-M/EM:

1. From the Components Tree pane, select the Control-M/EM component and from the Home tab, in the Definitions group, click System Parameters.
   The Control-M/EM System Parameters dialog box appears.
2. In the left pane, click Advanced.
3. From the system parameters table, in the Name column double click the CmsCommMode parameter.
   The CONTROL-M/EM - Update System Parameter dialog box appears.
4. In the Value field, type TCP.
5. Click Save.
6. Stop all Control-M components in the CCM and then shut down Control-M/EM Configuration Agent, Naming Service, and CMS, as follows:
   • stop_config_agent
   • stop_cms (not required for distributed EM)
7. Start the Control-M/EM Configuration Agent, Naming Service, and CMS, as follows:
   • start_config_agent
   • start_cms (not required for distributed EM)
8. Start all Control-M components in the CCM.

Disabling SSL on Control-M/Server

This procedure describes how to disable SSL on the Control-M/Server and the connected Control-M/Agents, using the Control-M/Server ctm.sys utility.

➢ To disable SSL on Control-M/Server:

1. From the Control-M/Server computer, run ctm.sys.
2. Select option 2 System Parameters.
3. Press n to move to the next page of parameters.
4. Set option 9 Secure Sockets Layer to DISABLE.
This also turns off SSL on all connected Control-M/Agents that were configured with SSL, if the **Secure Sockets Layer** field was set to Default in the CCM.

For more information, see SSL system parameters.

Disabling SSL on Control-M/Agents

This procedure describes how to disable SSL on Control-M/Agents that are not connected to a Control-M/Server.

➢ To disable SSL on Control-M/Agents:

1. Edit the **CONFIG.dat** file that is located under `<Agent home directory>/ctm/data`.
2. Change the value of **COMMOPT** to **SSL=N**.
3. Save the file and restart the Control-M/Agent.

Modifying SSL configuration between Control-M/Agent and Remote hosts

This procedure describes how to modify SSL configuration between Control-M/Agent and Remote hosts to enable running utilities on remote hosts.

**NOTE:** If you are using an expired SSL certificate for Control-M/Agent, all jobs with remote host utilities will fail.

The following message is an example that appears in the job output:

```
SEVERE: SSLException occurred while sending message to <vl-tlv-ctm-qa18:8000>.
SEVERE: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Certificates does not conform to algorithm constraints
SEVERE: Failed to send to Agent or receive from Agent.
Result: Failure
Failed to send to Agent or receive from Agent.
```

➢ To modify SSL configuration:

1. Do one of the following:
   - **Windows:** Navigate to the following path in the Registry Editor:
     
     HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M/Agent <instance>\SecurityPolicy\RU\server
   - **UNIX:** Navigate to the following directory:
2. Edit the **provider_options** parameter, if needed.

   **EXAMPLE:**
   
   ```
   SSLProtocol=TLS1,SSLV3CipherSuite=DHE-RSA-AES256-SHA AES256-SHA DES-CBC3-SHA DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC-SHA DHE-RSA-AES256-SHA AES256-SHA
   ```

3. From the **RU** key, create or edit the **client** key.

4. Add or edit the following parameters in the **client** key:
   - **ssl_protocol**
   - **cipher_suite**

   **EXAMPLE:**
   ```
   ssl_protocol=TLSv1 or TLSv1.2
   cipher_suite=TLS_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_3DES_EDE_CBC_SHA SSL_DHE_RSA_WITH_DES_CBC_SHA SSL_DHE_RSA_WITH_AES_128_CBC_SHA SSL_DHE_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_AES_256_CBC_SHA SSL_DHE_RSA_WITH_AES_128_CBC_SHA SSL_DHE_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_AES_256_CBC_SHA SSL_DHE_RSA_WITH_AES_128_CBC_SHA SSL_DHE_RSA_WITH_AES_256_CBC_SHA SSL_RSA_WITH_AES_128_CBC_SHA SSL_RSA_WITH_AES_256_CBC_SHA
   ```
LDAP SSL configuration

The following procedures describe how to configure SSL in an LDAP environment:

- Configuring communication with LDAP or Active Directory servers using SSL (on page 21)
- Obtaining a certificate file from the Windows Active Directory server (on page 22)

Configuring communication with LDAP or Active Directory servers using SSL

The following procedure describes how to enable SSL for LDAP and Active when Control-M/EM is installed on UNIX and Linux operating systems.

➢ To enable SSL:

1. Obtain a .pem format certificate file (em_ldap_ssl.pem) from the directory server. Creating and exporting certificate files are different for each LDAP server vendor. Refer to your LDAP server administrator to obtain the correct certificate file. For an example on how to obtain a certificate from the Windows Active Directory, see the Example above.

2. Place the em_ldap_ssl.pem file into the <Control-M/EM_directory>/etc/keystore directory.

   NOTE: If you are working in a high availability environment, place the certificate file (.pem) in the same location in both installations.

3. Do one of the following:

   • UNIX:
     a. Verify that a randomness device is installed on the Control-M/EM computer as follows:
     b. Locate either the random or urandom file in the /dev directory. If you find the random file, verify that its path is part of the search path.
     c. If neither of these files exist, open the <Control-M/EM_directory>/etc/ldap.conf file in a text editor.
     d. Locate the #TLS_RANDFILE <Control-M/EM_directory>/ini/ssl/rnd.bin line and remove the # character.
     e. Save the modified file.

   • Windows: Use the Microsoft MMC utility to install the certificate on your computer.

4. Set an environment variable named LDAPCONF with a value pointing to the ldap.conf file, which gets set by the EM UNIX account profile.

   EXAMPLE: setenv LDAPCONF <Control-M/EM_directory>/ctm_em/etc/ldap.conf

5. Restart all Control-M/EM components by applying stop_all and start_all commands.
6. Define an LDAP server that can communicate with Control-M/EM in SSL mode, as described in Defining LDAP system parameters. If you do not apply all of the above steps, LDAP authentication in SSL mode fails.

7. Recycle the GUI and CMS components.
   See the following example: Obtaining a certificate file from the Windows Active Directory server (on page 22).

8. To test the SSL connection Control-M/EM to the LDAP server, run the following:
   ```bash
   openssl s_client -connect <LDAP Server hostname>:<port> -CAfile <Control-M/EM Home Directory>/etc/keystore/em_ldap_ssl.pem
   ```
   The default port for SSL connections to the LDAP server is 636.

## Obtaining a certificate file from the Windows Active Directory server

This procedure describes how to obtain a certificate file from the Windows Active Directory server. The .pem format certificate file name must be renamed `em_ldap_ssl.pem`. The rename procedure is outlined in the Active Directory server example in step 8b.

1. Select **Programs => Administrative Tools => Certification Authority** to open the Certification Authority application.

2. Right-click **Certification Authority**, and select **Properties**.

3. Click **View Certificate** to view the certificate's page.

4. In the **Details** tab, click **Copy to file** to start the Certificate Export Wizard.

5. In the **Export File Format** page, select the Base-64 Encoded X.509 (.cer) format and click **Next**.

6. Enter a file name with a .cer extension that includes the Active Directory server name.

7. Complete the steps in the wizard to create an exported copy of the Certification Authority for the Active Directory server.

8. Convert the certificate from .cer format to .pem format as follows:
   a. Using FTP or another file copying application, copy the Active Directory server certificate file you just created to a system on which the Active Directory client runs.

   b. Log on to the system where you copied the certificate and run the following command:
   ```bash
   openssl x509 -in AD certificate name -out em_ldap_ssl.pem
   ```
   **AD certificate name** represents the file name given in step 6.

   **NOTE:** For a certificate file obtained from a different LDAP server, rename the file `em_ldap_ssl.pem`.

   The location and name of the certificate (.pem) file can be changed by configuring the TLS_CACERT parameter value in the `<Control-M/EM_directory>/etc/ldap.conf` file for the new path and name.
Additional SSL configurations

The following procedures describe how to configure SSL for Control-M Add-ons, Control-M/EM API, and CORBA:

- Enabling SSL for Control-M/EM Add-ons (on page 23)
- Disabling SSL for Control-M/EM Add-ons (on page 23)
- Configuring SSL in EMAPI and EMAPI_CLI (on page 24)
- Configuring SSL for CORBA (on page 25)
- Using your own encrypted password (on page 26)
- Replacing CORBA Certificates (on page 26)
- Disabling SSL for CORBA (on page 28)

Enabling SSL for Control-M/EM Add-ons

This procedure describes how to enable SSL for Control-M/EM Add-ons.

➢ To enable SSL:

- Do one of the following:
  - To enable SSL on the Control-M Workload Archiving server, run the Configuring SSL for CORBA (on page 25) on both the primary Control-M/EM computer and the Control-M/EM Distributed computer where Control-M Workload Archiving is installed.
  - To enable SSL on BIM, Control-M Self Service, and Control-M/Forecast, do the following:
    a. Run the Configuring SSL for CORBA (on page 25) procedure where the Add-on is installed. If you are working in a Distributed environment, run this procedure on the primary Control-M/EM as well.
    b. Run Configuring the SSL Control-M/EM Web Server in HTTPS (on page 10). If you are working in a Distributed environment, perform this procedure on each Control-M/EM Distributed computer.

Disabling SSL for Control-M/EM Add-ons

This procedure describes how to disable SSL for Control-M/EM Add-ons.
To disable SSL:

Do one of the following:

- To disable SSL on the Control-M Workload Archiving server, run the Disabling SSL for CORBA (on page 28) on both the primary Control-M/EM computer and the Control-M/EM Distributed computer where Control-M Workload Archiving is installed.

- To disable SSL on BIM, Control-M Self Service, and Control-M/Forecast, do the following:
  
  a. Run the Disabling SSL for CORBA (on page 28) procedure where the Add-on is installed. If you are working in a Distributed environment, run this procedure on the primary Control-M/EM as well.
  
  b. Run Disabling SSL for the Control-M Web Server (on page 13). If you are working in a Distributed environment, perform this procedure on each Control-M/EM Distributed computer.

Configuring SSL in EMAPI and EMAPI_CLI

This procedure describes how to configure SSL in EMAPI and EMAPI_CLI by creating a Keystore from Certificates using the JAVA keytool.

**NOTE:** In this procedure it is assumed that the `<password>` is your stored password and the `<keystore>` is your keystore file name. If you have files other than .pem files you need to use openssl to convert file types.

**Before you begin**

Ensure that JAVA_HOME is defined.

To configure SSL:

1. Prepare all CA's chain.pem files that are signed to your web server in the same directory.
2. Open a command line and use the installation cd to navigate to that directory.
3. For the root CA .pem file (such as `<root>` ) run the following command:
   ```
   %JAVA_HOME%/bin/keytool -keystore <keystore> -storepass <password> -importcert -noprompt -trustcacerts -file <root>
   ```
4. For other .pem files (such as `<file>` ) run the following command:
   ```
   %JAVA_HOME%/bin/keytool -import -trustcacerts -alias <alias unique name> -file <file> -keystore <keystore>
   ```
5. Do one of the following:
   
   - **EMAPI users:** Go to your emapi directory and replace the emapi.keystore with the new `<keystore>` file under /keystore directory.
   
   - **emapi_cli users:** Create a new directory for emapi_cli and move your `<keystore>` file to that directory.
6. Update the following tags in your **communication.xml** file:
   
   - SSLCertDir tag with value of the directory where `<keystore>` is located.
   
   - SSLClientKeystoreFile tag with value of `<keystore>`
SSLClientPassPhrase tag with value of <password>

**NOTE:** In case SSLClientPassPhrase tag is not set, the default behavior is to look for emapi_keystore.ini file under EMAPI_DIR directory.

### Configuring SSL for CORBA

This procedure describes how to configure SSL between components that use the CORBA protocol.

➢ **To configure SSL for CORBA:**

1. In the `jacorb.properties` file, located in `<Control-M/EM Home Directory>/etc/jacorb.properties`, do the following:
   a. Set the `jacorb.security.support_ssl` parameter to `on`.
   b. If you are using AIX with IBM JSSE implementation, set the following parameters:
      - `jacorb.security.jsse.server.key_manager_algorithm=IbmX509`
      - `jacorb.security.jsse.server.trust_manager_algorithm=IbmX509`
      - `jacorb.security.jsse.client.key_manager_algorithm=IbmX509`
      - `jacorb.security.jsse.client.trust_manager_algorithm=IbmX509`
   c. If you are using Sun Solaris, set the following parameters:
      - `jacorb.security.jsse.server.key_manager_algorithm=SunX509`
      - `jacorb.security.jsse.server.trust_manager_algorithm=SunX509`
      - `jacorb.security.jsse.client.key_manager_algorithm=SunX509`
      - `jacorb.security.jsse.client.trust_manager_algorithm=SunX509`
   d. If you are using a different operation system, these fields must be commented out.

2. Stop the Control-M/EM Configuration Agent, Naming Service, and CMS. If you are on Control-M/EM Distributed computer, stop the Control-M/EM Configuration Agent.

3. *(UNIX only)*, type the following command:
   ```
   setenv DISPLAY <terminal_IP_address>
   ```

4. From `<EM Home Directory>/bin`, run one of the following:
   - **UNIX**: `orbconfigure`
   - **Windows**: `orbconfigure.vbs`

   The **Domain Configuration** window appears.

5. In the **Domain Settings** panel, do the following:
   a. Check the **Use Secure Sockets Layer (SSL)** checkbox.
   b. In the given path, under **Use TAO internal configuration file** checkbox, change the file name `client_server.conf` to `ssl_client_server.conf`.

6. Click **Next**.

   The **Naming Service panel** appears (If needed configure the Host and Port values).
7. Click **Next** and then click **Finish**.

8. If you ran the above on a Control-M/EM Distributed computer, run the following on the primary Control-M/EM:
   - `oradmin ns stop`
   - `oradmin ns start`
   This registers the services again in the Naming Service using the new configuration.

9. Start the Control-M/EM Configuration Agent.

### Using your own encrypted password

The keystore password for demonstration certificates is not encrypted. To use an encrypted password, run the `changePass` utility as follows:

- (UNIX) **changePass** in the `<Control-M/EM_directory>/bin` directory
- (Windows) **changePass** in the `<Control-M/EM_directory>\bin` directory

This utility accepts a keytool password, encrypts it, and updates the `jacorb.security.keystore` and `jacorb.security.keystore_password_crypt` parameters in the `jacorb.properties` file.

**NOTE:** If you configure the `<Control-M/EM_directory>/etc/jacorb.properties` file to use SSL, you will not be able to browse non-secure naming services.

### Replacing CORBA Certificates

This procedure describes how to bring your own CORBA certificate.

**Before you begin:**

Verify that you have one or all of the following: the signed certificate, its private key, and its CA chain in one of the following formats:

- PEM (Privacy Enhanced Mail) files for each of the following: Certificate, Private Key, and Trusted Root CAs
- PKCS#12 file with the Certificate, private key, and CAs. If the PKCS#12 contains multiple certificates and key pairs, then you must also have available the name of the pair to use.

**NOTE:** All components must be signed using the same CA Certificate. Private key passwords must exist for PKCS#12 and PEM, however the Certificate PEM must not to be locked/protected by password.

To replace CORBA certificates:

1. Create a temporary folder in the root directory of the computer where the Control-M/EM resides.
2. Place your pem\pkcs12 files in the temporary folder.
3. Run the **Manage_SSL_BYO** script according to the following usage:
   ```
   PEM format: Manage_SSL_BYO -input pem -component {component name}
   ```
--output { Manage_SSL output deployment directory}
--output_keystores_password {Component keystore password}
--certificate {certificate pem file}
--private_key {certificate private key pem file}
--password {password for private key pem file}
--ca_certificates {CA certificate chain PEM file}

PKCS#12 format: Manage_SSL_BYO -input PKCS#12
--component {component name}
--output { Manage_SSL output deployment directory}
--output_keystores_password {Component keystore password}
--file {pkcs#12 file to import from}
--password {password of pkcs#12 file}
[-cert_and_key_name {name of the certificate and private key to import }]

Supported -component values:

CONTROL-M_Agent
CONTROL-M_Server
CONTROL-M_EnterpriseManagerServers
CONTROL-M_BPI
CONTROL-M_Web_Application
CONTROL-M_EnterpriseManagerAPI
CONTROL-M_zOS

4. To generate Control-M/EM keystore files while using pem files into the CTMEM folder, run the following:

    Manage_SSL_BYO -input pem -component CONTROL-M_EnterpriseManagerServers
    -output CTMEM -output_keystores -password abcd1234 -certificate certificate.pem
    -private_key privatekey.pem -password abcd1234 -ca_certificates ca-chain.cert.pem

5. To generate Control-M/EM keystore files while using the all.p12 file into the CTMEM folder, run the following:

    Manage_SSL_BYO -input PKCS#12 -component CONTROL-M_EnterpriseManagerServers
    -output CTMEM -output_keystores -file em.p12 -password abcd1234
    -cert_and_key_name


7. Mark as cert_dir the directory specified by -output in step 3.

8. From your current directory, run the following:
Disabling SSL for CORBA

This procedure describes how to configure SSL between components that use the CORBA protocol.

➢ To configure SSL for CORBA:

1. In the jacorb.properties file, located in `<Control-M/EM Home Directory>/etc/jacorb.properties`, set the jacorb.security.support_ssl parameter to off.

2. Stop the Control-M/EM Configuration Agent, Naming Service, and CMS. If you are on Control-M/EM Distributed computer, stop the Control-M/EM Configuration Agent.

3. (UNIX only), type the following command:

   ```bash
   setenv DISPLAY <terminal_IP_address>
   ```

4. From `<EM Home Directory>/bin`, run one of the following:

   **UNIX**: orbconfigure
   
   **Windows**: orbconfigure.vbs

   The Domain Configuration window appears.

5. In the Domain Settings panel, do the following:

   a. Clear the Use Secure Sockets Layer (SSL) checkbox.

   b. In the given path, under Use TAO internal configuration file checkbox, change the file name to ssl_client_server.conf to client_server.conf.

6. Click Next.

   The Naming Service panel appears (If needed configure the Host and Port values).

7. Click Next and then click Finish.

8. If you ran the above on a Control-M/EM Distributed computer, run the following on the primary Control-M/EM:

   • orbadmin ns stop
   
   • orbadmin ns start

   This registers the services again in the Naming Service using the new configuration.

9. Start the Control-M/EM Configuration Agent.
ctmkeytool

The ctmkeytool script can perform the following functions:

- Generating a private key (pem) file and certificate signing request (csr) file using the `create_csr` option (on page 29).
- Deploying a p12 keystore file including the certificate. This deployment updates the relevant SSL configuration on the computer, as described in Deployment option (on page 30).
- On Control-M/EM, testing the connection against a specific Control-M/Server using the Status option (on page 30).

The ctmkeytool script is located in the following directories:

- **Control-M/EM**: `<EM Home Directory>/bin/`
- **Control-M/Server**: `<Control-M/Server Home Directory>/scripts/`
- **Control-M/Agent**: `<Agent Home Directory>/EXE_9.0.19.000/`

**NOTE:**

- The script must be executed with the full path.
- (UNIX only) Verify that you run under em tcsh.
- The script is not available for Control-M/Agent for IBM i (AS/400).

`create_csr` option

The ctmkeytool script creates the private key file and the certificate signing request file, using the configuration file `csr_params.cfg` located in `<Product Home Directory>/data/SSL/config` directory. Verify that the user running the script has the correct permissions to create and update the directories.

Before running the script, edit the `csr_params.cfg` file and update the values of all its fields in the `[dn]` section. The CN field must contain the FQDN of the computer where the certificate is issued.

The script usage is, as follows:

```bash
<ctmkeytool location>/ctmkeytool -create_csr -password <private key password>
```

This command creates the private key file and the certificate signing request file:

- The default name for the generated private key file consists of the CN field in the configuration file, and the timestamp of the file generation. The suffix of the private key file is `.pem`. The file is located in the `<Product Home Directory>/data/SSL/private_keys` directory.

- The default name of the generated certificate signing request file consists of the CN field in the configuration file, and the timestamp of the file generation. The suffix of the certificate signing request file is `.csr`. The file is located in one of the following locations:
You can specify a different configuration file name using the -conf_file flag.

**EXAMPLE:** `<ctmkeytool location>/ctmkeytool -create_csr -password <private key password> -conf_file <Product Home Directory>/config_files/csr_config_file.cfg`

To specify a different name for the created private key file and certificate signing request file, use the -out flag.

**EXAMPLE:** `<ctmkeytool location>/ctmkeytool -create_csr -password <private key password> -out <filename>`

The provided name is used for both the pem file and the csr file.

**Deployment option**

The ctmkeytool script usage with the deployment option is as follows:

```
<ctmkeytool directory>/ctmkeytool -keystore <p12 keystore file with its full path> -password <keystore password> -passwkey <name of file containing the password encryption key with full path>
```

This creates and updates the relevant SSL configuration on the computer where Control-M components are installed.

After you run the script, you must restart the Control-M/EM Configuration Agent, CMS, Naming Service, and the relevant gateways, Control-M/Server and Control-M/Server Configuration Agent, and the relevant Control-M/Agents.

**Status option**

The ctmkeytool status option tests and receives details about the SSL environment on Control-M/EM and its SSL connection to Control-M/Server. The script usage is as follows:

```
<EM Home Directory>/bin/ctmkeytool -status -host <Control-M/Server name as displayed in CCM> -keystore_pass <password of the local keystore on EM> -key_pass <password of the private key in the keystore>
```

The displayed output includes the following details:

- SSL configuration enablement status.
- The status of the connection between the selected Gateway and Control-M/Server. If the connection is not ok, you are prompted for further testing.
- The ports on Control-M/Server that the Gateway and CMS connects to.
- The names of the file holding the keystore used by Control-M/EM Gateway(s) and CMS.
- SSL protocols used by Control-M/EM Gateway(s) and CMS
- SSL level used by Control-M/EM Gateway(s) and CMS
Uninstall option

The ctmkeytool-uninstall option is used to revert to the last SSL certificate and configuration used by the product before the current keystore was deployed. You can only revert to the previous configuration. Any configuration prior cannot be retrieved.

You can retrieve the previous configuration on Control-M/EM, Control-M/Server, and Control-M/Agent.

The ctmkeytool uninstall option script usage is as follows:

<ctmkeytool directory>/ctmkeytool -uninstall

After you run the script, you must restart the Control-M/EM Configuration Agent, CMS, Naming Service, and the relevant gateways, Control-M/Server and Control-M/Server Configuration Agent, and the relevant Control-M/Agents.
Advanced SSL configuration

The following topics describe how to set up advanced SSL configurations with certificates, security policies, and CORBA:

- Generating self signed certificates (on page 32)
- Security policies (on page 35)
- Advanced CORBA SSL configuration (on page 50)

Generating self signed certificates

This procedure describes how to generate self signed certificates for Control-M/EM and Control-M/Server and replace the pre-installed certificates, which includes updating expiration days and generating the certificates.

➢ To generate certificates:

1. In the CCM, from the Home tab, select System Configuration > Control-M/EM System Parameters.
2. Define SSL parameters, as described in Defining SSL system parameters.
3. Select the component in the left pane, and then from the Tools drop-down list, select Security > Manage SSL.
4. Do one of the following:
   - If you want to use the BMC-provided demo certificate, select Use the following site certificate authority, and do the following:
     a. The parameter fields in the first screen are populated with values supplied by BMC. Click Next.
     b. Select one of the following:
        o All Components of Control-M: Generate certificates for all components
        o By Component Type, and then select the components from the drop-down list.

You can also enter a Unique Component Instance ID (email). You can do this for all components of this type, or for each instance of this component. Note that this option is not available for the Control-M/EM Server component.

**NOTE:** For Control-M for z/OS only, you can enter a Key Store Password, which must be eight characters in length.
   c. Accept the default location to save the generated certificates, or enter a new path.
   d. Click Next to generate the certificates, and then Submit after the generation process finishes.
If you want to create a new and unique instance of the pre-installed site Certificate Authority, select Create new Certificate Authority for the site, and do the following:

e. Click Yes to accept generating a new certificate.

You are informed that certificates will be generated for all the Control-M components.

f. Enter the Country Name, Common Name (FQDN), Email Address and other optional parameters of the CA and click Next.

g. If you want to use a password, enter the password and click Next.

h. Accept the default location to save the generated certificates, or type in a new path.

i. Click Next to generate the certificates.

j. Click Submit after the generation process finishes.

The new certificate deployment directories are created in the location you requested in the CCM client machine.

5. Copy the directory Certificate_for_<component name> to a temporary directory in the computer where the component is installed. For example: <tempLocation>.

6. Stop the component.

7. From the root directory of the Control-M component, run the following command:

   - Windows - <tempLocation>\setup.bat
   - UNIX - <tempLocation>/setup.sh

EXAMPLE: If you placed the deployment directories in /p/Control-M_new_demo, and your Control-M/Enterprise Manager is installed at /bmc/Control-M_EM/Default, then you must run the commands inside the UNIX shell as follows:

   - $ cd /bmc/Control-M_EM/Default
   - $ /p/Control-M_new_demo/Certificate_for_CONTROL-M_EnterpriseManagerServes/setup.sh

The files are deployed to the required locations and the Control-M component uses either the default keystore password, or specified Key Store Password.

8. Restart the relevant component.
Certificate copies for Control-M for z/OS

For Control-M for Z/OS you need to pass the directory content to your z/OS Control-M administrator. The following table describes the keystore files for z/OS.

<table>
<thead>
<tr>
<th>Key store file</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOAGATE.p12</td>
<td>Export the certificate for Control-M for z/OS with the key-pair to be used by IOAGATE in PKCS#12 format. The password for the PKCS#12 file is displayed in the summary window that is generated when running the Generate Component Certificates wizard.</td>
</tr>
<tr>
<td>CA.pem</td>
<td>Export the certificate of the Site CA that signed the certificate in PEM format when CLIAUTH=YES (which uses client authentication) is defined in IOAGATE.</td>
</tr>
</tbody>
</table>

For more information about how to use these files, see the INCONTROL for z/OS Installation Guide, Appendix B "IOAGATE installation and configuration considerations, SSL support".

Restoring a BMC self-signed certificate

This procedure describes how to restore a BMC self-signed certificate from a backup for Control-M client, Control-M/EM server, Control-M/Server, and Control-M/Agent.

➢ To restore a BMC self-signed certificate:

- Run one of the following:
  - **UNIX**: `<sslBackupDir>/setup.sh`
  - **Windows**: `<sslBackupDir>\setup.bat`

  The setup scripts save a backup of the certificate state prior to the deployment in a separate directory in the `ssl_backup` directory.
Control-M Web Server certificates

The Control-M Web Server certificates are included in the Control-M/EM server installation. If you use these certificates, the Control-M client can connect to the Control-M/EM server if the following conditions are met:

- The user had confirmed the connection after a warning appeared on the login window, stating that the server’s certificate is not trusted by the Control-M client’s operating system.
- The certificate is the default BMC certificate provided during the Control-M/EM installation. This is checked according to the OU field on the certificate installed on Control-M client. The expected value is **BMC CTMDemo CA**.
- The `trusted_sites.txt` file does not exist under the root parent folder of the Control-M client installation.

**EXAMPLE:** If the installation is under `C:\Program Files\BMC Software\Control-M\EM\EXAMPLE_COMPUTER`, then the Control-M client searches for the file under `C:\Program Files\BMC Software\Control-M EM`.

Security policies

The security policy is defined by entries made in security policy tables. A Site Policy table is required for each major Control-M component in zone 2 and 3 (Control-M/Server, Control-M/Agent, and Control-M/EM). The entries in these Site Policy tables provide the basic framework for the Control-M site’s security policy. Additions and modifications to the Site Policy, if needed, are defined in optional Application Policy tables for various Control-M functions. Entries in these tables add to and supersede the entries in the Site Policy tables.

On UNIX computers, the security policy tables are contained in `.plc` files. On Microsoft Windows computers, these tables are contained in the Registry.

SSL communication policy is based on variable value pairs – called attributes – that are stored in Policy Tables. Each UNIX stanza (or Microsoft Windows Registry key) contains appropriate attributes. Some attributes do not apply to certain functions, some do not apply to certain security levels, and some cannot be changed.

Security policy is implemented by assigning values to the attribute variables described in the Security policy table referred to in Security policy variables (on page 36). Default policy values for each major Control-M component are specified in that component’s `.site.plc` file or `site` Registry hive.

When a network communication connection is established, the profile for that connection is obtained from variables in the `.plc` files (for UNIX) or in the Registry (for Microsoft Windows). The `.plc` files are described on Sample `.plc` files (on page 41). The Microsoft Windows Registry is described on Microsoft Windows environment (on page 43).

Changes to the key database, key database password, and security policy do not take effect until you restart Control-M/Server, Control-M/Agent, and Control-M/EM.
## Security policy variables

The following security policy variables are located in the appropriate Microsoft Windows Registry keys and UNIX .plc files and are applicable to Control-M/EM, Control-M/Server, and Control-M/Agent. To configure the security policy, you need to update the values of these variables.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>security_level</td>
<td>A digit from 1 through 4. These levels are described in Security levels (on page 37).</td>
</tr>
<tr>
<td>bindir</td>
<td>Absolute path to a subdirectory containing the dynamically loaded security binary modules. For example:</td>
</tr>
<tr>
<td></td>
<td>C:\ Program Files\ BMC Software\ Control-M Server\ ctm_server\ exe</td>
</tr>
<tr>
<td>bindir64</td>
<td>bindir for 64-bit computer. For example:</td>
</tr>
<tr>
<td></td>
<td>C:\ Program Files\ BMC Software\ Control-M Server\ ctm_server\ exe</td>
</tr>
<tr>
<td>sksdir</td>
<td>Absolute path to a Security Key Store read/write subdirectory where Control-M encrypted keys are stored. For example:</td>
</tr>
<tr>
<td></td>
<td>C:\ Program Files\ BMC Software\ Control-M Server\ ctm_server\ data\ SSL\ cert</td>
</tr>
<tr>
<td>securitydir</td>
<td>Absolute path to read only subdirectory where *.kdb key databases and key material files are stored. For example:</td>
</tr>
<tr>
<td></td>
<td>&quot;securitydir&quot;=&quot;C:\ Program Files\ BMC Software\ Control-M Server\ ctm_server\ data\ SSL\ cert&quot;</td>
</tr>
<tr>
<td>password</td>
<td>Encrypted password (generated by the bmcryptpw utility), followed by a comma, followed by the absolute path of the keymaterial file (used</td>
</tr>
<tr>
<td></td>
<td>for 3 DES key computation). Embedded blanks are not allowed. See To create an SSL key database (Recommended task summary) and To change the key database password (Maintaining certificates).</td>
</tr>
<tr>
<td>keyfile</td>
<td>Absolute path of the key database file. For example:</td>
</tr>
<tr>
<td></td>
<td>keyfile=C:\ Program Files\ BMC Software\ Control-M Server\ data\ SSL\ cert\ ctmkeystore.p12</td>
</tr>
<tr>
<td>identity</td>
<td>Key pair label (CADN, CODN, NSDN, or AGDN) in a key database.</td>
</tr>
<tr>
<td>logdir</td>
<td>Absolute path to subdirectory containing the log file. For example:</td>
</tr>
<tr>
<td></td>
<td>&quot;logdir&quot;=&quot;C:\ Program Files\ BMC Software\ Control-M/ Server\ ctm_server\ data\ SSL\ log&quot;</td>
</tr>
<tr>
<td>loglevel</td>
<td>One or more of the following values separated by commas:</td>
</tr>
<tr>
<td></td>
<td>ERROR WARNING INFO TRACE</td>
</tr>
<tr>
<td>logfile</td>
<td>Log file (path and) name. For example:</td>
</tr>
<tr>
<td></td>
<td>logfile=gtw_ssl.log</td>
</tr>
</tbody>
</table>
Variable Description

provider_options Determines SSL protocol(s) that will be used and cipher(s) that will be used for each protocol.

provider_options=SSLProtocol=SSLv3,SSLV3CipherSuite =<ciphers list>
provider_options=SSLProtocol=TLS1,SSLV3CipherSuite =<ciphers list>
provider_options=SSLProtocol=TLS1_2,TLSCipherSuite =<ciphers list>

NOTE: All ciphers with SHA256 can be used only with TLS1_2 protocol.

Security levels

There are 4 possible security levels determining the level of the connection’s security. The default security level for each product is 4.

The following table describes the security provided and requirements for each security level.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Security</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Encryption only</td>
<td>Key Pair, both endpoints must be configured for security level 1.</td>
</tr>
<tr>
<td>2</td>
<td>Encryption and presence of valid</td>
<td>Server was deployed with a valid certificate (possibly with a certificate</td>
</tr>
<tr>
<td></td>
<td>certificate on the server (with no server authentication)</td>
<td>chain), and the client was deployed with a certificate which is trusted by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the same root CA (possibly with a certificate chain).</td>
</tr>
<tr>
<td>3</td>
<td>Server authentication</td>
<td>Server was deployed with a valid certificate (possibly with a certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>chain), and the client was deployed with a certificate which is trusted by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the same root CA (possibly with a certificate chain).</td>
</tr>
<tr>
<td>4</td>
<td>Client and server authentication</td>
<td>Same as level 3, and in addition both sides must be configured with security level 4.</td>
</tr>
</tbody>
</table>

In zone 2, Control-M/EM is the client and Control-M/Server is the server. In zone 3, some of the connections Control-M/Server acts as the server and the Control-M/Agent acts as the client, and for other connections the Control-M/Agent acts as the server and the Control-M/Server acts as the client.
You must define the same security level for a pair of components that communicate with each other. However, you can define level 3 for communication in a server role and level 4 for communication in a client role to the communication channel between Control-M/User and Control-M/Server.

Security level 1

Security level 1 provides privacy only. After a secure connection is established, user data is encrypted using TripleDES. This level does not provide authentication. When a client-server connection is established, a session key is generated and exchanged using the Diffie-Helman secure key exchange method. Security level 1 usually prevents access by a casual network browser. To prevent access by a skilled and determined intruder, use security level 2 or later.

Security Level 2

Security level 2 implements the Secure Socket Layer protocol. A server operating at security level 2 accesses a private database of key pairs and retrieves the key pair named in the identity attribute of its security policy. It uses the key pair values and accompanying certificate to establish an SSL connection with the client.

A client operating at security level 2 accepts the server's certificate. SSL ordinarily requires the client to establish a chain of trust for the server's certificate down to a trusted root. But, in security level 2, the client omits this step and accepts the server's certificate if the certificate's attributes (for example, inception and expiration date) are acceptable.

When using security level 2, the server and client cannot be sure of each other's identity. Nevertheless, a secure exchange of the session key occurs and privacy superior to that of security level 1 is provided.

Security Level 3

Security level 3 operates like security level 2 except that the client must use its own database of certificates to establish a chain of trust for the server's certificate down to a trusted root. This is in addition to the requirement that all other attributes of the server's certificate be acceptable. Therefore, the client can be certain of the identity of the server, but the server cannot be certain of the identity of the client. This connection is said to have server authentication only.

Security Level 4

Security level 4 provides privacy and authentication for both client and server. Security level 4 is enforced by the server. After a handshake with the client as described in security level 3, the server sends a message to the client demanding an additional handshake.

The client returns its own certificate, which the server verifies down to a trusted root. If the client does not provide a certificate that the server can verify, the server shuts down the connection. Since each peer has identified itself to the other, this connection is said to have mutual authentication.

After changing the security level, restart the following components:
Access files

Access files use email fields in server certificates for authentication. Access files can be defined for Control-M/Server and Control-M/Agent. The default access file for Control-M/Server is called access, and it is located in the \texttt{<Control-M/Server Home Directory>/data/SSL/cert} directory. The default access file for Control-M/Agent is called access, and it is located in the \texttt{<Agent Home Directory>/data/SSL/cert} directory.

Both files contain lines similar to these:

\begin{verbatim}
[SSL_SERVER]
;
ALLOW_ACL = *
DENY_ACL =
\end{verbatim}

The following table describes the parameters in the access file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_SERVER</td>
<td>Authentication confirming a server's identity</td>
</tr>
<tr>
<td>ALLOW_ACL</td>
<td>Allows signed certificates to be sent to specified addresses. Default: *</td>
</tr>
<tr>
<td></td>
<td>(Allow every client).</td>
</tr>
<tr>
<td>DENY_ACL</td>
<td>Deny the sending of signed certificates to specified e-mail addresses.</td>
</tr>
<tr>
<td></td>
<td>Default: blank (Does not deny any client).</td>
</tr>
</tbody>
</table>

The security level must be 4. For more information, see Security Level 4 (on page 38).

The server certificate email field is checked after the regular SSL handshake, and after both peers have checked that the certificates that they received are signed by a trusted root CA.

DENY_ACL and ALLOW_ACL are used to control the sending of signed certificates to email destinations.

\textbf{EXAMPLE}: Include the following lines in an access file to accept only the certificates issued to controlm@bmc.com and email@bmc.com. The access file must deny all other certificates, including those signed by a trusted root CA.

\begin{verbatim}
[SSL_SERVER]
;
ALLOW_ACL = controlm@bmc.com,email@bmc.com
DENY_ACL =
\end{verbatim}
UNIX environment

In the UNIX environment, Policy Tables are implemented in ASCII text Policy Files in standard .INI format. Policy Tables are stored in .plc files located in these directories:

- **Control-M/Server**: <CONTROL-M/Server home directory>/data/SSL/cert
- **Control-M/Agent**: <CONTROL-M/Agent home directory>/ctm/data/SSL/cert
- **Control-M/Agent for IBM i (AS/400)**: <CONTROL-M/Agent home directory>/data/SSL/cert
- **Control-M/EM**: <CONTROL-M/EM home Directory>/etc/site/resource/ssl/cert

Stanzas in the Site Policy and Application Policy files specify the security module that supports the role defined by the stanza. If an application acts like a network server, security attributes are obtained from the [server] stanza. If an application acts like a network client, security attributes are obtained from the [client] stanza.

A typical Site Policy is shown in Control-M/Server site.plc file (on page 41). When establishing the type of communication listed in the table below, the values (if any) in the relevant application .plc file override the values in the site.plc file.

<table>
<thead>
<tr>
<th>Application .plc file</th>
<th>Type of communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>ns.plc</td>
<td>Control-M/Server to Control-M/Agent</td>
</tr>
<tr>
<td>co.plc</td>
<td>Control-M/Server to Control-M/EM</td>
</tr>
<tr>
<td>ca.plc</td>
<td>Control-M/Server Configuration Agent to CCM</td>
</tr>
<tr>
<td>ag.plc</td>
<td>Control-M/Agent to Control-M/Server</td>
</tr>
<tr>
<td>ru.plc</td>
<td>Control-M/Agent and Remote host utilities</td>
</tr>
<tr>
<td>gtw.plc</td>
<td>Control-M/EM Gateway to Control-M/Server</td>
</tr>
<tr>
<td>cmsg.plc</td>
<td>Control-M Configuration Server to Control-M Agent</td>
</tr>
<tr>
<td>em.plc</td>
<td>Control-M/EM internal encryption purposes</td>
</tr>
</tbody>
</table>
Sample .plc files
Sample .plc files similar to the following are provided with the installation:

- Control-M/Server co.plc file (on page 41)
- Control-M/Server site.plc file (on page 41)
- Control-M/Server ns.plc file (on page 42)
- Control-M/Enterprise Manager site.plc file (on page 42)
- Control-M/Enterprise Manager site.plc file (on page 42)

Control-M/Server co.plc file

[server]
identity=CODN
logfile=cosrv.log

[client]
logfile=cocln.log
identity=CODN
keyfile=$CONTROLM/data/SSL/cert/ctmkey.kdb

Control-M/Server site.plc file

[server]
bindir=<CONTROLM>/exe_<MACHINE>
bindir64=<CONTROLM>/exe_<MACHINE>
keyfile=ctmkey.kdb
security_level=4
logdir=$CONTROLM/data/SSL/log
loglevel=ERROR
securitydir=$CONTROLM/data/SSL/cert
sksdir=$CONTROLM/data/SSL/cert
password=a877b993b0b40c558176b07efc54da43505b61b5d07d9d,<CONTROLM>/data
/SSL/cert/tree.bin
provider_options=SSLProtocol=SSLv3;TLS1;TLS1_2,SSLV3CipherSuite=DES-CBC3-SHA DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC-SHA DES-CBC-SHA

[client]
bindir=<CONTROLM>/exe_<MACHINE>
bindir64=<CONTROLM>/exe_<MACHINE>
keyfile=ctmkey.kdb
Control-M SSL Guide

security_level=4
logdir=$CONTROLM/data/SSL/log
loglevel=ERROR
securitydir=$CONTROLM/data/SSL/cert
skmdir=$CONTROLM/data/SSL/cert
password=a877b993b0b40c558176bbb07efc54da43505b61b5d07d9d,<CONTROLM>/data/SSL/cert/tree.bin
provider_options=SSLProtocol=SSLv3,SSLV3CipherSuite=DES-CBC3-SHA
DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC-SHA DES-CBC-SHA
[keystore]
bindir=<CONTROLM>/exe_<MACHINE>
bindir64=<CONTROLM>/exe_<MACHINE>
keyfile=ctmkey.kdb
security_level=4
logdir=$CONTROLM/data/SSL/log
loglevel=ERROR
securitydir=$CONTROLM/data/SSL/cert
skmdir=$CONTROLM/data/SSL/cert
password=a877b993b0b40c558176bbb07efc54da43505b61b5d07d9d,<CONTROLM>/data/SSL/cert/tree.bin

Control-M/Server ns.plc file
[server]
identity=NSDN
logfile=nssrv.log
security_level=3
[client]
identity=NSDN
logfile=nscln.log
keyfile=$CONTROLM/data/SSL/cert/ctmkey.kdb

Control-M/Enterprise Manager site.plc file
[client]
use_openssl=N
bindir=$EM_HOME/lib
Control-M SSL Guide

bindir64=${EM_HOME}/lib
logdir=${EM_HOME}/site/resource/ssl/log
securitydir=${EM_HOME}/site/resource/ssl/cert
sksdир=${EM_HOME}/site/resource/ssl/cert
provider_options=SSL
Protocol=TLS1_2

Control-M/Enterprise Manager gtw.plc file
[client]
logfile=gtw_ssl.log
identity=CODN
keyfile=${EM_HOME}/site/resource/ssl/cert/gtwkey.kdb
password=a877b993b040c558176bcb07efc54da43505b61b5d07d9d,${EM_HOME}/site/resource/local/tree.bin

Microsoft Windows environment

The security policy is defined by string entries in policy tables in the Windows Registry. The site Policy key is always required. It defines the basic security policy for this component. Modifications, if needed, can be defined by optional component policy keys.

The security policy is determined by the role the application is playing: client or server. Therefore, the policy tables might contain two communications keys, server and client, under site and under each other component entry.

NOTE: BMC does not recommend editing the Windows registry unless you have experience working with the registry and you back up the registry before proceeding.

The Policy Tables are at the following Registry locations:

- **Control-M/Server and Control-M/Agent:** [HKEY_LOCAL_MACHINE\SOFTWARE\BMC\Software\CONTROL-M\{Control-M/Agen|Control-M/Server}\SecurityPolicy\{site|NS|CA|CO|AG|RU}\{client|server|common|keystore]

  You can update the site section in the registry to affect all communications or update a specific hive to control a specific connection. Values that are specified in the other sections override the values specified in the site Registry key, for the relevant SSL connections. Sample Policy Tables for Microsoft Windows are listed under Control-M/Server registry (on page 44).

- **Control-M/EM:** HKEY_LOCAL_MACHINE\SOFTWARE\BMC\Software\CONTROL-M\CONTROL-M/Enterprise Manager\9.0.X\Default\SecurityPolicy\{site|GTW|CMSG\EM}\{client|server|common

  Sample Policy Tables for Microsoft Windows are listed under Control-M/Enterprise Manager registry (on page 46).

  You can update the site section in the registry to affect all communications or update a specific hive to control a specific connection. Values that are specified in the GTW and CMSG sections override the values specified in the site Registry key, for the relevant SSL connections.
NOTE: The EM Registry contains an EM key for internal encryption purposes. Do not change this key.
To set the TLS1.2 SSL Protocol, see Setting the TLS1.2 SSL Protocol (on page 44).

Setting the TLS1.2 SSL Protocol

This procedure describes how to set the TLS1.2 SSL Protocol in the Policy table of Control-M/EM for communication with Control-M/Server (both gateways and CMS).

To set the TLS1.2 SSL Protocol:

1. Navigate to the Policy table in Windows Registry, as described in Microsoft Windows environment (on page 43).
2. Select site > client.
3. Add the following provider_options key in the registry:
   - **Value name:** provider_options
   - **Value data:** SSLProtocol=TLS1_2,[TLSCipherSuite= <desired ciphers list>]

   **EXAMPLE:**
   - **Value name:** provider_options
   - **Value data:** SSLProtocol=TLS1_2,TLSCipherSuite=DHE-RSA-AES256-SHA256

   For the TLSCipher list, see Configuring protocols and ciphers for zones 2 and 3 (on page 16).
4. After updating the configuration, you need to restart the Control-M/EM Configuration Agent, Naming Service, CMS, and relevant gateways.

Sample Microsoft Windows registry keys

These are the following Default Registry key entries for Control-M/Server and Control-M/EM:

- **Control-M/Server registry** (on page 44)
- **Control-M/Enterprise Manager registry** (on page 46)

Control-M/Server registry

The Security Policy for Control-M/Server can be found in the following location:

[\HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M/Server\SecurityPolicy]

[\HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M/Server\SecurityPolicy\client]

- "logfile"="cocln.log"
- "keyfile"="D:\Program Files\BMC Software\CONTROL-M Server\ctm_server\data\ssl\cert\ctmkey.kdb"
- "identity"="CODN"
- [HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\CO\server]
  o "identity"="CODN"
  o "logfile"="cosrv.log"

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\NS]
- [HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\NS\client]
  o "identity"="NSDN"
  o "logfile"="nscln.log"
  o "keyfile"="D:\Program Files\BMC Software\CONTROL-M\Server\ctm_server\data\ssl\cert\ctmkey.kdb"

- [HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\NS\server]
  o "identity"="NSDN"
  o "logfile"="nssrv.log"
  o "security_level"="3"

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\site]
- [HKEY_LOCAL_MACHINE\SOFTWARE\BMC]
  Software\CONTROL-M\Server\SecurityPolicy\site\client]
  o "bindir64"="D:\Program Files\BMC Software\CONTROL-M\Server\ctm_server\exe"
  o "securitydir"="D:\Program Files\BMC Software\CONTROL-M\Server\ctm_server\data\ssl\cert"
  o "logdir"="D:\Program Files\BMC Software\CONTROL-M\Server\ctm_server\data\ssl\log"
  o "loglevel"="ERROR,WARNING,INFO,TRACE"
  o "keyfile"="ctmkey.kdb"
  o "security_level"="4"
  o "provider_options"="SSLProtocol=SSLv3,SSLV3CipherSuite=DES-CBC3-SHA DHE-RSA-AES128-SHA AES128-SHA EDH-RSA-DES-CBC-SHA DES-CBC-SHA"
  o "sksdir"="D:\Program Files\BMC Software\CONTROL-M\Server\ctm_server\data\ssl\cert"
  o "password"="a877b993b0b40c558176bb07efc54da4350b5d07d9d, D:\Program Files\BMC Software\CONTROL-M\Server\CTM_SERVER\DATA\SSL\Cert\tree.bin"
Control-M/Enterprise Manager registry

The Security Policy for Control-M/EM is located here:

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M\Control-M/Enterprise Manager\9.0.X]\Default\SecurityPolicy]

The sections and examples for field valued are specified below:

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M\CONTROL-M/Enterprise Manager\9.0.X]\Default\SecurityPolicy\CMSG]

- [HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M\CONTROL-M/Enterprise Manager\9.0.X]\Default\SecurityPolicy\CMSG\client]
  - "securitydir"="D:\Program Files\BMC Software\CONTROL-M EM\Default\etc\resource\ssl\cert"
  - "loglevel"="ERROR"
  - "logfile"="cmsgssl.log"
  - "keyfile"="D:\Program Files\BMC Software\CONTROL-M EM\Default\etc\resource\ssl\cert\cmsgkey.kdb"
  - "password"="a877b993b0b40c558176bbb07efc54da43505b61b5d07d9d, D:\Program Files\BMC Software\CONTROL-M EM\Default\ini\local\tree.bin"
  - "identity"="CADN"
Control-M SSL Guide

- "security_level"="4"
- "sksdir"="D:\Program Files\BMC Software\CONTROL-M
  EM\Default\etc\resource\ssl\cert"

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M\CONTROL-M/Enterprise
  Manager\9.0.X\Default\SecurityPolicy\GTW]
  - [HKEY_LOCAL_MACHINE\SOFTWARE\BMC
    Software\CONTROL-M\CONTROL-M/Enterprise
    Manager\9.0.X\Default\SecurityPolicy\GTW\client]
    - "sksdir"="D:\Program Files\BMC Software\CONTROL-M
      EM\Default\etc\resource\ssl\cert"
    - "security_level"="4"
    - "identity"="CODN"
    - "password"="a877b993b0b40c558176b0b07efc54da43505b61b5d07d9d,D:\Program
      Files\BMC Software\CONTROL-M
      EM\Default\ini\local\tree.bin"
    - "keyfile"="D:\Program Files\BMC Software\CONTROL-M
      EM\Default\etc\resource\ssl\cert\gtwkey.kdb"
    - "logfile"="gtwssl.log"
    - "loglevel"="ERROR"
    - "securitydir"="D:\Program Files\BMC Software\CONTROL-M
      EM\Default\etc\resource\ssl\cert"

[HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M\CONTROL-M/Enterprise
  Manager\9.0.X\Default\SecurityPolicy\site]
  - [HKEY_LOCAL_MACHINE\SOFTWARE\BMC
    Software\CONTROL-M\CONTROL-M/Enterprise
    Manager\9.0.X\Default\SecurityPolicy\site\client]
    - "bindir64"="D:\Program Files\BMC Software\CONTROL-M
     EM\Default\bin"
    - "logdir"="D:\Program Files\BMC Software\CONTROL-M
     EM\Default\ini\local\log"
    - "provider_options"="SSLProtocol=TLS1_2"
SSL communication parameters

The following describes the SSL-related parameters that determine communication modes for Control-M/Server, Control-M/Agent, and Control-M/EM:

- Control-M/EM (on page 48)
- Control-M/Server (on page 49)
- Control-M/Agent (on page 49)

Control-M/EM

The system parameter CmsCommMode determines if the communication protocol between Control-M/EM and Control-M/Server are TCP or SSL. The following table describes the possible values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>TCP connections are supported between Control-M/EM and Control-M/Server only.</td>
</tr>
<tr>
<td>AUTO</td>
<td>CMS and the gateways attempt to communicate with Control-M/Server using SSL, and on failure, switch to TCP.</td>
</tr>
<tr>
<td>SSL</td>
<td>SSL connections are supported between Control-M/EM and Control-M/Server only.</td>
</tr>
</tbody>
</table>
Control-M/Server

The Secure Sockets Layer system parameter determines the communication mode the Server uses to communicate with Agents and Control-M/EM. You can set this parameter to any of the communication modes shown in the following table.

**Control-M/Server communication modes**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLED</td>
<td>Control-M/Server works in SSL mode. When attempting to connect to an Agent that is in SSL=N mode (discussed subsequently), the Server tries to switch the Agent to SSL=Y mode.</td>
</tr>
<tr>
<td>INACTIVE</td>
<td>Control-M/Server works in non-SSL mode. When attempting to connect to an Agent that is in SSL=Y mode, the Server tries to switch the Agent to SSL=N mode.</td>
</tr>
<tr>
<td>DISABLED</td>
<td>Control-M/Server works in non-SSL mode. When attempting to connect to an Agent that is in SSL=Y mode, the Server does not try to switch the Agent to SSL=N mode.</td>
</tr>
</tbody>
</table>

**NOTE:** Changing the Server communication mode from ENABLED to DISABLED can cause all agents to become unavailable. In that case, you need to change the Server mode to INACTIVE and wait until all required agents are available again. Then, you can change the Server mode to ENABLED or DISABLED.

Control-M/Agent

For Control-M/Agent, the COMMOPT parameter determines the Agent’s communication mode. Valid values for COMMOPT are SSL=Y (communication is enabled) or SSL=N (communication is disabled).

- **Windows:** COMMOPT is under the Control-M/Agent’s CONFIG registry section located at: `\HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M/Agent\CONFIG` for the default installation, or under `\HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\Control-M/Agent\<instance_name>\CONFIG`.
- **UNIX:** COMMOPT is in the `<Agent Home Directory>/ctm/data/CONFIG.dat` file.
- **IBM i (AS/400):** COMMOPT is in the `<Agent Home Directory>/data/CONFIG` file.
Advanced CORBA SSL configuration

The following topics describe how to set up advanced SSL configurations for CORBA:

- Storing new certificates (on page 50)
- ssl_client_server.conf parameters (on page 51)
- Configuring ciphers for CORBA connections (on page 51)
- Updating the private key password (on page 52)
- Updating a private key (on page 52)
- Common SSL error messages (on page 52)
- CORBA::TRANSIENT exceptions (on page 54)
- Certificate expiration (on page 54)
- Key Store files (on page 55)

Storing new certificates

This procedure describes how to store the CA and signed certificates. Default CA and application certificates are provided and stored in standard PEM format.

**NOTE:** Definitions that are defined in the `<Control-M/EM Home Directory>/etc/ssl_ns.conf` file apply on connections between the Naming Service and services registered on it. The definitions in the `<Control-M/EM Home Directory>/etc/ssl_client_server.conf` file apply on connections between the services registered on the Naming Server and themselves.

- To store a Root Certificate of Authority (CA) and signed certificates:
  1. Place the certificates (`ca_cert.pem`, `cert_name.pem`, and `cert_name_priv_key.pem`) in the `<Control-M/EM_directory>/ini/ssl/new_ca` directory.
  2. Update the `ssl_client_server.conf` and `ssl_ns.conf` files in the `<Control-M/EM_directory>/etc>` directory by changing the names of the demonstration certificates to the names of your certificates. Parameters for `ssl_client_server.conf` are described in `ssl_client_server.conf parameters (on page 51).

**EXAMPLE:** If the original content of the `ssl_client_server.conf` file is:

```plaintext
dynamic SSLIOP_Factory Service_Object *
TAO_SSLIOP::make_TAO_SSLIOP_Protocol_Factory() "
-SSLAuthenticate SERVER_AND_CLIENT
-SSLPriateKey 'PEM:/home/ecs1/ctm_em/ini/ssl/CertDemoU_pk.pem'
-SSLCertificate 'PEM:/home/ecs1/ctm_em/ini/ssl/CertDemoU.pem'
-SSLCAfile 'PEM:/home/ecs1/ctm_em/ini/ssl/new_ca.pem'
-SSLrand /home/ecs1/ctm_em/ini/ssl/rnd.bin" static Client_Strategy_Factory "
-ORBConnectStrategy blocked" static Resource_Factory "
-ORBProtocolFactory SSLIOP_Factory"
```

50
Change the full path name of the certificates (bold above) to the names of your certificates. In this example, authentication of both the server and the client is required because the `-SSLAuthenticate` parameter is set to `SERVER_AND_CLIENT`.

**ssl_client_server.conf parameters**

The following table describes parameters in the `ssl_client_server.conf` file.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-SSLAuthenticate</code></td>
<td>Indicates whether authentication is required for server, client, or both. Valid values: SERVER, CLIENT, SERVER_AND_CLIENT</td>
</tr>
<tr>
<td><code>-SSLPrivateKey</code></td>
<td>Points to the location of the private key.</td>
</tr>
<tr>
<td><code>-SSLCertificate</code></td>
<td>Points to the location of the certificate.</td>
</tr>
<tr>
<td><code>-SSLCAfile</code></td>
<td>Points to the CA certificate.</td>
</tr>
<tr>
<td><code>-SSLrand</code></td>
<td>Points to a binary file used to generate random numbers for dynamically encrypting communications between client and server. The file provided by Control-M/EM can be replaced with another binary file. Client and server binary files are independent and do not need to match. Default: <code>&lt;Control-M/EM_directory&gt;/ini/ssl/rand.bin</code></td>
</tr>
<tr>
<td>NOTE: This parameter is optional for Windows installations.</td>
<td></td>
</tr>
<tr>
<td><code>-SSLCipher</code></td>
<td>Defines the list of ciphers that can be used, as described in Configuring ciphers for CORBA connections (on page 51).</td>
</tr>
</tbody>
</table>

**Configuring ciphers for CORBA connections**

This procedure describes how to configure the list of available ciphers for CORBA connections. The default configuration supports all ciphers except export ciphers.

➢ To configure ciphers for CORBA connections:

1. Navigate to the following directory:

   `<EM Home Directory>/etc`  

2. Open the `ssl_ns.conf` and `ssl_client_server.conf` files and edit the `-SSLCipher` option, as described in `ssl_client_server.conf parameters` (on page 51).
You can place single or group of ciphers as values for this option.

3. Use the following syntax between the ciphers and cipher groups:
   - `:` - include
   - `!` - exclude
   - `+` - move to last in the cipher list

**EXAMPLE:** If you set the value of `-SSLCipher` to be `TLSv1.2+RSA:!EXPORT:!NULL`, which includes all TLSv1.2 ciphers, put the RSA ciphers last in the cipher order, and exclude all export ciphers and null ciphers.

### Updating the private key password

This procedure describes how to update the private key password for demonstration certificates. They are stored in the `ClientServerSSL.ini` file in the `<Control-M/EM_directory>/ini/ssl` directory. Control-M/EM components read and decode this password and provide it to the SSL layer.

- To update the private key password for use with your site’s certificates:
  1. Navigate to the `<Control-M/EM_directory>/ini/ssl` directory.
  2. Update the `ClientServerSSL.ini` file with the new encrypted password by entering the command `cryptocli new_password ClientServerSSL.ini`.

### Updating a private key

This procedure describes how to update a private key. The Naming Service requires the private key password interactively during startup. This requirement prevents users from activating the Naming Service in batch mode.

In the Control-M/EM demonstration certificates, the password has been stripped from the private key so that the Naming Service can be invoked without entering the password. The `ssl_ns.conf` configuration file points to the stripped private key file.

- To activate the Naming Service using a new stripped private key:
  1. Use the `<EM Home Directory>/etc/ssl_ns.conf` file for the Naming Service.
  2. Place the stripped private key file in the `<Control-M/EM_directory>/ini/ssl` directory.
  3. Update the `ssl_ns.conf` file with the new private key file name, by updating the SSLPrivateKey value, as described in `ssl_client_server.conf` parameters (on page 51).

### Common SSL error messages

The following are common SSL error messages:

**Message 1**

ACE_SSL (2372 | 1656) error code: 336151576 - error:14094418:SSL routines:SSL3_READ_BYTES:tlsvl alert unknown ca
Failed to register in the CORBA services.
Explanation: The GUI server fails to resolve a secure Naming Service. The **-SSLCAfile** parameter is not specified in the TAO configuration file, or it points to an invalid location.

Corrective Action: Determine which reason caused the failure and correct the problem.

Message 2

**ACE_SSL** (3632|2580) error code: 336134278  - error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed

Failed to register in the CORBA services.

Explanation: The GUI server fails to resolve a secure Naming Service for one of the following reasons:

The **-SSLCAfile** parameter is not specified in the TAO configuration file.

The **-SSLCAfile** parameter points to an invalid location.

The CA PEM file (`new_ca.pem`) is corrupted.

The CA PEM file (`new_ca.pem`) doesn't match the certificates used.

Corrective Action: Determine which reason caused the failure and correct the problem.

Message 3

Failed to register in the CORBA services.

Explanation: An attempt was made to connect to a non-secure Naming Service.

Corrective Action: Ensure that the attempted connection is to a secure Naming Service and ensure that the Naming Service was started as a secure Naming Service.

Message 4

**ClientServerSSL.ini** was not found at D:\ Program Files\ BMC Software\ Control-M EM 7.0.00\ Default\ ini\ ssl
dynamic initialization failed for SSLIOP_Factory (3868|2956) Unable to initialize the Service Configurator: Invalid argument
Failed to register in the CORBA services.

Explanation: The GUI server fails to initialize. The **ClientServerSSL.ini** file was not found in the `<Control-M/EM_directory>/ini/ssl` directory.

Corrective Action: Ensure that the **ClientServerSSL.ini** file is located in the `<Control-M/EM_directory>/ini/ssl` directory.

Message 5

Password decryption error.Key string file may be corrupted.: Unknown error dynamic initialization failed for SSLIOP_Factory (1556|2364) Unable to initialize the Service Configurator: Invalid argument
Failed to register in the CORBA services.

Explanation: The GUI server fails to initialize. The **ClientServerSSL.ini** file is corrupted or contains a password that was encrypted using the wrong key.

Corrective Action: Ensure that the **ClientServerSSL.ini** file is not corrupted and contains a properly encrypted password.

Message 6
dynamic initialization failed for SSLIOP.Factory
(3868|3820) Unable to initialize the Service Configurator: Invalid argument
Failed to register in the CORBA services.

Explanation: The GUI server fails to initialize. The private or public key certificate was not found.

User Response: Ensure that the -SSLPrivateKey parameter points to the file containing the private key. Ensure that the -SSLCertificate parameter points to the file containing the public key. When using the demonstration certificates, the default values are:
-SSLPrivateKey 'PEM:/home/ctm_em/ini/ssl/CertDemoU.pk.pem'
-SSLCertificate'PEM:/home/ctm_em/ini/ssl/CertDemoU.pem'

Message 7
TAO (2196|3224) Service Configurator unable to open file be D:\ Program Files\ BMC Software\ Control-M EM 7.0.00\ Default\ ini\ ssl
(2196|3224) Unable to initialize the Service Configurator: Invalid argument
Failed to register in the CORBA services.

Explanation: The GUI server fails to initialize. The configuration file referenced in the -ORBSvcConf parameter was not found. For more information, see the example in Storing new certificates (on page 50).

Corrective Action: Ensure that the file that is being pointed to exists in the specified location.

CORBA::TRANSIENT exceptions

A CORBA::TRANSIENT exception usually indicates that the client was unable to connect to the server when attempting to invoke a request. For standard IIOP, this normally occurs when the client cannot resolve the hostname embedded in the IOR or cannot reach the specified IP address.

In the case of SSLIOP, a CORBA::TRANSIENT exception may also be thrown when the certificates in use are invalid (for example, expired), or the certificate authority certificate has not been set.

Corrective Action: Verify that all required fields are specified in the files <EM Home Directory>/etc/ssl_client_server.conf and <EM Home Directory>/etc/ssl_ns.conf, and that the specified values are correct, as described in ssl_client_server.conf parameters (on page 51).

Certificate expiration

Control-M/EM comes with demonstration SSL certificates with an expiration period of 4 years. The client applications check certificate expiration on each connection attempt. The client issues a warning if the certificate expires in less than the number of days specified in the WarningSSLExpirationDays system parameter, as described in General parameters. Valid values: 1 - 365. Default: 60.

If an SSL certificate is going to expire in less than the number of days specified in this parameter, a message appears in the Message column of the CCM, and a record is written to the application log.
Key Store files

The following table describes the Key Store files that are used by Control-M.

<table>
<thead>
<tr>
<th>Key Store file</th>
<th>Control-M component</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>KDB key database file</strong></td>
<td>Control-M/Agent 9.0.00.200 and lower</td>
</tr>
<tr>
<td></td>
<td>Control-M/Server 9.0.00.300 and lower</td>
</tr>
<tr>
<td></td>
<td>Control-M/EM servers (Gateway, CMS) 9.0.00.400 and lower</td>
</tr>
<tr>
<td><strong>PEM Privacy enhanced mail</strong></td>
<td>Control-M/EM servers (GSR and BIM server)</td>
</tr>
<tr>
<td></td>
<td>Control-M/EM client</td>
</tr>
<tr>
<td><strong>Java KeyStore</strong></td>
<td>Control-M/Server 9.0.00.300 and lower</td>
</tr>
<tr>
<td></td>
<td>Control-M/EM EMAPI client</td>
</tr>
<tr>
<td></td>
<td>Control-M Web Services and Messaging API</td>
</tr>
<tr>
<td></td>
<td>Control-M/EM BMC Batch Impact Manager</td>
</tr>
<tr>
<td><strong>PKCS#12</strong></td>
<td>Control-M/EM Web Server</td>
</tr>
<tr>
<td></td>
<td>Control-M/EM servers (Gateway, CMS) 9.0.00.500 and higher</td>
</tr>
<tr>
<td></td>
<td>Control-M/Agent 9.0.00.300 and higher</td>
</tr>
<tr>
<td></td>
<td>Control-M/Server 9.0.00.400 and higher</td>
</tr>
<tr>
<td></td>
<td>Control-M for z/OS</td>
</tr>
</tbody>
</table>