

Server Administration and Configuration

This appendix includes the following information on the administration and configuration of CTM GateWay/CORBA:

- [B.1 Creating an OSS Client Profile for CTM GateWay/CORBA, page B-1](#)
- [B.2 Deleting an OSS Client Profile for CTM GateWay/CORBA, page B-2](#)
- [B.3 Viewing Currently Logged In CTM GateWay/CORBA OSS Users, page B-2](#)
- [B.4 Logging Out CTM GateWay/CORBA OSS Users, page B-3](#)
- [B.5 Using Encryption Between the OSS Client and CTM GateWay/CORBA, page B-3](#)
- [B.6 Using Multiple Naming Servers, page B-4](#)
- [B.7 Naming Conventions for Published CTM GateWay/CORBA Objects, page B-4](#)
- [B.8 Location of the Naming Service IOR File, page B-5](#)
- [B.9 Useful Debugging Utilities for Resolving Naming Service-Related Issues, page B-6](#)
- [B.10 Configuring CTM GateWay/CORBA, page B-6](#)
- [B.11 Using the CLI to Start and Stop CTM GateWay/CORBA, page B-8](#)
- [B.12 Configuring Secure Socket Layer for CTM GateWay/CORBA, page B-9](#)
- [B.13 Installation Program, page B-12](#)
- [B.14 CTM R7.0 to CTM R8.0 Migration, page B-12](#)

B.1 Creating an OSS Client Profile for CTM GateWay/CORBA

The CORBA gateway authenticates the OSS against a previously created user profile before allowing access to CTM. You can create up to sixteen OSS client profiles for CTM GateWay/CORBA sessions. Each OSS profile defines CTM GateWay/CORBA parameters, such as the OSS profile name, password, and IP address.

OSS client profiles are stored in the CTM GateWay/CORBA Users table.

-
- Step 1** Log into the CTM client with administrator privileges.
 - Step 2** In the Domain Explorer window, choose **Administration > GW/CORBA Users**.
 - Step 3** Choose **Edit > Add** (or click the **Create a New User** tool).
 - Step 4** Enter the following OSS client information in the **Add GW/CORBA User** window:

- OSS Profile Name—Name of the OSS profile.
 - Password—Password that the OSS client uses to log into the CTM server. Confirm the password in the Confirm Password field.
- Step 5** Click **OK** to confirm the information. Changes take effect immediately. The GW/CORBA Users table gets a refresh event. If automatic refresh is turned on, the new OSS client profile appears as a new row in the table. If automatic refresh is turned off, click the **Refresh Data** tool to see the new OSS client profile in the table.
- Step 6** In the Control Panel window, choose **Administration > GW/CORBA Users**. The GW/CORBA Users wizard displays a profile for each OSS client that uses a CTM GateWay/CORBA service.

B.2 Deleting an OSS Client Profile for CTM GateWay/CORBA

- Step 1** Log into the CTM client with administrator privileges.
- Step 2** In the Domain Explorer window, choose **Administration > GW/CORBA Users**.
- Step 3** The GW/CORBA Users table displays the list of available OSS users. Select the OSS user to delete.
- Step 4** Choose **Edit > Delete** (or click the **Delete a User** tool) to delete the OSS profile from the CTM database.
- Step 5** Click **OK** to confirm the deletion. The OSS client profile name is deleted from the GW/CORBA Users table.



Note

If the OSS is connected to CTM when the profile is being deleted, CTM does not terminate the OSS session.

B.3 Viewing Currently Logged In CTM GateWay/CORBA OSS Users

- Step 1** Log into the CTM client with administrator privileges.
- Step 2** In the Domain Explorer window, choose **Administration > GW/CORBA Users**
- Step 3** The GW/CORBA Users table displays the list of available OSS users. Click the **Show Logged in GW CORBA Users** tool.
- Step 4** In the Active GW/CORBA Users table, a list of currently logged-in users is displayed, including the OSS profile name, IP address to which the user is logged in, and the login time.

B.4 Logging Out CTM GateWay/CORBA OSS Users

-
- Step 1** Log into the CTM client with administrator privileges.
- Step 2** In the Domain Explorer window, choose **Administration > GW/CORBA Users**
- Step 3** The GW/CORBA Users table displays the list of available OSS users. Click the **Show Logged in GW CORBA Users** tool.
- Step 4** In the Active GW/CORBA Users table, a list of currently logged-in users is displayed, including the OSS profile name, IP address to which the user is logged in, and the login time. Select a user (a row from the table) to log off.
- Step 5** Click the **Log Out GW CORBA User** tool.
- Step 6** The user session is cleared from the Active GW/CORBA Users table. You will notice the loss of session during the next ping cycle or when you try to perform an operation on another manager. Some examples of user operations are:
- If the user is connected and performs a query operation on the EMS. The OSS user starts to query the EMS by getting a fresh object reference from the manager through an `emsSession` query. Because the session has been cleared by the CTM GateWay/CORBA service, the OSS user receives an exception and notices the loss of session.
 - The CTM client forcefully logs out the user. The OSS user does not immediately notice the loss of session when the CTM client forces a logout. To immediately log out the user, the CTM GateWay/CORBA service makes a call to the NMS session interface, which forces the OSS client applications to modify their shutdown application. This is not the preferred method.
 - The CTM GateWay/CORBA service clears the user session information from its internal memory and database.
-

B.5 Using Encryption Between the OSS Client and CTM GateWay/CORBA

CTM uses improved encryption of usernames and passwords for network security.

You can set the CTM client Control Panel to send encrypted usernames and passwords to CTM GateWay/CORBA:

-
- Step 1** Log into the CTM client with administrator privileges.
- Step 2** In the Domain Explorer window, choose **Administration > Control Panel**.
- Step 3** Click the **GateWay/CORBA Service** tab for the GateWay/CORBA Service property sheet.
- Step 4** Click the **Global** tab and check the Enable Encryption for Username and Password check box.
- Step 5** Click **Save**; then, click **Yes** in the confirmation dialog box. Changes take effect immediately.
-

If the OSS clients enable the encryption feature, they must provide implementation for RSA-based encryption by retrieving the RSA public key or the public key pair from CTM GateWay/CORBA and by using cryptographic libraries.

- To obtain the RSA public key from CTM, use the `emsSessionFactory::EmsSessionFactory_I::getEmsPublicKey` API. See [3.5.2 `emsSessionFactory::EmsSessionFactory_I::getEmsPublicKey`, page 3-50](#) for details.
- To obtain the RSA public key pair from CTM, use the `emsSessionFactory::EmsSessionFactory_I::getEmsPublicKeyPair` API. See [3.5.3 `emsSessionFactory::EmsSessionFactory_I::getEmsPublicKeyPair`, page 3-51](#) for details.

CTM uses a 512-bit (64-byte) key size and returns the string representation of the RSA public key or public key pair, encoded in the Base64 encoding scheme. OSS clients should use Base64 decoders to decode the public key and get the `byte[]` of the public key from the decoded public key string. The `byte[]` corresponding to the public key represents the key in its primary encoded format (X.509 SubjectPublicKeyInfo). Using this `byte[]` and cryptographic libraries, the RSA public key can be created.

One example of the security provider is Bouncy Castle Provider.

Use the public key to encrypt the username and password. Before passing the encrypted username and password to CTM for login, OSS clients should encode the encrypted username and password by using Base64 encoders to obtain the string equivalent of the encrypted data.


Note

Use cryptographic libraries implementing RSA public key encryption supporting the “PKCS #1 v2.0 EME-PKCS1-v1_5 (PKCS #1 v1.5 block type 2), PKCS1Padding” encoding scheme. CTM does not provide these cryptographic libraries.

B.6 Using Multiple Naming Servers

CTM registers with multiple naming servers. Add the following parameters to the `<CTM_server_installation_directory>/cfg/corbagw.properties` config file:

```
corbagw.namingservice.ServerList=ctmc4-u80,ctm7-u60      (default value is empty)
corbagw.namingservice.RootIORLoc=/namingroot.ior        (default value)
```

The first parameter lists all hosts on which the naming service is running. These hosts should be reachable from the CTM server host. In addition, the Hypertext Transfer Protocol (HTTP) server must be running on all naming service hosts. The naming service root Interoperable Object Reference (IOR) must be published in a file. The location and name of the file are defined by the second parameter. The IOR file must be accessible through the following HTTP call:
`http://<name_server_IP_address>:80/namingroot.ior.`

In addition to these naming service hosts, CTM registers itself with the local naming service. The local naming service port is 14005 and is bundled with CTM.

B.7 Naming Conventions for Published CTM GateWay/CORBA Objects

CTM GateWay/CORBA publishes two top-level objects: `EMSSessionFactory` and `NotificationChannel`. CTM creates these objects and registers them with the CORBA name server.

CTM GateWay/CORBA creates naming contexts under the root as shown in [Figure B-1](#). The last context in the tree must have a different name. To change this value in the CTM client GUI:

-
- Step 1** Log into the CTM client with the appropriate CTM user access profile.
 - Step 2** In the Domain Explorer window, click the **CTM Domain** node.
 - Step 3** In the Management Domain Properties sheet, click the **Identification** tab.
 - Step 4** In the EMS Domain section, look for **EMS ID**. The value of this field should be used as the “id” field for context, where “kind” equals “EMS.” The default value is *CTM*. By using different names, you can install multiple instances of CTM and use a centralized naming server and repository.
-

The following figure shows the naming scheme for CTM GateWay/CORBA objects.

Figure B-1 Naming Scheme for CTM GateWay/CORBA objects



B.8 Location of the Naming Service IOR File

The naming service IOR is located at
`/opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NameService/NameSingleton/NameSingleton.ior.`

B.9 Useful Debugging Utilities for Resolving Naming Service-Related Issues

The following are samples of CTM commands (bundled utility programs) for debugging naming service connectivity issues:

Obtain the list of registered objects in the OpenFusion naming service:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
setenv NS_IOR_LOCATION
file:///opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NameService/NameSingleton/NameSingleton.ior
nsMgrTool -l
```

Decode an IOR file:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
dior -f <IOR file name>, or
dior -i <IOR string>
```

Check if the naming service is running:

```
setenv PATH /opt/CiscoTransportManagerServer/openfusion/bin:$PATH
server -status NameService
```



Note

The `/opt/CiscoTransportManagerServer/openfusion/bin` directory contains `nsMgrTool`, `dior`, and `server` utility tools.

B.10 Configuring CTM GateWay/CORBA

You can configure the following CTM GateWay/CORBA properties in the CTM client Control Panel.

- Step 1** From the Domain Explorer, choose **Administration > Control Panel**.
- Step 2** In the Control Panel, click **GateWay/CORBA Service**. Configure the following properties:



Note If CTM GateWay/CORBA is running, changes to the config file do not take effect dynamically. You must restart CTM GateWay/CORBA for the changes to take effect.

- **Enable Encryption for username and password:**

This property defines whether to encrypt the username and password used for the CTM GateWay/CORBA client.

- **Heartbeat for Notification Channel (min): 0**

This property is the rate at which the notification service is checked. A zero entry means not to check the notification service.

- **Enter the maximum number of simultaneous sessions: 4**

This property is the number of CTM GateWay/CORBA sessions that can be active at the same time. The range is from 4 to 25.

- **Enter the maximum events per consumer: 10000**

CTM GateWay/CORBA uses this property to set the `MaxEventsPerConsumer` administrative QoS parameter of the notification channel. The notification server uses this property to bound the maximum number of events in a given channel that are allowed to queue at any given time. The default value is 0, where the notification server does not impose a limit on the maximum number of events that can be queued. If no limits are imposed on the queue, the notification server might run out of memory if a client behaves incorrectly. The server must keep all events in memory until they are consumed by all registered consumers.

**Caution**

Any change to this value should be made with extreme caution. If you set the value too low, the NMS will not receive all notifications. If you set the value too high, the CTM notification server will run out of memory. The current value is set to handle alarm bursts of 10,000 events per minute.

- **Enter the notification service name: NotificationService**

This property defines the service name that the `resolve_initial_reference` function uses to get a reference to the notification service. The CTM GateWay/CORBA installation installs the notification service automatically. To use your own notification service, modify this parameter.

**Tip**

You do not need to change this parameter if you plan to use the notification service that is bundled with CTM GateWay/CORBA.

- **Enter the notification service naming context: services/NotifyChannelFactory**

`NamingContext` defines the naming context of `NotificationService`. This property is used when `resolve_initial_reference` fails to resolve `NotificationService`. CTM GateWay/CORBA contacts the naming service to resolve the name context defined in this property. The value of this property must match the value published by your notification server.

**Tip**

You do not need to change this parameter if you plan to use the notification service that is bundled with CTM GateWay/CORBA.

- **Enter the notification service factory IOR filename:**

`file:/opt/CiscoTransportManagerServer/openfusion/domains/OpenFusion/localhost/NotificationService/NotificationSingleton/NotificationService.ior`

The `FactoryIORFile` property defines the path to a text file that contains the IOR of `NotificationService`. This property is used only after `resolve_initial_reference` and naming service fail. CTM GateWay/CORBA opens the file as defined by the URL format in this property and attempts to retrieve the IOR from this file. This parameter lets you run your notification service on a different host to improve performance.

**Tip**

You do not need to change this parameter if you plan to use the notification service that is bundled with CTM GateWay/CORBA.

- **Enter the notification service listening port number: 0**

This property is used to set the port that the notification service uses to listen for incoming requests. The port number is set in the IOR for the notification service. The use IOR and use IOR endpoint properties will be set properly. The default port number is zero, which signifies the port number to be allocated by the operating system.

- **Enter the session port number: 0**

This property configures the IIOP listening port. The CTM GateWay/CORBA service listens to CORBA requests on this port. If this property is set to zero, the session port number is allocated by the operating system.

- **Enter the name service server list:**

This property defines where the name servers are running. This property accepts a comma-separated list of hostnames.

- **Enter the name service root IOR:**

This property defines the path used to find the naming service IOR on each host defined in ServerList. The complete path is constructed as `http://<item_of_ServerList><RootIORLoc>`

- **Error level: Minor**

This property defines the error level of messages to log.

This CTM GateWay/CORBA property can be configured by modifying a configuration file in `<CTM_server_installation_directory>/cfg/corbawg.properties`.

- **corbagw.CTP.getLayeredParameters=false**

By default, this property is not enabled. If the NMS requires CTP-related transmission parameters to be included as part of an object reporting TerminationPoint_T structure, this property must be set to true. However, the ManagedElementMgr_I.getTP interface always returns transmission parameters as part of the TerminationPoint_T structure and is independent of this property setting.

B.11 Using the CLI to Start and Stop CTM GateWay/CORBA

CTM can manage the CTM GateWay/CORBA service from the command line:

- To start a CTM GateWay/CORBA service, run the `/opt/CiscoTransportManagerServer/bin/gwcorba-start` script from the command line.
- To stop a CTM GateWay/CORBA service, run the `/opt/CiscoTransportManagerServer/bin/gwcorba-stop` script from the command line.

Only CTM users with administrative privilege can run these scripts. If the CTM GateWay/CORBA service is already running and you attempt to run the `gw-start` script, the script exits with the message “GWCORBA already running.” If the CTM GateWay/CORBA service is stopped and you attempt to run the `gw-stop` script, the script exits with the message “GWCORBA not running.”

You must have a CTM username and password with a SysAdmin or SuperUser profile to start or stop the scripts.

B.12 Configuring Secure Socket Layer for CTM GateWay/CORBA

To ensure network security, CORBA calls can be made over Secure Socket Layer (SSL).

The current JacORB implementation is precompiled with JacORB security libraries. To configure SSL for CTM GateWay/CORBA, you must set up a keystore and configure the properties in the client-side `jacorb.properties` file.

The client must enforce SSL by modifying the `jacorb.properties` file. The server-side keystore is generated using the JSSE keystore. CTM bundles a default keystore and a certificate for the CTM GateWay/CORBA service.

As explained in the following sections, you must generate the server-side certificate and add it to the client-side keystore; then generate and add the client-side certificate to the server-side keystore.

B.12.1 Generating the Server-Side Certificate

Step 1 Use the `keytool` command to generate a keystore and a key:

```
keytool -genkey -alias gwcorba_service -validity 25000 -keystore gwcorba_service_ks
-storepass gwcorba_service_ks_pass -keypass gwcorba_service_ks_pass
```

What is your first and last name?

[Unknown]: **gateway corba server**

What is the name of your organizational unit?

[Unknown]:

What is the name of your organization?

[Unknown]: **cisco**

What is the name of your City or Locality?

[Unknown]:

What is the name of your State or Province?

[Unknown]:

What is the two-letter country code for this unit?

[Unknown]:

Is <CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown> correct?

[no]: **y**

Step 2 Verify that the generated keystore and key have the following attributes:

```
Keystore name: gwcorba_service_ks
Alias: gwcorba_service
Keystore password: gwcorba_service_ks_pass
Key password: gwcorba_service_ks_pass
Validity: 25000 days
```

Step 3 Enter the following command to generate a server-side certificate that will be issued to the client:

```
keytool -export -keystore gwcorba_service_ks -alias gwcorba_service -storepass
gwcorba_service_ks_pass -file gwcorba_service_cert
```

Certificate stored in file <gwcorba_service_cert>

Step 4 Verify that the certificate is stored in the `gwcorba_service_cert` file. The server-side certificate and keystore are present in the `/opt/CiscoTransportManagerServer/cfg` directory.

B.12.2 Generating the Client-Side Certificate

Note the following conventions:

- `ascii_client_ks`—Denotes client-side keystore.
- `ascii_client_cert`—Denotes client-side certificate.
- `gworba_service_ks`—Denotes server-side keystore.
- `gworba_service_cert`—Denotes server-side certificate.

Step 1 Use the `keytool` command to generate a keystore:

```
keytool -genkey -alias ascii_client -validity 25000 -keystore ascii_client_ks -storepass
ascii_client_ks_pass -keypass ascii_client_ks_pass
```

What is your first and last name?

[Unknown]: **ascii client**

What is the name of your organizational unit?

[Unknown]:

What is the name of your organization?

[Unknown]: **cisco**

What is the name of your City or Locality?

[Unknown]:

What is the name of your State or Province?

[Unknown]:

What is the two-letter country code for this unit?

[Unknown]:

Is CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown correct?

[no]: **y**

Step 2 Verify that the generated keystore and key have the following attributes:

```
Keystore name: ascii_client_ks
Alias: ascii_client
Keystore password: ascii_client_ks_pass
Key password: ascii_client_ks_pass
Validity: 25000 days
```

Step 3 Enter the following command to generate a client-side certificate that will be issued to the server:

```
keytool -export -keystore ascii_client_ks -alias ascii_client -storepass
ascii_client_ks_pass -file ascii_client_cert
```

Certificate stored in file <ascii_client_cert>

Step 4 Verify that the certificate is stored in the `gworba_service_cert` file.

B.12.3 Adding the Client Certificate to the Server-Side Keystore

Step 1 Enter the following command to add the client-side certificate to the server-side keystore. (Use FTP or a similar tool to deliver the `ascii_client_cert` file to the server. The server-side keystore is located in the `/opt/CiscoTransportManagerServer/cfg` directory on the server.)

```
keytool -import -keystore gworba_service_ks -alias ascii_client -storepass
gworba_service_ks_pass -file ascii_client_cert
```

The command output resembles the following example:

```
Owner: CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Issuer: CN=ascii client, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Serial number: 441bf39c
Valid from: Sat Mar 18 17:18:44 GMT+05:30 2006 until: Fri Jul 23 10:50:28 GMT+05:30 2038
Certificate fingerprints:
    MD5: 42:53:98:7C:BA:CB:28:39:50:50:9F:E4:56:F2:43:FF
    SHA1: F5:1D:B9:BB:1D:66:C2:A1:32:BE:47:0C:85:47:17:16:A2:69:17:4C
Trust this certificate? [no]: y
Certificate was added to keystore
```

Step 2 Verify that the certificate issued by the client was added to the server keystore.

B.12.4 Adding the Server Certificate to the Client-Side Keystore

Step 1 Enter the following command to add the server-side certificate to the client-side keystore. (Use FTP or a similar tool to deliver the previously generated gwcorba_service_cert file from the server. The server-side certificate is located in the /opt/CiscoTransportManagerServer/cfg directory on the server.)

```
keytool -import -keystore ascii_client_ks -alias gwcorba_service -storepass
ascii_client_ks_pass -file gwcorba_service_cert
```

The command output resembles the following example:

```
Owner: CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Issuer: CN=gateway corba server, OU=Unknown, O=cisco, L=Unknown, ST=Unknown, C=Unknown
Serial number: 441bf43c
Valid from: Sat Mar 18 17:21:24 GMT+05:30 2006 until: Fri Jul 23 10:53:08 GMT+05:30 2038
Certificate fingerprints:
    MD5: 5C:41:39:AD:D0:F8:63:5D:81:8D:47:A0:33:02:8E:7D
    SHA1: 38:CD:C8:57:F7:15:22:DC:1A:6E:99:CD:13:A1:9A:67:90:2C:65:C2
Trust this certificate? [no]: y
Certificate was added to keystore
```

Step 2 Verify that the certificate issued by the server was added to the client keystore.

B.12.5 Configuring the Client-Side Properties

To enforce SSL, complete the following configuration on the client-side jacorb.properties file.



Note

- To enforce SSL, the supported and required options must be set to 60.
- No changes are required to the server-side jacorb.properties file, because it has already been changed.

```
jacorb.security.support_ssl=on

# IIOP/SSL parameters (numbers are decimal values):
# EstablishTrustInClient = 40
# EstablishTrustInTarget = 20
# mutual authentication = 60
```

```
jacorb.security.ssl.client.supported_options=60
jacorb.security.ssl.client.required_options=60

jacorb.ssl.socket_factory=org.jacorb.security.ssl.sun_jsse.SSLSocketFactory

jacorb.security.keystore_password= ascii_client_ks_pass
jacorb.security.keystore= ascii_client_ks

# Read trusted certificates from the keystore
jacorb.security.jsse.trustees_from_ks=on
```

B.13 Installation Program

The CTM installation program installs the CTM GateWay/CORBA component, which includes OpenFusion 3.0.2 Notification Service from Prism Technologies, Inc.

IDL files are installed under the /opt/CiscoTransportManagerServer/idl directory. See the [Cisco Transport Manager Release 8.0 Installation Guide](#) for more information.

B.14 CTM R7.0 to CTM R8.0 Migration

No migration is needed from CTM R7.0 to CTM R8.0 for CTM GateWay/CORBA.