Hewlett Packard Enterprise

HPE Operations Manager i

Software Version: 10.11

OMi FIPS Configuration Guide

Document Release Date: 25 May 2016
Software Release Date: May 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD, the AMD Arrow symbol and ATI are trademarks of Advanced Micro Devices, Inc.

Citrix® and XenDesktop® are registered trademarks of Citrix Systems, Inc. and/or one more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPad® and iPhone® are trademarks of Apple Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft®, Windows®, Lync®, Windows NT®, Windows® XP, Windows Vista® and Windows Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NVIDIA® is a trademark and/or registered trademark of NVIDIA Corporation in the U.S. and other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Red Hat® is a registered trademark of Red Hat, Inc. in the United States and other countries.

SAP® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/manuals.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support website at: https://softwaresupport.hpe.com

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to https://softwaresupport.hpe.com and click **Register**.

To find more information about access levels, go to: https://softwaresupport.hpe.com/access-levels

HPE Software Solutions & Integrations and Best Practices

Visit HPE Software Solutions Now at https://softwaresupport.hpe.com/km/KM01663677 to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Contents

Overview

This document provides information on how to configure OMi to be compliant with Federal Information Processing Standards (FIPS) 140-2.

FIPS 140-2 is a standard for security requirements for cryptographic modules defined by the National Institute of Standards and Technology (NIST). To view the publication for this standard, go to:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Caution: FIPS mode cannot be reverted. After OMi is configured to run in FIPS mode, it cannot be reconfigured to run in standard, non-FIPS mode. To run OMi in non-FIPS mode, you must reinstall the application and configure it as described in the *OMi Installation and Upgrade Guide*.

This section includes:

OMi in FIPS Mode

When you configure OMi to run in FIPS mode, the following components are also configured to operate in FIPS mode:

- Embedded Apache web server
- HPE Operations Agent installed on the OMi servers
- Java Runtime Environment

OMi automatically uses FIPS-compliant cryptographic methods for the following:

- HTTPS communication (if configured) between clients and the OMi web server or load balancer
- HTTPS communication (if configured) between RTSM clients and RTSM
- HTTPS communication between HPE Operations Agents or Operations Connectors (OpsCx) and OMi (HTTPS required by default)
- LDAPS communication between OMi and LDAP server
- Java keystore and Java Runtime Environment
- Policy signing

Considerations When Running OMi in FIPS Mode

Before configuring OMi to run in FIPS mode, consider the following points:

- **Installation and Configuration:**
  - FIPS mode can be configured at installation time only. It is not possible to upgrade an existing OMi installation to OMi in FIPS mode.
  - FIPS mode cannot be reverted. You must reinstall OMi to switch to non-FIPS mode.
  - Express configuration in FIPS mode is not supported.
  - The Microsoft IIS web server is not supported.
- **Integrations:**

  Typically, FIPS is not enabled for only a single application. Instead, all integrated systems must be FIPS-compliant for the entire deployment to be FIPS-compliant. For OMi, this means that all clients, connected databases, data providers, and integrations must be configured for FIPS compliance.

  For client requirements, see "Client Requirements" on page 7. For information on how to configure the database to be FIPS-compliant, see database vendor documentation.
- **Encryption:**
  - Encryption with a key length of less than 2048 bits is not supported.
  - FIPS mode does not enforce encryption. However, when encryption is used, only approved algorithms are allowed. OMi automatically uses FIPS-compliant cryptographic methods when HTTPS communication is enabled.
  - Configuration exchange using content packs is not supported between OMi servers running in FIPS mode and OMi servers running in non-FIPS mode if the artifacts contain passwords.
- **Database:**

  Automatic import of the certificate for TLS communication with the database does not work. The certificate must be imported manually.

  The **BBCTrustServer** command-line interface and the **Retrieve from server** link in the Outgoing Connection properties of a connected server do not work in FIPS mode. The certificate must be exported on the integrating server and manually imported to the OMi server. For details, see "Establish Trust Between OMi and OM Deployments" on page 20.
- **Miscellaneous:**
  - Authentication using the Security Assertion Markup Language 2.0 (SAML2) protocol is not supported.
  - Secure email notifications are not supported.

Requirements

This section includes:

Server Requirements

In addition to the hardware and software requirements listed in the *OMi Installation and Upgrade Guide*, make sure the systems on which you plan to run OMi in FIPS mode meet the following requirements:

- OMi 10.11 or later is installed.
- FIPS mode is enabled in the operating system of the OMi server.

For up-to-date information about supported components and versions, see Support Matrices for Operations Center products.

Database Requirements

When configuring OMi in FIPS mode, you must use either the Microsoft SQL Server or Oracle database.

Certificate Requirements

In FIPS mode, certificates must have a key length of at least 2048 bits.

When using HTTPS communication between OMi and the database, the database certificate cannot be imported automatically by the configuration wizard. You must import the certificate manually.

The **BBCTrustServer** command-line interface and the **Retrieve from server** link in the Outgoing Connection properties of a connected server do not work when OMi runs in FIPS mode. The certificate must be exported on the integrating server and manually imported to the OMi server. For details, see "Establish Trust Between OMi and OM Deployments" on page 20.

Client Requirements

In addition to the client requirements listed in the *OMi Installation and Upgrade Guide*, make sure you do the following:

Configure the Browser for FIPS Mode

Configure the browser that you want to use to access OMi running in FIPS mode as follows:

Internet Explorer users must enable the use of TLS 1.2 or later (**Internet Options > Advanced > Security**).

Configure the JRE for FIPS Mode

To be able to access OMi UIs that use Java applets or to access the Java UI of the RTSM, you must place the required libraries in the JRE directory of your client system:

1. Copy the Crypto-J libraries into the JRE directory of your client system:

   Copy from:

   `<OMi_HOME>/odb/lib/cryptojce-6.2.jar`

   `<OMi_HOME>/odb/lib/cryptojcommon-6.2.jar`

   `<OMi_HOME>/odb/lib/jcmFIPS-6.2.jar`

   Copy to:

   `<jre_dir_path>/lib/ext/`
2. Download the JCE Unlimited Strength Jurisdiction Policy libraries from the Oracle Java website:

   http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html

   Copy the downloaded JCE Unlimited Strength Jurisdiction Policy libraries to the Java security directory on your client system:

   `<jre_dir_path>/lib/security`
3. The `java.security` file should contain the JsafeJCE provider as a standard cryptography provider in the providers list. In addition for TLS communication we also configure the SunJSSE TLS provider in FIPS mode. This is done by performing the change to the security provider from the fifth position. SunJSSE is configured in FIPS mode by associating it with an appropriate FIPS 140 certified cryptographic provider (JsafeJCE) that supplies the implementations for all cryptographic algorithms required by SunJSSE.

   Edit the file `<jre_dir_path>/lib/security/java.security`.

   Insert the following lines right before the list of providers:

   ```
   com.rsa.cryptoj.fips140initialmode=FIPS140_SSL_MODE
   com.rsa.cryptoj.kat.strategy=on.load
   ```

   Edit the cryptographic provider list so that it includes the FIPS 140-2 certified cryptographic provider (JsafeJCE):

   ```
   security.provider.1=sun.security.provider.Sun
   security.provider.2=com.rsa.jsafe.provider.JsafeJCE
   security.provider.3=sun.security.rsa.SunRsaSign
   security.provider.4=sun.security.ec.SunEC
   security.provider.5=com.sun.net.ssl.internal.ssl.Provider JsafeJCE
   security.provider.6=com.sun.crypto.provider.SunJCE
   ```

```
security.provider.7=sun.security.jgss.SunProvider
security.provider.8=com.sun.security.sasl.Provider
security.provider.9=org.jcp.xml.dsig.internal.dom.XMLDSigRI
security.provider.10=sun.security.smartcardio.SunPCSC
security.provider.11=sun.security.mscapi.SunMSCAPI
```

4. Create the FIPS-compliant client truststore:
   a. Create the `jssecacerts` trusted certificates store of type PKCS12 using the JsafeJCE provider:

      In FIPS mode the client JRE will use a different trusted certificate store, which is of type PKCS12, created using the JsafeJCE provider. The new `jssecacerts` file is generated by converting the client JRE cacerts file from JKS to PKCS12 and by copying all the trusted certificates from `cacerts` inside `jssecacerts`. In the *<OMi_HOME>*`\odb\tools\security` folder, a new java tool `jks2pkcs12.jar` is added for performing this conversion. The keystore converter tool is getting two parameters, the keystore to be converted of type JKS (`cacerts`) and the newly generated keystore of type PKCS12 (`jssecacerts`).

      In this guide, the `cacerts` file from the client JRE machine (for example, `C:\Program Files (x86)\Java\jre1.8.0_45\lib\security\cacerts`) is copied to a folder on the UCMDB server machine. Next, run the following command to perform the needed conversion.

      Create `jssecacerts` by converting the client JRE `cacerts` file:

      <OMi_HOME>`\JRE\bin\java -Djava.security.properties=`*<OMi_HOME>*`\JRE\lib\security\java.security.FIPS -jar `*<OMi_HOME>*`\odb\tools\security\jks2pkcs12.jar `*<input_folder>*`\cacerts `*<output_folder>*`\jssecacerts`

      When prompted for the keystore password, you should use the password `changeit` because this is the default password for the `cacerts` file.

   b. Export the `hproot` server root certificate by running the following command from *<OMi_HOME>*`\JRE\bin`:

      <OMi_HOME>`\JRE\bin\keytool -exportcert -alias hproot -keystore `*<OMi_HOME>*`\odb\conf\security\hproot.keystore -storetype pkcs12 -providername JsafeJCE -providerclass com.rsa.jsafe.provider.JsafeJCE -file `*<output_folder>*`\hproot.crt`

      When prompted for the keystore `hproot.keystore` password, use `hppass`.

   c. Import the `hproot` server root certificate, which you created in the previous step, into the client `jssecacerts` keystore as a trusted certificate:

      Import `hproot` into client truststore (`jssecacerts`):

      <OMi_HOME>`\JRE\bin\keytool -import -trustcacerts -keystore `*<path_to_jssecacerts>* `-storetype pkcs12 -providername JsafeJCE -providerclass com.rsa.jsafe.provider.JsafeJCE -storepass changeit -alias hproot -file `*<path_to_hproot.crt>*

      If you are prompted whether to trust this certificate, answer `yes`.

   d. Import the web server root CA certificate from `ca_root.cer` into the client `jssecacerts` keystore as a trusted certificate:

Import `ca_root.cer` into client truststore (`jssecacerts`):

```
<OMi_HOME>\JRE\bin\keytool -import -trustcacerts -keystore <path_to_
jssecacerts> -storetype pkcs12 -providername JsafeJCE -providerclass
com.rsa.jsafe.provider.JsafeJCE -storepass changeit -file <OMi_
HOME>\WebServer\conf\ca_root.cer
```

If you are prompted whether to trust this certificate, answer `yes`.

e. Copy the newly generated `jssecacerts` file from the server machine to the client JRE, inside the `lib\security` folder (for example, `C:\Program Files (x86)\Java\jre1.8.0_45\lib\security`).

f. Configure the JRE on the client machine to use the new `jssecacerts` file. To do this, choose one of the following methods:

- Update the values of the `JAVA_TOOL_OPTIONS` environment variable to the correct path of the `jssecacerts` file:

```
-Djavax.net.ssl.trustStoreType=PKCS12
-Djavax.net.ssl.trustStoreProvider=JsafeJCE
-Djavax.net.ssl.trustStorePassword=changeit
-Djavax.net.ssl.keyStorePassword=changeit
-Djavax.net.ssl.keyStoreType=PKCS12
-Djavax.net.ssl.keyStoreProvider=JsafeJCE
```

- Add these values as runtime parameters by using the Java Control Panel (the `javacpl` tool).

Note: All the Java applications executed on the client machine may be affected by the changes made in this step.

5. Restart your web browser.

Configure OMi for FIPS 140-2 Compliance

This section includes:

Install and Configure OMi

You can install and configure OMi in a distributed environment in any of the following ways:

- **Parallel installation, serial configuration.** You can run the OMi installation on all servers in parallel. The configuration wizard, however, must be run on the data processing server first. After you configure OMi on the first data processing server, continue by configuring it on the other data processing servers, and then on the gateway servers.
- **Serial installation and configuration.** You can run the OMi installation and configuration on each server successively. In this case, install and configure OMi on the data processing server first. After you install and configure OMi on the first data processing server, continue by installing and configuring OMi on the other data processing servers, and then on the gateway servers. The wizard will direct you as to when to begin the installation on the gateway server.

Caution: When the OMi post-installation wizard offers you the option to start the configuration wizard automatically, click **Quit**. To configure OMi in FIPS mode, you **must start the configuration wizard manually**. For details, see "Configure OMi in FIPS Mode" below.

When installing OMi, make sure to do it in the following order:

1. Install OMi 10.10.
2. Install OMi 10.11 on top of OMi 10.10.

For detailed information on how to install OMi, see the *OMi Installation and Upgrade Guide*.

Configure OMi in FIPS Mode

To configure OMi in FIPS mode, follow these steps:

1. Start the configuration wizard manually:
   - Windows: `<OMi_HOME>\bin\config-server-wizard.bat -FIPS`
   - Linux: `/opt/HP/BSM/bin/config-server-wizard.sh -FIPS`
2. In the FIPS Configuration dialog box, click **Yes** to confirm that you want to configure OMi to run in FIPS mode.

Caution: FIPS mode cannot be reverted. After OMi is configured to run in FIPS mode, it cannot be reconfigured to run in standard, non-FIPS mode. To run OMi in non-FIPS mode, you must reinstall the application and configure it as described in the *OMi Installation and Upgrade Guide*.

3. In the Configuration Options page, click **Custom configuration**, and then click **Next**.

   Tip: To configure OMi in silent mode based on a configuration file, click **Create configuration file for silent configuration** and continue with the wizard. After the configuration wizard completes, OMi generates the configuration file at the location you specified. The file contains the values that you selected in the configuration wizard. To start the silent configuration, type:

   - Windows: `<OMi_HOME>\bin\silentConfigureBSM.bat <ConfigurationFile>.xml -FIPS`
   - Linux: `/opt/HP/BSM/bin/silentConfigureBSM.sh <ConfigurationFile>.xml -FIPS`

4. In the Database Settings page, select the database you want to use with OMi. You can choose to connect to an already existing, preconfigured database or user schema (this applies to the database that is originally created with a system in FIPS mode), or let the configuration wizard create a new database or user schema.

   Click **Next** to continue.

5. In the TLS Setup page, **Enable HTTPS** is selected by default to configure OMi to accept only secure connections to its web server and JMX console.

   If your company uses a Certificate Authority (CA) that can generate certificates for OMi, click the **Upload certificates** option. Alternatively, click **OMi-generated certificates** if you want OMi to generate the certificates required for the configuration.

   Click **Next** to continue.

6. In the Certificate Upload page, specify the certificates you received from the CA used by your company.

   Caution: The minimum key length for certificates is 2048 bits.

   If you let OMi generate the required certificates, you can optionally customize the key options and contents of the certificates generated by the OMi CA. You can define certificate settings for the OMi root CA and for the OMi server for which the certificate is issued.

   Click **Next** to continue.

7. *Optional.* In the Client Certificate Authentication page, configure OMi to require a client certificate when users log in to OMi or when web services connect to OMi.

   Depending on the deployment, you can configure OMi to authenticate the client on the OMi web server or, if available, the load balancer.

   Caution: Do not enable client certificate authentication if you are configuring OMi for the first time. Before enabling client certificate authentication, OMi must be already configured and a superadmin user must exist. For more information, see the *OMi Administration Guide*.

   Click **Next** to continue.

8. In the Connection Settings page, **Apache HTTP Server** is selected by default.

   OMi automatically configures the embedded Apache web server for FIPS. In FIPS mode, Apache requires TLS 1.2 or later.

Note: If you have a load balancer in the environment, enter the FQDN and port of the load balancer in the **URL** field.

Click **Next** to continue.

9. In the License page, configure the license that OMi uses, and then click **Next**.
10. In the Login Settings page, set the passwords of the OMi users.

    OMi supports central user management and corporate password policies, it can communicate with the directory services by using LDAP. HPE recommends such configuration to enforce compliance of OMi user passwords with the respective security policy in your company. To configure the LDAP integration, navigate to **Administration > Users > Authentication Management** in the OMi user interface.

    LDAP authentication of all users is possible only when the mixed mode authentication is disabled in the OMi LDAP infrastructure settings. For instructions on how to adjust this setting, see the *OMi Administration Guide*.

    Click **Next** to continue.
11. In the Server Deployment page, you can enable User Engagement and define the size of your OMi deployment.

    Click **Next** to continue.
12. In the Management Packs page, select the management packs to install in your OMi deployment. Dependencies between management packs are resolved automatically.

    Click **Next** to continue.
13. In the Confirmation page, verify your selections, and then click **Next** to start the configuration in FIPS mode.
14. After OMi is successfully configured, a summary of the configuration changes appears. Click **Finish** to conclude the configuration.

Post-Configuration Steps

1. On each OMi server in the deployment, increase the TLS handshake timeout:
   a. Run the following command to edit the server configuration:

      ```
      ovconfchg -edit
      ```

   b. Add the following lines at the end of the file:

      ```
      [bbc.http]
      SSL_HANDSHAKE_TIMEOUT=60000
      ```

2. Start the OMi server processes:

   Note: *Distributed environments only.* Before starting OMi server processes on the data processing server, make sure that OMi is installed and configured on at least one gateway server.

   - Windows 2008: Select **Start > Programs > HPE Operations Manager i > Administration > Enable Operations Manager i**.
   - Windows 2012: Press **Ctrl** + **Esc** and start typing **Enable HPE Operations Manager i**. Then click **Enable Operations Manager i** in the search results.
   - Linux: `/opt/HP/BSM/scripts/run_hpbsm start`

Log in to OMi

To log in to OMi, follow these steps:

1. Make sure the computer and browser that you want to use to access OMi meet the requirements listed in "Client Requirements" on page 7.
2. In the browser, enter the following URL:

   `https://<server_name>.<domain_name>/omi`

   In this instance, *<server_name>* and *<domain_name>* represent the Fully Qualified Domain Name (FQDN) of the OMi server (for example, `https://server.example.com/omi`). If there are multiple servers, or if OMi is deployed in a distributed architecture, specify the load balancer or gateway server URL, as required.

For more information on logging in to OMi, see the *OMi User Guide*.

Configure Operations Agent for FIPS 140-2 Compliance

This section provides a brief description of how to install Operations Agent in FIPS mode and how to enable FIPS mode for an already installed agent. For more detailed information on Operations Agent in FIPS mode, see the *Operations Agent User Guide*.

This section includes:

Requirements

Before installing Operations Agent for FIPS mode, make sure the following requirements are met:

- OMi server is running in FIPS mode.
- Operations Agent 12.00 or later for running Operations Agent in FIPS mode.
- Operations Agent12.01 or 12.00 with hoftix QCCR1A184109 to install Operations Agent in FIPS mode.

Install Operations Agent

This section includes:

Install Operations Agent in FIPS mode

To install Operations Agent in FIPS mode, follow these steps:

1. Create a profile file manually on the node.
2. Add the following line to the file:

   ```
   set nonXPL.config:FIPS_MODE=true
   ```

   If JRE is installed on the agent system, also add the following line:

   ```
   set nonXPL.config:FIPS_JAVAHOME=<jre_dir_path>
   ```

   Replace `<jre_dir_path>` with the location of the JRE on the node, for example `"C:\Program Files (x86)\Java\jre1.8.0_66"`. The agent installation automatically sets the `FIPS_JAVAHOME` variable if the HPE Software ovJREb shared component is installed.
3. Install Operations Agent by using the profile file.

Example:

```
cscript oainstall.vbs -i -a -agent_profile <path>\<profile_file> -s <management_server> [-cs <certificate_server>]
```

Depending on your OMi deployment, specify the gateway server, load balancer, or reverse proxy as the agent's management server, and the data processing server as certificate server.

For detailed information on how to install Operations Agent by using the profile file, see the *Operations Agent and Operations Smart Plug-ins for Infrastructure Installation Guide*.

4. In the OMi user interface, open the Certificate Requests manager and accept the new certificate request:

   Administration > Setup and Maintenance > Certificate Requests

   For more information on granting certificate requests in OMi, see the *OMi Administration Guide*.

5. *Optional.* Check that the agent is running in FIPS mode:

   ```
   ovbbccb –status
   ```

   If the output includes `FIPS mode: ON`, the agent is running in FIPS mode.

Switch Operations Agent to FIPS mode

You can switch an already installed Operations Agent to FIPS mode by running FIPS_tool locally on the agent system. If there are already policy templates installed on the node, you must redeploy the configuration from OMi.

To switch an already installed Operations Agent to FIPS mode, follow these steps:

1. Run the FIPS_tool CLI on the Operations Agent system:
   a. Navigate to the following location:
      - Windows: `%OvInstallDir%\lbin\secco\FIPS_tool`

        `%OvInstallDir%` default: `C:\Program Files\HP\HP BTO Software\`
      - HP-UX, Linux, and Solaris: `/opt/OV/lbin/secco/FIPS_tool`
      - AIX: `/usr/lpp/OV/lbin/secco/FIPS_tool`
   b. Run the following command:

      ```
      perl FIPS_tool -enable_FIPS [-Java_Home <jre_dir_path>]
      ```

      Alternatively, use an already installed Java on your system, and set `-Java_Home` with the location of the JRE on the system.

      Example:

      ```
      "C:\Program Files\HP\HP BTO Software\nonOV\perl\a\bin\perl.exe" FIPS_tool -enable_FIPS -Java_Home "C:\Program Files (x86)\Java\jre1.8.0_66"
      ```

      Note: The FIPS_tool CLI automatically sets the `-Java_Home` option if the HPE Software OvJREB shared component is installed on the node.

      Note: Make sure to run the FIPS_tool CLI under the same user as the agent processes.

   For more information on the FIPS_tool CLI, run `FIPS_tool -help`.

2. *Optional.* Check that the agent is running in FIPS mode:

   ```
   ovbbccb -status
   ```

   If the output includes `FIPS mode: ON`, the agent is running in FIPS mode.
3. If the agent was previously not connected to an OMi sever running in FIPS mode, connect the agent to it and reassign the configuration to the monitored node.
4. Redeploy the assignments to the node.

Configure the Data Flow Probe for FIPS 140-2 Compliance

This section includes:

Requirements

Before you start configuring the Data Flow Probe for FIPS mode, make sure the following requirements are met:

- OMi server is running in FIPS mode.
- Data Flow Probe has the same version as the RTSM on the OMi server.

Configure the Data Flow Probe for FIPS Mode

Note: Data Flow Probes that are upgraded to version 10.21 are switched to FIPS mode automatically.

To configure the Data Flow Probe for FIPS mode, follow these steps:

1. Install the Data Flow Probe as described in the *OMi Data Flow Probe Installation Guide*.
2. Switch the probe to FIPS mode:
   - If the OMi/RTSM server is running in FIPS mode with *HTTP* enabled, the Data Flow Probe is switched automatically to FIPS mode when you connect it to OMi, and you do not have to perform any additional steps.
   - If the OMi/RTSM server is running in FIPS mode with *HTTPS* enabled (the default), follow these steps:
     i. Stop the probe.
     ii. Open the following file in a text editor:

     `<DFP install folder>/conf/security/ssl.properties`

     iii. Locate the following attributes, and update their values as follows:

     ```
     javax.net.ssl.keyStore=FIPS_HPProbeKeyStore.jks
     javax.net.ssl.trustStore=FIPS_HPProbeTrustStore.jks
     ```

     iv. Restart the probe.
3. *Optional.* Verify that the probe is switched to FIPS mode:

a. Go to the probe's JMX Console.

   For example: `<Probe_IP>:<Probe_Port>/jmx-console/`

b. Search for `getFipsStatus`.

c. On the result page, check whether the value of the `FipsStatus` attribute is `Current probe is in FIPS mode`.

Establish Trust Between OMi and OM Deployments

For connection and communication between OMi and OM hosts or other OMi hosts, you must establish a trust relationship between the systems. In FIPS mode, the trusted certificates must be exchanged manually. To do so, follow these steps:

1. On the OMi data processing server, execute the following command:

   ```
   ovcert -exporttrusted -file <omi.cer>
   ```
2. On the external system (OM or other OMi deployment), execute the following command:

   ```
   ovcert -exporttrusted -file <other.cer>
   ```
3. Copy *<other.cer>* from the external system to the OMi data processing server.
4. Copy *<omi.cer>* from the OMi data processing server to the external system.
5. On the OMi data processing server, execute the following commands:

   ```
   ovcert -importtrusted -file <other.cer>
   ovcert -importtrusted -file <other.cer> -ovrg server
   ```
6. On the external system, execute the following commands:

   ```
   ovcert -importtrusted -file <omi.cer>
   ovcert -importtrusted -file <omi.cer> -ovrg server
   ```

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on OMi FIPS Configuration Guide (Operations Manager i 10.11)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to ovdoc-asm@hpe.com.

We appreciate your feedback!

Go OMi!