HP Operations Manager

Common Access Card Authentication

Software Version: 9.11

for the UNIX and Linux operating systems

Manufacturing Part Number: None

November, 2013

Legal Notices

Warranty.

The only warranties for HP 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. HP 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 HP 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 Notices.

Trademark Notices.

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

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

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

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

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

UNIX® is a registered trademark of The Open Group.

Conventions

The following typographical conventions are used in this manual:

Table 1 **Typographical Conventions**

Font	Meaning	Example
Italic	Book titles and manual page names	For more information, see the *HPOM Administrator's Reference* and the *opc(1m)* manual page.
	Emphasis	You *must* follow these steps.
	Variable that you must supply when entering a command (in angle brackets)	At the prompt, enter **`rlogin`** ***`<username>`***.
	Parameters to a function	The *`oper_name`* parameter returns an integer response.
`Computer`	Text and other items on the computer screen	The following system message displays: `Are you sure you want to remove current group?`
	Command names	Use the `grep` command...
	Function names	Use the `opc_connect()` function to connect...
	File and directory names	Edit the `itooprc` file... `/opt/OV/bin/OpC/`
	Process names	Check to see if `opcmona` is running.
`Computer Bold`	Text that you enter	At the prompt, enter **`ls -l`**.

Table 1 Typographical Conventions (Continued)

Font	Meaning	Example
Keycap	Keyboard keys	Press **Return**.
	Menu name followed by a colon (:) means that you select the menu, and then the item. When the item is followed by an arrow (->), a cascading menu follows.	From the menu bar, select **Actions: Filtering -> All Active Messages**.
	Buttons in the user interface	Click **OK**.

In This Document

This document describes how to configure HPOM to provide smart card authentication using the Common Access Card (CAC). The CAC is a physical device issued by the United States Department of Defense (DoD) and it is used to identify users (that is, active-duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel) in secure systems. This smart card can be used to store certificates both verifying the user’s identity and allowing access to secure environments.

In this document, you can also read how secure communication is established and which events constitute an HPOM CAC session.

For detailed descriptions, see the following sections:

- “HPOM for CAC Authentication” on page 8
- “Configuring HPOM for CAC Authentication” on page 10
- “Structure of an HPOM CAC Session” on page 17
- “Viewing Log Files” on page 19

1 Common Access Card Authentication

HPOM for CAC Authentication

HPOM supports CAC technologies to authenticate and authorize users. By configuring HPOM for CAC authentication, access to HPOM user interfaces is allowed only to operators who possess a valid CAC with a valid certificate. Therefore, security is increased and access procedures are simplified.

When configuring HPOM to use CAC authentication, you must first set up a CAC environment and then customize access privileges for each user. For details, see “Configuring HPOM for CAC Authentication” on page 10.

Authentication and Secure Communication

Authentication plays a vital role in ensuring that system access is as secure as possible. In response to increased security requirements, HPOM can be configured to use certificates instead of the standard model where each user enters a user name and a password manually. This means that two-factor authentication (that is, requiring a CAC PIN entry as well as possession of a valid smart card and a certificate contained on the card) can now be used instead of one-factor authentication (that is, using something known only to the user).

With CAC authentication, the certificate stored on the card is checked for a valid expiration date, then against the certificate authority server to verify that it is not revoked.

The main communication security components responsible for creating and managing certificates are a certificate server, a keystore, and a certificate client. The following conditions are required for secure communication:

❏ The server system hosts the certificate server that contains the needed certification authority (CA) functionality.

❏ Each system that is involved in communication has a certificate that was signed by the certificate server with the CA private key.

- ❑ Each system has a list of trusted root certificates that must contain at least one certificate. The trusted root certificates are used to verify the identity of the communication partners. A communication partner is trusted only if the presented certificate can be validated using the list of trusted certificates.

Secure Data Exchange

To provide secure data exchange, HPOM uses assymetric encryption. This means that two related keys—a key pair—are used to encrypt a message. The key pair consists of a public key and a private key. The intended recipient’s public key is available to anyone who wants to send a message, whereas the private key that is needed for decryption of the message is known only to the receiver. Therefore, a message that is encrypted by using the public key can only be decrypted by using the corresponding private key and vice versa.

Configuring HPOM for CAC Authentication

To configure HPOM for CAC authentication, complete these tasks:

❑ Task 1: “Setting up a CAC Environment” on page 10

❑ Task 2 (*optional*): “Customizing a CAC Environment” on page 15

Setting up a CAC Environment

For the HP Operations management server to support CAC authentication, a CAC environment must be set up. The setup of the CAC environment is done by using the `cacsetup` script, the syntax of which is as follows:

```
cacsetup enable
         disable
         authgrp [<group>]
```

You can choose among the following log-on modes:

❑ `enabled`

Enables a logon to the HPOM user interfaces only by using a CAC for authentication.

❑ `legacy`

Enables a logon to the HPOM user interfaces either by providing a user name and a password or by using a CAC for authentication.

❑ `disabled`

Enables a logon to the HPOM user interfaces only by providing a user name and a password.

To set up the HP Operations management server for CAC authentication, follow these steps:

1. Install all the required patches as described in the *HPOM Software Release Notes*.

IMPORTANT Make sure that the Accessories patch version 09.10.230 is installed.

2. Enable CAC authentication by running the `cacsetup enable` command.

   For detailed information about the actions that are performed during the Java GUI or Administration UI setup, see “Java GUI and Administration UI Setup” on page 12.

3. *Optional:* Enable command line authentication.

   A new command, `cacsetup authgrp <group>`, allows you to specify an operating system user group that is authorized to run some of the command line interfaces that required the `root` user before the CAC feature was supported with HPOM.

NOTE If you run `cacsetup authgrp` only (that is, without specifying the desired authorized group), this option is disabled.

4. *Optional:* Customize the CAC authentication options to meet your needs.

   For detailed information, see “Customizing a CAC Environment” on page 15.

5. Start the HP Operations management server processes by running the following command:

   ```
   /opt/OV/bin/ovc -start
   ```

Configuration Files

Before you start configuring HPOM for CAC authentication (that is, before you run the `cacsetup` script), you can find all CAC configuration files at the following location:

```
/var/opt/OV/conf/webserver/
```

NOTE CAC authentication is disabled by default. After you run the `cacsetup` script, the configuration files are moved to the correct location (for example, the web server configuration directory, HTML document directories, and so on).

The following is the list of all CAC configuration directories:

`certificates` Contains all DoD root certificates that are trusted. All certificates used for authentication must be directly or indirectly signed by these certificates.

`java` Contains the filters that are attached to the Tomcat or Jetty web server so that the certificates are accepted and their owner is mapped to a particular HPOM user. Some of these filters also include the source code so that you can provide your own user mapping implementation.

`perl` Contains an alternative implementation of the Java GUI's Perl launcher that allows CAC authentication.

Java GUI and Administration UI Setup

The Java GUI and Administration UI setup actions are performed in the following order:

1. *Enabling certificate revocation checks in the HPOM Tomcat or Jetty web server*

   Even if the certificate is valid and not expired, it could be revoked because of one or more of the following reasons:

   - The CA issued a wrong certificate.
   - The owner's contract is terminated.
   - The owner misused the certificate or failed to adhere to CA policies.
   - The private key is leaked or otherwise compromised.

   In any of these cases, the certificate cannot be trusted anymore. Because of this, HPOM must check the certificate against a list of revoked certificates. These lists are published by the CA and renewed regularly.

2. *Creating a certificate keystore*

   A keystore is a file that serves as a container for one or more certificates. The keystore created by using the `cacsetup` script contains the certificates for all DoD certification authorities. Therefore, the Tomcat or Jetty web server can check if the CAC certificate provided by the user is valid.

3. *Copying the default mapping library to the Tomcat or Jetty library directory*

   When the certificate is accepted, a method for determining if a user has access to the application must be established. In addition, the certificate user must be mapped to the HPOM user.

   When a user logs on to the Java GUI or the Administration UI with a CAC certificate, a mapping procedure that assigns a certificate user to a particular Java GUI or Administration UI user is required. By default, the mapping procedure is done in the `com.hp.ov.tomcat.UserAuth` class in the `OmRealm.jar` file. If the `com.hp.ov.tomcat.UserAuth` class is used, the `/etc/opt/OV/share/conf/OpC/mgmt_sv/CAC_JGUI_users` file (for the Java GUI) or the `/etc/opt/OV/share/conf/OpC/mgmt_sv/CAC_ADMINUI_users` file (for the Administration UI) must be created. This file contains a series of text lines that indicates a certificate's common name and assigns the Java GUI or Administration UI user to it. For example:

   ```
   John Doe=opc_adm
   John Smith=john_smith@mycompany.com
   ```

   Therefore, you can add or reassign users by manually editing this file.

   If you want to implement a different or more complex authentication system, you must create a custom class named `com.auth.custom.UserAuth` in a jar file, and then copy that jar file to the `/opt/OV/nonOV/tomcat/b/libs` directory (for the Java GUI) or `/opt/OV/OMU/adminUI/lib/midas` directory (for the Administration UI).

IMPORTANT

Administration UI only: Make sure that the name of the jar file is `user-auth.jar`.

The class must contain a single, static method that is in accordance with the following definition:

```
public static String authorizeUser (X509Certificate
userCert){}
```

This method processes the provided user certificate and returns the corresponding Java GUI or Administration UI user name. If the provided user certificate is incorrect or its user is not authorized, the method returns null.

After deploying the custom class, make sure to reload the Java GUI or Administration UI configuration by running the following commands:

- *For the Java GUI:*

  ```
  /opt/OV/bin/ovc -stop ovtomcatB
  ```

  ```
  /opt/OV/bin/ovc -start ovtomcatB
  ```

- *For the Administration UI:*

  ```
  /opt/OV/OMU/adminui clean
  ```

  ```
  /opt/OV/OMU/adminui start
  ```

4. *Replacing authentication procedures in the Java GUI or Administration UI web applications*

   When authentication requisites are met, the Java GUI or Administration UI web application is modified to enable certificate authentication. In addition, a smart card filter is enabled. This filter checks if the provided certificate is stored in the smart card and if it is intended for authentication purposes.

5. *Java GUI only: Replacing the Java GUI Perl launcher with a CAC-enabled launcher*

   The Java GUI is run as an applet by using the `ito_op_applet_cgi.ovpl` Perl script. A modified script, `ito_op_applet_cgi_cac.ovpl`, which receives the certificate information for Tomcat, encrypts the information, and sends it to the Java GUI, is provided. The Java GUI receives this authentication information and an automatic logon is performed (that is, with no need to provide a user name and a password).

6. *Setting up required HP Operations management server configuration variables (`Mode` and `TokenTimeout`)*

   The `cacsetup` script creates several variables that are read by HPOM processes. These variables influence the behavior of the processes. For example, some of these variables represent the mode of operation and a timeout that indicates the maximum period of time that is allowed to pass from the moment the user enters a certificate until the connection attempt takes place. If the timeout is too long, the certificate is rejected and the user must provide it again.

For detailed information, see “Customizing a CAC Environment” on page 15.

7. *Java GUI only: Configuring the Tomcat HTTPS port to enable certificate authentication*

   The Tomcat HTTPS port must also be modified so that it can access the keystore and ask the user for a matching certificate.

8. *Restarting the Tomcat or Jetty web server*

   A restart of the `ovtomcatB` or `adminui` service is required for HPOM to accept the new configuration.

Customizing a CAC Environment

When configuring a CAC environment, you can set the following variables to meet your needs:

`Mode`

Specifies if CAC is enabled. The possible values are as follows:

- `enabled`
- `legacy` (*the default value*)
- `disabled`

For details, see “Setting up a CAC Environment” on page 10.

If you want to change the mode manually, you can only change it from `enabled` to `legacy` and vice versa. To do so, run the following command:

```
/opt/OV/bin/ovconfchg -ovrg server -ns CAC \
-set Mode <value>
```

In this instance, <*value*> is either `enabled` or `legacy`.

Changing the mode from `enabled` or `legacy` to `disabled` and vice versa can only be done by using the `cacsetup` script.

`TokenTimeout` Indicates the maximum period of time that is allowed to pass from the moment the user enters a certificate until the connection attempt takes place (that is, the period during which the certificate is still valid). The default value is 15 seconds and the time format is set to 00h00m00s (for example, 15h12m13s).

`OPC_JGUI_TIMEOUT`

Represents the number of minutes after which the user that is inactive for an extended period of time is logged out of the Java GUI. To set the desired number of minutes, run the following command:

```
ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_TIMEOUT <number_of_minutes>
```

For example, for a user to be logged out of the system after being inactive for one minute, run the following command:

```
ovconfchg -ovrg server -ns opc -set \
OPC_JGUI_TIMEOUT 1
```

`AuthGrp` Checks if a user belongs to a specified operating system group (the default value is `CACauth`). If the user belongs to the specified operating system group that is stored in the `AuthGrp` variable, access is granted. Changing this variable can only be done by using the `cacsetup` script.

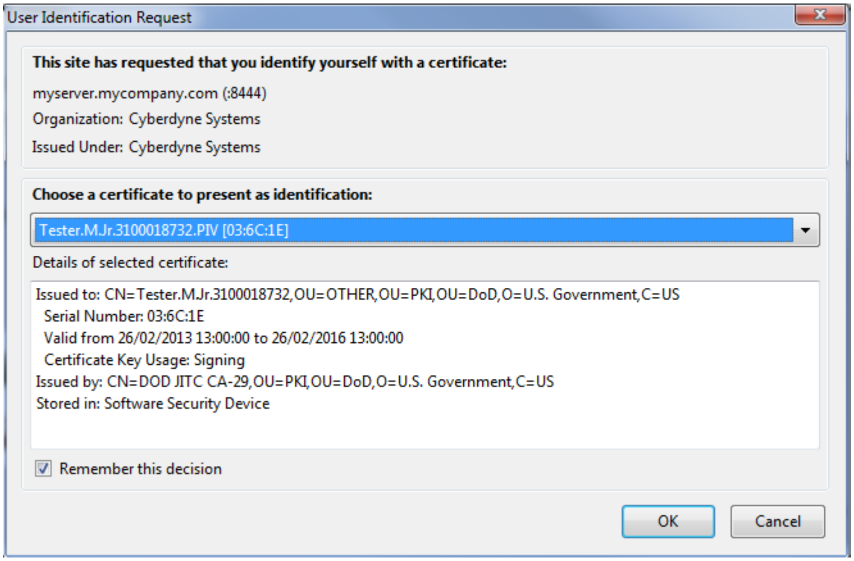
Structure of an HPOM CAC Session

The following represents the sequence of events for a user’s HPOM CAC session:

- ❑ Each CAC session begins when the user inserts the CAC into the card reader and validates it by entering the correct PIN.
- ❑ After the user enters the link to access the HPOM user interface, identification is requested.

  In the User Identification Request window, the user must choose the correct certificate, and then click OK (see Figure 1-1).

Figure 1-1 User Identification Request Window



User Identification Request

This site has requested that you identify yourself with a certificate:

myserver.mycompany.com (:8444)

Organization: Cyberdyne Systems

Issued Under: Cyberdyne Systems

Choose a certificate to present as identification:

Tester.M.Jr.3100018732.PIV [03:6C:1E]

Details of selected certificate:

```
Issued to: CN=Tester.M.Jr.3100018732,OU=OTHER,OU=PKI,OU=DoD,O=U.S. Government,C=US
  Serial Number: 03:6C:1E
  Valid from 26/02/2013 13:00:00 to 26/02/2016 13:00:00
  Certificate Key Usage: Signing
Issued by: CN=DOD JITC CA-29,OU=PKI,OU=DoD,O=U.S. Government,C=US
Stored in: Software Security Device
```

☑ Remember this decision

The certificate is validated by the following steps:

- The certificate is read from the CAC.
- The certificate is verified. It must be created by a trusted CA, and it may not be expired or revoked.
- The certificate user is mapped to the HPOM user.

❏ The authorization information is sent to the server that allows the HPOM user interface to establish a connection. When the connection is established, the user is logged on to the HPOM user interface.

❏ The CAC session ends when the user logs out of the Java GUI or the Administration UI, or closes the browser window.

Viewing Log Files

When troubleshooting, you can use a log file analysis that represents a useful methodology for understanding all the aspects of HPOM for CAC authentication as well as for investigating the cause of problems. Log files can help you pinpoint when and where problems occurred.

Depending on what you want to view, choose one of the following log files:

❏ `/var/opt/OV/log/tomcat/ovtomcatb.out`

  Used for viewing the debug of Tomcat web server's authentication (that is, provided certificates, validation, results, possible errors, and so on).

❏ `/opt/OV/OMU/adminUI/logs/web.log`

  <*Jetty_home*>`/logs/jetty*.log`

  Used for viewing the debug of Jetty web server's authentication (that is, provided certificates, validation, results, possible errors, and so on).