

HP OpenView Configuration Management

for Windows operating systems

Software Version: 5.00

SSL Implementation Guide

Document Release Date: April 2007

Software Release Date: April 2007



Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

© Copyright 1998-2007 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

Trademark Notices

Linux is a registered trademark of Linus Torvalds.

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

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

PREBOOT EXECUTION ENVIRONMENT (PXE) SERVER
Copyright © 1996-1999 Intel Corporation.

TFTP SERVER
Copyright © 1983, 1993
The Regents of the University of California.

OpenLDAP

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA.

Portions Copyright © 1992-1996 Regents of the University of Michigan.

OpenSSL License

Copyright © 1998-2001 The OpenSSLProject.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

DHTML Calendar

Copyright Mihai Bazon, 2002, 2003

Documentation Updates

This manual's title page 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 and to verify that you are using the most recent edition, visit:

ovweb.external.hp.com/lpe/doc_serv/.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP OpenView support web site at:

www.hp.com/managementsoftware/support

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

HP OpenView online 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 site to:

- Search for knowledge documents of interest
- Submit enhancement requests online
- Download software patches
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1	Introduction to SSL, Certificates, and Private Keys	11
	Overview.....	12
	An Introduction to SSL Encryption.....	12
	The Key Pair.....	12
	Private Key	12
	Public Key	13
	Certificates	13
	Certificate Authorities.....	13
	Certificates and Your Environment	13
	SSL in a Configuration Management Environment	14
	The Certificate Generation Utility.....	14
	Certificate Generation Utility Considerations	14
	Supported Configuration Management Products	14
	SSL Cipher Suite Information	15
	Requirements.....	15
	CM Server Components	15
	CM Agent Components	16
	Communications in a Configuration Management Environment.....	16
2	The Certificate Generation Utility	19
	The Certificate Generation Utility	20
	Important Considerations	20
	The Certificate Generation Utility.....	20
	Using the Certificate Generation Utility to Generate Certificates.....	21
	The Server Certificate Request File	24
	The Signed Server Certificate Request File	25
	The Private Key File.....	26
3	Configuration and Use	29
	Overview.....	30

CM Reporting Server.....	30
CM Enterprise Manager	31
User's Browser to CM Enterprise Manager.....	32
CM Enterprise Manager to CM Portal.....	33
CM Messaging Server	35
CM Configuration Server	36
CM Distributed Configuration Server.....	37
SSL Considerations.....	38
SSL Port Settings.....	38
SSL vs. non-SSL Configurations.....	39
CM Patch Manager Server.....	39
CM Integration Server	40
CM Proxy Server	41
CM Proxy Server Preload.....	42
CM Proxy Server Upstream Request	42
CM Policy Server.....	42
CM Portal.....	43
To Secure CM Portal-to-CM Portal Communications	46
Closing Steps.....	48
CM Application Usage Manager.....	49
CM Application Usage Manager Agent in a CM Environment.....	49
CM Application Usage Manager Agent in a Non-CM Environment	49
CM Agents.....	50
CM Application Self-service Manager Agent.....	51

A Troubleshooting..... 53

Certificate Authorities	53
Existing Certificate or Private Key.....	54
SSL Port is Not Enabled.....	54

B Product Name Changes 55

Index 57

1 Introduction to SSL, Certificates, and Private Keys

At the end of this chapter, you will have had the opportunity to:

- Review some of the important *components, concepts, and terms* that are integral to SSL encryption, including:
 - Private Keys
 - Public Keys
 - Certificates
 - Certificate Authorities
- Become familiar with the *cipher suite* that is used by the HP-supplied **Certificate Generation Utility**
- Become familiar with the Certificate Generation Utility *considerations*
- Review the list of *HP OpenView Configuration Management (CM) products* that can be used with the Certificate Generation Utility
- Review the various server-agent *communications relationships* that are possible in a Configuration Management (CM) environment.

Overview

This chapter starts with the section An Introduction to SSL Encryption, which provides an introduction to some of the important components, concepts, and terms that are relevant to SSL encryption.

Following the introduction is the section, SSL in a Configuration Management Environment (starting on page 14), which provides a more specific discussion of SSL in an HP OpenView Configuration Management environment, including:

- The Certificate Generation Utility, which has been provided for ease-of-use in creating certificates—especially self-signed certificates for testing, and
- Supported Configuration Management Products, which includes:
 - SSL cipher-suite information,
 - SSL encryption requirements, and
 - A list of the Configuration Management products that can be used with the Certificate Generation Utility.

An Introduction to SSL Encryption

This section details some of the components, concepts, and terms that are part of SSL encryption.

The Key Pair

SSL encryption uses a **key pair** to encrypt a transmission. The key pair is a **private key** and a **public key**.

Private Key

A key pair must be generated for each server. The server retains the **private key** and must keep it secure.

Public Key

The **public key** is passed to the agent by the server. The agent must trust that the public key that it receives is truly from the server that it (the agent) thinks it is communicating with. **Certificates** are used to provide this trust.

Certificates

A certificate contains the server's public key, the server name, and a signature from a trusted **Certificate Authority (CA)**. The agent is configured with certificates from the CAs that it trusts. Therefore, as long as the server's certificate has been *signed* by a CA that the agent trusts (see The Server Certificate Request File, starting on page 24), the server's certificate is considered "trusted," and SSL communications between the server and agent can be initiated.

For SSL encryption to work, the following three things are needed.

- A private-public key pair on the server
- A certificate that is based on the server's public key and that has been signed by a trusted CA
- The trusted CA's certificate

Certificate Authorities

In this document, the term "trusted, external CA" refers to any of the Certificate Authorities.

Certificates and Your Environment

Production Situations

It is best to generate a signing request that can be signed by a trusted, external CA.

Test Situations

You can provide either:

- A **self-signed certificate**
You must configure the agent to trust each server's certificate.

- **A private CA-signed certificate**
You can sign each server's certificate quickly (because you are the signing authority) and you only need to configure the agent to trust the private CA's certificate.

SSL in a Configuration Management Environment

This section presents introductory information about the HP-supplied **Certificate Generation Utility**, as well as the various Configuration Management (CM) products that can be configured for SSL communications, and an overview of the protocols that are used to secure the various CM server-CM agent communications.

The Certificate Generation Utility

The HP-supplied **Certificate Generation Utility** (CGU) is an optional utility that has been provided for ease-of-use in creating certificates—especially self-signed certificates for testing.

Prior to using the CGU, HP recommends that you review the following considerations.

Certificate Generation Utility Considerations

- The Certificate Generation Utility is **not** a supported HP OpenView Configuration Management product.
- The Certificate Generation Utility is provided *free of charge*.
- The Certificate Generation Utility is used at *your own discretion*; HP Technical Support **will not** address any issues regarding its use or functionality.

Supported Configuration Management Products

This section presents SSL cipher-suite information and requirements that are specific to Configuration Management products. Also included is a list of the Configuration Management products that can be used with the Certificate Generation Utility. See the sections:

- CM Server Components, starting below, and
- CM Agent Components, starting on page 16.

SSL Cipher Suite Information

HP's Configuration Management (CM) products use the following cipher from the SSL version 3 cipher suite: 168-bit triple DES cipher block chaining mode, 1024-bit RSA asymmetric key exchange, and secure hash algorithm version 1.0.

Requirements

To ensure that SSL encryption will work with the CM products, the following requirements must be met.

- CM servers must have a **server certificate**, a **private key**, and a **Certificate Authority (CA)** root certificate.
- CM agents must have a **Certificate Authority (CA)** root certificate.

CM Server Components

The following is a list of the Configuration Management **server** products that can be used with the Certificate Generation Utility.

- HP OpenView Configuration Management Reporting Server (CM Reporting Server), see CM Reporting Server on page 30
- HP OpenView Configuration Management Enterprise Manager (CM Enterprise Manager), see CM Enterprise Manager on page 31
- HP OpenView Configuration Management Messaging Server (CM Messaging Server), see CM Messaging Server on page 35
- HP OpenView Configuration Management Configuration Server (CM Configuration Server), see CM Configuration Server on page 36
- HP OpenView Configuration Management Distributed Configuration Server (CM Distributed Configuration Server), see CM Distributed Configuration Server on page 37
- HP OpenView Configuration Management Patch Manager (CM Patch Manager), see CM Patch Manager Server on page 39
- HP OpenView Configuration Management Integration Server (CM Integration Server), see CM Integration Server on page 40

- HP OpenView Configuration Management Policy Server (CM Policy Server), see CM Policy Server on page 42
- HP OpenView Configuration Management Proxy Server (CM Proxy Server), see CM Proxy Server on page 41
- HP OpenView Configuration Management Portal (CM Portal), see CM Portal on page 43
- HP OpenView Configuration Management Application Usage Manager (CM Application Usage Manager), see CM Application Usage Manager on page 49

CM Agent Components

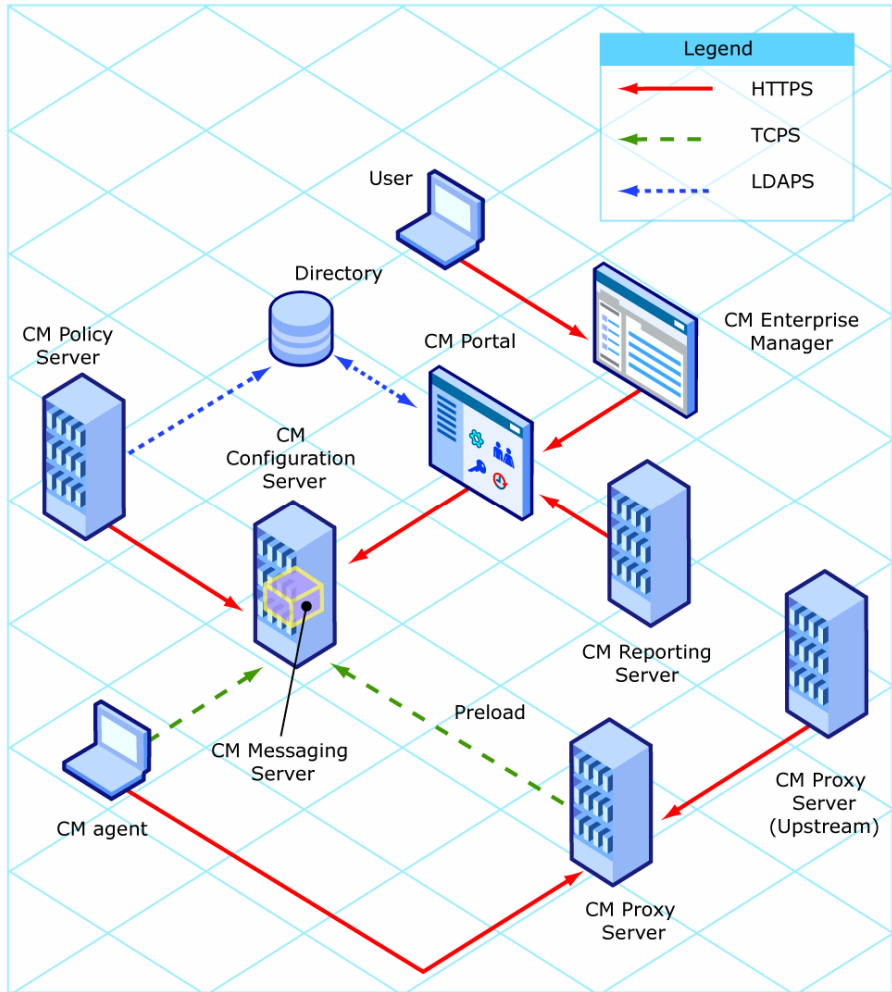
The following is a list of the Configuration Management **agent** products that can be used with the Certificate Generation Utility. For information about these products, see the section, CM Agents, starting on page 50.

- HP OpenView Configuration Management Application Manager agent (CM Application Manager agent)
- HP OpenView Configuration Management Application Self-service Manager agent (CM Application Self-service Manager agent), see CM Application Self-service Manager Agent
- HP OpenView Configuration Management Inventory Manager agent (CM Inventory Manager agent)
- HP OpenView Configuration Management Patch Manager agent (CM Patch Manager agent)

Communications in a Configuration Management Environment

Figure 1 on page 17 presents an overview of the various types of communications and relationships that are possible in an HP OpenView Configuration Management environment.

Figure 1 Communications Overview



2 The Certificate Generation Utility

At the end of this chapter, you will have:

- A better understanding of HP's **Certificate Generation Utility**
- Chosen whether to use an existing certificate or generate a new certificate



UNIX Note

HP's **Certificate Generation Utility** can generate certificates on Windows platforms only.

However, once generated on a Windows system, certificates can be copied over to and used on UNIX platforms.

The Certificate Generation Utility

The HP-supplied **Certificate Generation Utility** is an optional utility that has been provided for ease-of-use in generating certificates, especially self-signed certificates for testing.



UNIX Note:

For the following options, add the `-hostname` parameter in order to generate a certificate for a specific host. If `-hostname` is not specified, the default (the current computer's hostname) will be used.

Important Considerations

- The Certificate Generation Utility is **not** a supported HP OpenView Configuration Management product.
- The Certificate Generation Utility is provided *free of charge*.
- The Certificate Generation Utility is used at *your own discretion*; HP Technical Support **will not** address any issues regarding its use or functionality.

The Certificate Generation Utility

The Certificate Generation Utility can be found on the Configuration Management media in:

```
INFRASTRUCTURE\extended_infrastructure\certificate_mgmt
```

- In order to perform the tasks that are outlined in this chapter, the `certificate_mgmt` directory must be copied from the Configuration Management media to a directory on the local machine, such as:

```
C:\temp\certificate_mgmt
```



This document uses the directory, `C:\temp\certificate_mgmt`, in its examples.

When working with the Certificate Generation Utility, be sure to specify the directory into which you have copied the `certificate_mgmt` directory.

Using the Certificate Generation Utility to Generate Certificates

This section provides instructions for creating certificates that will be used for SSL configuration.

- ▶ If you are already creating certificates in your environment with existing tools, skip to the next chapter Configuration and Use, starting on page 29.

Task 1 Private Key File

Do you have a private key file in PEM format?

If YES:

Copy your private key file to the `server\hostname` directory.

- `hostname` is the name of the server for which a signed certificate is to be created.

For example: **cmserver1**.

- The private key file should be named `hostname-prvkey.pem`.

For example: `certificate_mgmt\servers\cmserver1\cmserver1-prvkey.pem`.

If NO:

Continue to the next step, Generating a Signed Certificate.

Task 2 Generating a Signed Certificate

There are three methods by which to generate a signed certificate: *self-signing*, via a *generated CA*, and via an *external, trusted CA*. This task details how to use the Certificate Generation Utility with these three options.

- ▶ The `-hostname` parameter can be used in order to generate a certificate for a host other than the current computer.
If `-hostname` is not specified, the current computer's hostname will be used.

Option 1: Generating a Self-signed Certificate

- 1 From the `certificate_mgmt` directory, run the command
certificate_mgmt> cert_mgr create self

- ▶ To generate a certificate for a host other than the current computer, add the parameter `-hostname` at the end of the command line, as shown.

```
certificate_mgmt> cert_mgr create self -hostname  
NewServer01
```

- 2 Answer the configuration questions; these will be used to create the **Distinguished Name** for the certificate.

- ▶ The **Distinguished Name (DN)** is a unique identifier that is used just to provide a name that is unique for the certificate. Location, company name, and host name information make the DN unique.

It is important that the **Common Name (CN)** part of the certificate's DN be the same as the server's host name. This is vital to the agent trusting that it is communicating with the expected host.

The output file locations will be displayed on the screen when complete. For example:

```
servers\cmserver1\cmserver1.cnf  
servers\cmserver1\cmserver1-cert.pem  
servers\cmserver1\cmserver1-cert.txt  
servers\cmserver1\cmserver1-prvkey.pem  
servers\cmserver1\cmserver1-signer.pem  
servers\cmserver1\cmserver1-signer.txt  
servers\cmserver1\cmserver1-cert.rnd
```

If you are already creating certificates in your environment with existing tools, feel free to skip to Configuration and Use, starting on page 29.

Option 2: Generating a Re-usable Certificate Signed by Generated CA


- 1 From the `certificate_mgmt` directory, run the command

```
certificate_mgmt> cert_mgr create signed
```

- ▶ To generate a certificate for a host other than the current computer, add the parameter `-hostname` at the end of the command line, as shown.

```
certificate_mgmt> cert_mgr create signed -hostname  
NewServer01
```

- 2 Answer the configuration questions; these will be used to create the DN for the certificate.

 This series of questions will include a prompt for a Common Name.

The output file locations will be displayed on the screen when complete. For example:

```
certificate_mgmt\ca\ca.cnf
certificate_mgmt\ca\ca.rnd
certificate_mgmt\ca\ca-prvkey.pem
certificate_mgmt\ca\ca-index.txt
certificate_mgmt\ca\ca-serial
certificate_mgmt\ca\ca-cert.pem
certificate_mgmt\servers\cmserver1\cmserver1-cert.txt
certificate_mgmt\servers\cmserver1\cmserver1-cert.pem
certificate_mgmt\servers\cmserver1\cmserver1-signer.pem
```

 With this option, the Signing Authority Certificate is copied from `certmgr\ca` directory.


If a `ca-cert.pem` exists in this directory, it will be used. Otherwise, it will be created on the first run and used for generating subsequent certificates.

If you are already creating certificates in your environment with existing tools, feel free to skip to Configuration and Use, starting on page 29.

Option 3: Generating a Certificate Signed by a Trusted, External CA (such as VeriSign, Inc.)

- 1 From the `certificate_mgmt` directory, run the command

```
certificate_mgmt> cert_mgr create request
```

 To generate a certificate for a host other than the current computer, add the parameter `-hostname` at the end of the command line, as shown.

```
certificate_mgmt> cert_mgr create request -  
hostname NewServer01
```

- 2 Answer the configuration questions; these will be used to create the DN for the certificate.

The output file locations will be displayed on the screen when complete.
For example:

```
servers\cmserver1\cmserver1.cnf  
servers\cmserver1\cmserver1.rnd  
servers\cmserver1\cmserver1-prvkey.pem  
servers\cmserver1\cmserver1-request.pem  
servers\cmserver1\cmserver1-request.txt
```

- 3 Request a signed certificate by sending the *hostname-request.pem* to your signing authority.
- 4 When you receive this signed certificate, paste it into the *servers\hostname\hostname-cert.pem* file.
- 5 Paste the Signing Authority Certificate (must be in PEM format) into the *servers\hostname\hostname-signer.pem* file.

You now have a private key, a signed certificate, and the signing authority certificate files that are needed for product configuration. See *CM Reporting Server*, starting on page 30, and *CM Enterprise Manager*, starting on page 31.

The Server Certificate Request File

The Certificate Generation Utility generates a **Server Certificate Request file** such as,

```
host.HP.com-request.pem.
```

To have the Server Certificate Request file (**SCR file**) signed and returned, follow the procedure that is required by your public **Certificate Authority (CA)**. Typically, the SCR file must be opened in a text editor, its text copied to a clipboard, and then pasted into a text field on the signing CA's web page.

To issue a signed certificate, the signing CA will also require proof-of-identity and authority—such as your company's DUNS number, Articles of Incorporation, Partnership Papers, or Business License.



Be sure that the server certificate that is purchased is a **base-64 encoded x.509** certificate. This is typical for certificates that are generated for the Apache Freeware (ModSSL or OpenSSL) Server.

- For the HP OpenView Configuration Management Configuration Server (CM Configuration Server) the SCR file is located in:
 - bin\Certificates\requests (Windows)
 - exe/Certificates/requests (UNIX).
- For the HP OpenView Configuration Management Integration Server (CM Integration Server) the SCR file is located in:
 - \etc\Certificates (Windows)
 - exe/Certificates (UNIX).

If the SCR file is opened with a text editor, it will appear similar to that which is shown in the following figure.

Figure 2 Server Certificate Request file

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCCAQcCAQAwwgaQxCzAJBgNVBAYTA1VTMRMwEQYDVQKIIEwpOZXcgSmVyc2V5
MQ8wDQYDVQQHEwZNYWVh3YWgXHjAcBgNVBAoTFU5vdmFkaWdtIEN1c3RvbWVyeIENv
LjEnMCUGA1UECXMtWFuYWdlbWVudCBJbmZvcmlhdGlvbiBTeXNOZW1zMSYwJAYD
VQODEx1yYWRpYTAwMS5Ob3ZhdG1nbUN1c3RvbWVyeLmNvbTBcMAOGCSqGSIb3DQEB
AQUAAOsAMEgCQQDMg53F1yIsmZjAeKLqSUQkZg8xEWNC476KIPL0T/4bkSB9r1bv
eN5gdVOSVrDsJyGZjBjNQEW60DaAJELakMevAgMBAAGgADANBgkqhkiG9wOBAQQF
AANBAAMs5KqyJwu88AspdZWucFcDaxcSBVvRIyr2wmfw5cLzGwwZMWgiX93Xublx
7G4xohoZddAbSdZWIU39EBpRg1Y=
-----END CERTIFICATE REQUEST-----

```

The Signed Server Certificate Request File

When the signed SCR file is returned from the public CA:

- 1 In the signed SCR file's name, change the **request** (request) to **cert** (certificate). For example, change

```
host.HP.com-request.pem
```

to

```
host.HP.com-cert.pem.
```



The SCR file might have a different name when it is returned from the CA.

- 2 Place the renamed SCR file (host.HP.com-cert.pem) in the appropriate folder, as below.

- For the CM Configuration Server, place the file in:

bin\Certificates (Windows)

exe/Certificates (UNIX).

- For the CM Integration Server, place the file in:

\etc\Certificates (Windows)

exe/Certificates (UNIX).

- 3 Restart the CM Configuration Server or CM Integration Server, and examine its log to verify that the SSL Manager task starts correctly and successfully verifies the CA certificate and server certificate.

The Private Key File

The Certificate Generation Utility also generates a **private key** such as,

host.HP.com-prvkey.pem.

- For the CM Configuration Server, the private key is located in:
 - bin\Certificates (Windows)
 - exe/Certificates (UNIX).
- For the CM Integration Server, the private key is located in:
 - \etc\Certificates (Windows)
 - exe/Certificates (UNIX).

If the private key is opened with a text editor, it will appear similar to the following.

Figure 3 Private key file

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-CBC, 6EC0947550541AAB

1MV8Y4rkyw1Yn3OyUBSULtKLfjOYSzX+KZvxCeuw+9x95x1Ikvej4b8iBDuEOaTR
fp4IDVLuNOH57psT+XdCtRAam493t8csfOC18CURHO/PskT5S1H80EGOPnHcg1rg
YzaVt+pM7ZtxZuWRPKS1RbvRi5YTFU/3Tjtfn0qieWaqbxFOTVnzfICX7I1VODOC
OFBwd5XB6cMOZf003yQhte2k2UHvG8PRDlpOrRPEgUvlqqBI1xQ005GSc020nnwP
WYhUwjAhjB1ALVubZKw5wk/E5lowy4qucWzCp/7c7fyXwiBIk3QWehEwe/NA1kWc
BbOXUiB1PZGtodasgusKDrOmrazm/h1bTbxMinNgz1OwMX/ZztTuN+bX+pSLEh3u
piAcdw46e3wKf40KRpiXRbJyoWiIhgeaqwJ7wEr907w=
-----END RSA PRIVATE KEY-----
```

In order to maintain compatibility with industry standards, HP has adopted the RSA crypto-system method of obtaining certificate requests. The RSA crypto-system is a public key crypto-system that offers encryption and digital signatures (authentication). In the private key shown above the key type (**RSA**) is indicated at the beginning and end of the file.

3 Configuration and Use

At the end of this chapter, you will know how to:

Configure secure connections for:

- CM Reporting Server via HTTPS
- CM Enterprise Manager via HTTPS
- CM Messaging Server via HTTPS
- CM Configuration Server via TCPS
- CM Distributed Configuration Server via HTTPS
- CM Patch Manager Server via TCPS
- CM Integration Server components:
 - CM Proxy Server via HTTPS
 - CM Policy Server via HTTPS and LDAPS
- CM Portal via HTTPS and LDAPS
- CM Application Usage Manager via HTTPS and LDAPS

Set up CM Agents to use SSL

Overview

This chapter describes how to implement SSL functionality in your Configuration Management (CM) environment in order to secure the communications between CM servers and CM agents.

CM Reporting Server


The steps in this section detail how to set up the CM Reporting Server to create a secure (**HTTPS**) connection when using web services to connect to the CM Portal.

Establishing a secure connection between the CM Reporting Server and the CM Portal

- 1 Edit the `rrs.cfg` file that is located in the CM Reporting Server `etc` folder.

(Alternatively, you can use the web-based setup for CM Reporting Server.)


- Within the `::rrs::packconfig "" {}` section, add/edit the following entries:

 If you prefer to use the defaults, the following edits are not necessary.

SSL_CADIR: The CA Certificates directory. If left blank, this will default to `etc\CACertificates`.

SSL_CAFILE: The CA Certificates file. If left blank, this will default to `cacert.pem`.

- 2 Copy the CA Certificates file (for example, `cmserver1-signer.pem`) into the directory that is specified for `SSL_CADIR`. The default is `etc\CACertificates`.

 This step is needed only if your certificate isn't signed by an established and trusted, external CA.

- 3 Configure the following parameters in the CM Reporting Server configuration file, `rrs.cfg`.

- a Configuring CM Reporting Server to authenticate against the CM Portal:
 - RMPLOGON: Enable/disable CM Portal logon support
 - RMPIP: The fully qualified host name (*localhost* is acceptable) of the CM Portal server
 - RMPPORT: The port of the CM Portal server (**443** if SSL is used)
 - RMPUSESSL: Enable/disable use of SSL web services
- b Configuring CM Reporting Server to use web services to populate its Directory Browser:



All changes here are under the LDAP portion of the `rrs.cfg` file.

- TYPE: **rmp-ws**
 - SERVER: The fully qualified host name of the CM Portal server
 - PORT: The port of the CM Portal server (**443** if SSL is used)
 - USER: The CM Portal *service account user ID* (for example, **admin**)
 - PASS: The CM Portal *service account password* (for example, **secret**)
 - USESSL: **1** (to enable SSL support)
- 4 Verify that you can logon to the CM Reporting Server and that the Directory Browser appears properly.

On the CM Reporting Server logon page, there should be a lock icon; this indicates that SSL web services are enabled.

CM Enterprise Manager

This section details the two potential secure (**HTTPS**) connections that CM Enterprise Manager can have.

- A user's browser to the CM Enterprise Manager, (starting on page 32) and
- The CM Enterprise Manager to the CM Portal (starting on page 33).

- ▶ The HP CM Enterprise Manager can also be used to create a directory service connection for LDAPS.

For more information, refer to the section *To Configure LDAP Directory Services with SSL* in the *HP OpenView Configuration Management Enterprise Manager User Guide*.

User's Browser to CM Enterprise Manager

In this scenario the CM Enterprise Manager is acting as a *server* so it must have a key pair and a signed certificate for the public key.

- ▶ The CM Enterprise Manager is written in Java which uses keystores to hold the key pair and signed certificate.

The CM Enterprise Manager administrator must create the keystore file, and can do so using the Certificate Generation Utility, as described in this section.

If you create a privately signed or self-signed certificate, the keystore file is automatically created.

If you generate a request to be signed by a trusted, external CA, then you must import the certificate—after it has been signed—into the directory to create the keystore file, as described below.

Establishing a secure connection between the CM Enterprise Manager and a user's browser

- ▶ The first step needs to be performed only if you are using a certificate tool other than the HP-provided Certificate Generation Utility; otherwise skip to step 2.

- 1 Use the following command to import a signed certificate into the HP Certificate Generation Utility.

```
certificate_mgmt\cert_mgr import signed -hostname xxxxxx  
-signedcert YYYYYY -signercert zzzzz
```

Where

xxxxxxx = The fully qualified host name of the system to which the certificate belongs, such as **cmserver1.mycorp.com**.

yyyyyy = The fully qualified path and file name of the signed certificate that was returned by the CA, such as **C:\certs\cmserver1.mycorp.com-cert.pem**.

`zzzzzzz` = The fully qualified path and file name to the certificate of the signing CA, such as **C:\certs\cmserver1.mycorp.com-signer.pem**.

This process will import the certificate files into the `servers\hostname` directory that will be used in step 2.

The Java keystore file is located in

```
certificate_mgmt\servers\emsvrname\emsvrname-keystore.jks
```

Where

`emsvrname` = the host name of the CM Enterprise Manager server

- 2 Copy the Java keystore file from the above-mentioned location to

```
<EM Install Dir>\nonOV\jre\b\lib\security\cm-ec.keystore
```



On a typical install, `<EM Install Dir>` will be `C:\Program Files\HP OpenView`.

CM Enterprise Manager to CM Portal

In this case, the CM Enterprise Manager is the client and the CM Portal is the server.



The CM Enterprise Manager is written in Java, so it uses a truststore file to store the certificates of trusted CAs.

Make sure that the CM Enterprise Manager truststore file contains the certificate for the CA that signed the CM Portal signed certificate.

Establishing a secure connection between the CM Enterprise Manager and the CM Portal

- 1 Ensure that the CM Portal server is configured for SSL before continuing on to step 2.



The next step needs to be performed only if you are using a certificate tool other than the HP-provided Certificate Generation Utility; otherwise skip to step 3.

- 2 Use the following command to generate the truststore.

```
certificate_mgmt\cert_mgr import signed -hostname xxxxxx  
-signedcert yyyyyyy -signercert zzzzzz
```

Where

xxxxxxx = The host name of the CM Portal server, such as **cmserver1.mycorp.com**.

(The certificate must be the same as that which is used when configuring the CM Portal for SSL.)

yyyyyyy = The fully qualified path and file name of the signed certificate that was returned by the CA, such as **C:\certs\cmserver1.mycorp.com-cert.pem**.

zzzzzzz = The fully qualified path and file name of the certificate of the signing CA, such as **C:\certs\cmserver1.mycorp.com-signer.pem**.

The Java truststore file is located in

```
certificate_mgmt\servers\emsvrname\emsvrname-  
truststore.jks
```

Where

emsvrname = the host name of the CM Portal server

This process will import the certificate files into the `servers\portalsvrname` directory that will be used in step 3.

3 Copy the Java truststore file to

```
<EM Install Dir>\nonOV\jre\b\lib\security\cm-  
ec.truststore
```



On a typical install, *<EM Install Dir>* will be `C:\Program Files\HP OpenView`.

4 Go to `<EM Install Dir>\CM-EC\tomcat\webapps\em\WEB-INF`, and edit the `console.properties` file as indicated below.

- Change protocol from `protocol=http\://` to: **`protocol=https\://`**.
- Change the value of `port` to the value that was used to configure the CM Portal SSL port

5 Restart the CM Enterprise Manager service to begin using the new truststore.

CM Messaging Server

The steps in this section detail how to set up the CM Messaging Server for secure (**HTTPS**) connections.

The `Overrides Config` section of the CM Messaging Server configuration file, `rms.cfg`, has to be populated with the *certificate path*, *private key path*, and *secure port* values. The CM Messaging Server installation puts `cacert.pem` in the `/etc/CACertificates` directory.

Establishing a secure connection on the CM Messaging Server

- 1 Stop the CM Messaging Server service (**rms**).
- 2 Copy the private key and signed certificate into the CM Messaging Server Certificates directory.

The default is `C:\Program Files\Hewlett-Packard\CM\Messaging Server\etc\Certificates`.


- 3 Verify that `tls.tkd` exists in the `modules` directory.
- 4 Navigate to the `MessagingServer\etc` directory and open `rms.cfg` in a text editor.
 - a Verify that `module load tls` is uncommented.
 - b In the `Overrides Config` section, add the following parameters:

```
Overrides Config {  
    SSL_CERTFILE "C:/Program Files/Hewlett-  
Packard/CM/Messaging Server  
/etc/Certificates/myserver-cert.pem"  
    SSL_KEYFILE "C:/Program Files/Hewlett-  
Packard/CM/Messaging Server  
/etc/Certificates/myserver-prvkey.pem"  
    HTTPS_PORT "443"  
}  
  
module load tls
```

- 5 Save your changes and close `rms.cfg`.
- 6 Restart the CM Messaging Server service (**rms**).
- 7 Check the `rms.log` to ensure that the secure server has been started; look for the following message.

```
MSG/HTTPD: secure httpd on tcp://0.0.0.0:443 started
```

To use SSL for outgoing HTTP posts, specify **HTTPS** as the **TYPE**, and use a URL with **https** specified and include the secure port of the server that will be receiving the posts, as shown in the following example.

 This update is required for the `rms.cfg` file or for any data delivery agent (`core.dda.cfg`, `inventory.dda.cfg`, etc.) that is configured in the CM Messaging Server environment.

```
msg::register secure1 {
  TYPE  HTTPS
  ADDRESS {
    PRI  10
    URL  https://localhost:443/proc/inventory
  }
}
```


CM Configuration Server

This section details how to set up the CM Configuration Server for secure (**TCPS**) connections.

To confirm that the CM Configuration Server is configured for SSL support, use a text editor to open the `edmprof` file, which is located in the CM Configuration Server `bin` (Windows) / `exe` (UNIX) directory. Verify the following:

- The `MGR_ATTACH_LIST` section contains the `zsslmgr` `CMD_LINE`, as shown:

```
[MGR_ATTACH_LIST]
CMD_LINE = (zsslmgr) RESTART = YES
```

 This line might need to be uncommented in the `edmprof` file.

- The `MGR_SSL` exists and is populated with the correct location and file names, as shown:

```
[MGR_SSL]
CA_FILE = C:\Program Files\Hewlett-Packard\CM\Configuration
Server\bin\CACertificates\
```

Copy the `cacert.pem` file that is provided in the `CACertificates` directory.

```
CERTIFICATE_FILE = C:\Program Files\Hewlett-Packard\CM\
ConfigurationServer\bin\Certificates\
```

Copy the cert.pem file from the servers\hostname directory.

```
KEY_FILE = C:\Program Files\Hewlett-Packard\CM\
ConfigurationServer\bin\Certificates\
```

Copy the prvkey.pem file from the servers\hostname directory.

```
SSL_PORT = 443
```

The following table describes these settings of the MGR_SSL section.

Table 1 MGR_SSL Settings

Setting	Usage
CA_FILE	This setting is used to identify and locate the Certificate Authority's certificate. The CA certificate is usually stored in a file in PEM (Private Enhanced Mail) format. The value for this setting is the full path to a valid and existing certificate file. The SSL Manager task requires a CA certificate to start. An expired or corrupt CA certificate prevents the SSL Manager task from starting.
CERTIFICATE_FILE	This setting is used to identify and locate the server certificate of the CM server. The certificate is usually stored in a file in PEM format. The value for this setting is the full path to a valid and existing certificate file. The SSL Manager requires a certificate to start. An expired or corrupt certificate prevents the SSL Manager task from starting.
KEY_FILE	This setting is used to identify and locate the private key. The private key is usually stored in a file in PEM format. The value for this setting is the full path to a valid and existing key file. Usually the private key is stored in the same file as the server certificate, in which case you don't have to include KEY_FILE in the MGR_SSL section.
SSL_PORT	This setting is used to set the port that the SSL Manager should attend for client connections. The SSL protocol default port is 443 .

CM Distributed Configuration Server

This section details the SSL considerations for secure CM Distributed Configuration Server (CM-DCS) connections via **HTTPS**.



The CM Distributed Configuration Server configuration file is `dmabatch.rc`. It can be found in the directory into which the CM-DCS was installed.

SSL Considerations

In order to enable SSL functionality, the following conditions must be met.

- The `zsslmgr` setting (`CMD_LINE=(zsslmgr) RESTART=YES`) must be present and enabled in the `MGR_ATTACH_LIST` section of the master and slave (*Source* and *Destination*) CM Configuration Server `edmprof` files.
- In the `edmprof` file of the master CM Configuration Server, the value of `SSL_PORT` in the `MGR_SSL` section must be different than the value of `HTTPS_PORT` in `risroot\etc\httpd.rc` (the CM Integration Server's configuration file).
- The port that is set in `dmabatch.rc` for:

```
-https-port nnn
```

must match the port that is set in the `Overrides Config` section of `httpd.rc`:

```
HTTPS_PORT nnnn
```

SSL Port Settings

Table 2 lists the SSL port settings that are in the CM-DCS configuration file, `dmabatch.rc`. Also listed are the CM server configuration settings that they must match.

Table 2 CM-DCS configuration file equivalents

dmabatch.rc Setting	Equivalent Setting	Location
<code>-master-ssl-port</code>	<code>SSL_PORT</code>	Source (master) CM Configuration Server <code>edmprof</code> file
<code>-slave-ssl-port</code>	<code>SSL_PORT</code>	Destination (slave) CM Configuration Server <code>edmprof</code> file
<code>-https-port</code>	<code>HTTPS_PORT</code>	<code>httpd.rc</code> file of CM Integration Server

SSL vs. non-SSL Configurations

You can switch between an SSL and a non-SSL configuration by adjusting the `-ssl` line of the CM-DCS configuration file. Specify:

- **1** for an SSL configuration
- **0** for a non-SSL configuration

For example, if the SSL-enabled CM Configuration Server ports are **443**, and the SSL-enabled CM Integration Server port is **444**, the following could be put into `dmabatch.rc`.

```
array set 0 {  
    -ssl                1  
    -master-port       3464  
    -master-ssl-port   443  
    -slave-port        3464  
    -slave-ssl-port    443  
    -http-port         3466  
    -https-port        444  
}
```

CM Patch Manager Server

This section details how to set up the CM Patch Manager Server for secure (**TCPS**) connections.

Enable the CM Integration Server under which the CM Patch Manager Server is running, as documented in the section CM Integration Server starting on page 40.

Post-installation Notes

To establish a secure Security Patch Acquisition session, only the following CM Patch Manager Server configuration setting needs to be updated.



This can be done via the interface.

- Modify the CM Configuration Server URL to a *secure connection* value, such as:

```
tcps://Configuration_Server_machine:4430
```

Replacing a standard, non-secure TCP connection value, such as:

```
radia://machine_name:3464.
```

CM Integration Server

This section details how to set up secure (**TCPS** and **HTTPS**) connections for the Configuration Management products that run under the CM Integration Server.

To enable SSL so that the CM Integration Server can be accessed in a browser using HTTPS

- 1 Navigate to the location into which the Certificate Generation Utility was copied.
- 2 Copy the following two files.

```
servers\cmserver1\cmserver1-cert.pem
```

```
servers\cmserver1\cmserver1-prvkey.pem
```

- 3 Paste these files into:

```
C:\Program Files\Hewlett-  
Packard\CM\IntegrationServer\etc\Certificates.
```

To confirm that the CM Integration Server is configured for SSL support (via **HTTPS**), use a text editor to open the `httpd.rc` file, which is located in the `IntegrationServer` directory, and confirm that the `Overrides Config` section has been added, as shown below.

```
Overrides Config {  
  
    SSL_CERTFILE "C:/Program Files/Hewlett-Packard/CM/  
    IntegrationServer/etc/Certificates/host.HP.com-cert.pem"  
  
    SSL_KEYFILE "C:/Program Files/Hewlett-Packard/CM/  
    IntegrationServer/etc/Certificates/host.HP.com-prvkey.pem"  
  
    HTTPS_PORT "443"
```

The following table describes the settings of the `Overrides Config` section.

Table 3 Overrides Config section settings

Setting	Usage
SSL_CERTFILE	This setting is used to identify and locate the server certificate of the HP OpenView CM server. The certificate is usually stored in a file in PEM (Private Enhanced Mail) format. The value for this setting is the full path to a valid and existing certificate file. The SSL Manager requires a certificate to start. An expired or corrupt certificate prevents the SSL Manager task from starting.
SSL_KEYFILE	This setting is used to identify and locate the private key. The private key is usually stored in a file in PEM format. The value for this setting is the full path to a valid and existing key file. Usually the private key is stored in the same file as the server certificate, in which case you don't have to include KEY_FILE in the MGR_SSL section.
HTTPS_PORT	This setting is used to set the port that the SSL Manager should attend for client connections. The SSL protocol default port is 443 .

When the CM Integration Server is running you can connect to it, via HTTPS, by opening a web browser and typing

```
https://server:ssl_port
```

To disable standard HTTP (leaving only HTTPS available), open the `httpd.rc` file and in the `Overrides Config` section set `PORT` to **-1**, as in:

```
Overrides Config {  
    SSL_CERTFILE "D:/Program Files/Hewlett-Packard/CM/  
IntegrationServer/etc/Certificates/host.HP.com-cert.pem"  
    SSL_KEYFILE "D:/Program Files/Hewlett-Packard/CM/  
IntegrationServer/etc/Certificates/host.HP.com-prvkey.pem"  
    HTTPS_PORT 443  
    PORT -1
```

To configure LDAPS and HTTPS support for the CM Portal, see CM Portal on page 43.

CM Proxy Server

To enable SSL communications with a CM Proxy Server, follow the instructions below to set up a **Server Access Profile (SAP)** in the HP OpenView Configuration Management Configuration Server Database (CM Configuration Server Database [CM-CSDB]) via the HP OpenView

Configuration Management Configuration Server Database Editor (CM Configuration Server Database Editor [CM-CSDB Editor]).

- 1 Log on to the CM-CSDB Editor.
- 2 Navigate:
File=**PRIMARY**, Domain=**CLIENT**, Class=**Server Access Profile (SAP)**.
- 3 Set ENABLED=**y** for individual Instances, or to affect all Instances of the Class, set ENABLED=**y** in the **_BASE_INSTANCE_**.

CM Proxy Server Preload

To confirm that the CM Proxy Server preload Server is configured for SSL support, use a text editor to open the `rps.cfg` file, which is located in the `IntegrationServer` directory, and confirm that it has the following settings.

```
rps::init {
    -static-ssl    1
    -stager        0
}
```

CM Proxy Server Upstream Request

To confirm that the CM Proxy Server dynamic upstream request is configured for SSL support, use a text editor to open the `rps.cfg` file, which is located in the `IntegrationServer` directory, and confirm that it has the following settings.

```
rps::init {
    ...
    -dynamic-url  https://upstream:3466
}
```

CM Policy Server

To confirm that CM Policy Server LDAP is configured for SSL (**LDAPS**) support, use a text editor to open the `pm.cfg` file, which is located in the `IntegrationServer/etc` directory. Verify that the following settings have been edited for secure LDAP communication. Use the following settings as an example.

```
ldap::init {
    TYPE          ldaps
    LDAP_CACERTDIR      etc/CACertificates
    LDAP_CACERTFILE    etc/CACertificates/cacert.pem
}
```

```
LDAP_REQUIRE_CERT    demand
PORT                 636
}
```

CM Portal

This section details how to set up secure (**LDAPS** and **HTTPS**) connections for the CM Portal.

To confirm that the CM Portal is configured to connect to a secure LDAP directory using SSL (LDAPS), start the CM Portal service and check the following:

- 1 The `ldaps82.dll` is in the root `ManagementPortal` directory.
The `ldaps82.dll` file is unpacked by the `tls.tkd` module when the CM Portal service starts. If `ldaps82.dll` is missing, stop the CM Portal service, delete any existing `ldaps82.dll` file in the `ManagementPortal` directories or path, and restart the CM Portal service.
- 2 A CA Certificate file containing the LDAP server's CA root certificate (public key) is in a local directory on the CM Portal.

The Certificate Generation Utility installs a default CA Certificate file, `cacert.pem`, which includes the public keys for Entrust, VeriSign, Inc., and G.E, and is located in

```
C:\Program Files\Hewlett-
Packard\CM\ManagementPortal\etc\CACertificates.
```

To enable SSL so that the CM Portal can be accessed in a browser using HTTPS

- 1 Navigate to the location into which the Certificate Generation Utility was copied.
- 2 Copy the following two files:
`servers\cmserver1\cmserver1-cert.pem`
`servers\cmserver1\cmserver1-prvkey.pem`
- 3 Paste these files into:

```
C:\Program Files\Hewlett-
Packard\CM\ManagementPortal\etc\Certificates.
```

To confirm that the CM Portal is configured for SSL support, use a text editor to open the `httpd-managementportal.rc` file, which is located in the `ManagementPortal` directory. Confirm that the `Overrides Config` section has been added, as shown below.

```
Overrides Config {  
    SSL_CERTFILE "C:/Program Files/Hewlett-Packard/CM/  
ManagementPortal/etc/Certificates/host.HP.com-cert.pem"  
    SSL_KEYFILE "C:/Program Files/Hewlett-Packard/CM/  
ManagementPortal/etc/Certificates/host.HP.com-prvkey.pem"  
    HTTPS_PORT "443"
```

- 4 Place the `tls.tkd` file into the `modules` directory.
- 5 Edit the `http-managementportal.rc` file so that the `tls.tkd` module is loaded before the `rmp.tkd` module, as shown below.

```
module load tls.tkd  
module load rmp.tkd
```

- 6 Restart the CM Portal.

When the CM Portal is running you can connect to it, via HTTPS, by opening a web browser and typing

```
https://server:ssl_port
```


To disable standard HTTP (leaving only HTTPS available), open the `httpd-managementportal.rc` file and in the `Overrides Config` section set `PORT` to `-1`, as in:

```
Overrides Config {  
    SSL_CERTFILE "D:/Program Files/Hewlett-Packard/CM/  
ManagementPortal/etc/Certificates/host.HP.com-cert.pem"  
    SSL_KEYFILE "D:/Program Files/Hewlett-Packard/CM/  
ManagementPortal/etc/Certificates/host.HP.com-prvkey.pem"  
    HTTPS_PORT 443  
    PORT -1
```

To add a CA Root Certificate (Public Key) for the LDAPS Server

If the server that is hosting the LDAP directory is using a CA other than Entrust, VeriSign, Inc., or G.E., obtain and place the CA root certificate on a local directory of the CM Portal host machine. Then:

- Add the contents of the public key to the top of the default `cacert.pem` file,

 In order to allow for multiple LDAPS connections, add the contents of multiple public keys to the `ca.cert.pem` file.

or

- Copy the CA root certificate file to a local directory on the CM Portal host machine.

To add a directory service connection for LDAPS

- 1 To enable the CM Portal to connect to an LDAP directory using SSL, log on to the CM Portal and navigate to **Zone** → **Configuration** → **Directory Services**.
- 2 In the Model Administration task group, click **Add Directory Service** and complete the entries that are needed for a directory service **type** of **ds-ldaps**.
- 3 Complete the Directory Service Properties for LDAPS by specifying the following.

 The URL, CA Certificate Directory, and CA Certificate File options require specific entries for an LDAPS connection.

- Specify a Common Name.
- Optionally, specify a Display Name and Description.
- Optionally, specify a Startup type.
- Select **ds-ldaps** as the Type.
- Type the URL as shown below, substituting the items in `< >` with your specific values.

```
ldaps://<LDAP_hostname_in_certificate>:<LDAP_secure_port>/  
<bind_User>@<domain>  
<LDAP_hostname_in_certificate>
```

If this value does not match the server's common name, as specified in the LDAP server's certificate, the connection will fail. Therefore, if the subject line of the certificate specifies the CN= value using the fully-qualified DNS hostname, the URL must specify the fully-qualified DNS hostname.

```
<LDAP_secure_port>
```

specifies the LDAP secure port; the default port for LDAPS is **636**.

```
<bind User>@<domain>
```

defines the user and domain that will bind to the directory service.

- Specify the Password for the bind User that is specified in the URL.
- Optionally, type a Use to specify a fully-qualified domain at which to mount the directory service. If left blank, the common name will be used to mount the directory service at the highest level.
- In the CA Certificate Directory and CA Certificate File fields, specify the local directory and the file that contain the public key for the LDAP server. The default CA Certificate file that is installed by the Certificate Generation Utility is `cacert.pem`.
- Optionally, increase the LDAP Debug Level to 5 to create an LDAP Debug Log for troubleshooting the LDAP connection. If left at the default value of 0, the LDAP Debug Log is suppressed.

For detailed information on specifying these properties, refer to the *HP OpenView Configuration Management Portal Installation and Configuration Guide*. Review the section, Specifying LDAP or LDAPS Directory Service Properties.

4 Click **Submit**.

You will be redirected to the root of your LDAP directory at the base domain that was specified in the Use field.

To Secure CM Portal-to-CM Portal Communications

After a secure CM Portal is established, the next step is to secure the client end of the connection. To do this, the public keys and the signed certificates that were previously created (for example, `ManagementPortal\etc\Certificates\fully_qualified_DNS_Hostname-cert.pem`) must be shared.

The following instructions will use the references of a *master* CM Portal which will mount a *subordinate* CM Portal.

- 1 Make a new file, `cacert.pem`, in the `CACertificates` directory of the subordinate CM Portal (`ManagementPortal\etc\CACertificates\cacert.pem`).
- 2 Open `ManagementPortal\etc\Certificates\Master-fully_qualified_DNS_Hostname-cert.pem` and from it, copy all the lines starting from (and including):

```
-----BEGIN CERTIFICATE-----
```

to

```
-----END CERTIFICATE-----
```

- 3 Paste these lines into the `cacert.pem` file that was created in Step 1.
- 4 Repeat steps 1 – 3, but copy the contents of the certificate on the subordinate CM Portal to a `cacert.pem` file on the master CM Portal.

The following file locations are for the certificate files for the master and subordinate CM Portals.

Master CM Portal

```
ManagementPortal\etc\CACertificates\cacert.pem  
ManagementPortal\etc\Certificates\Master-fully qualified  
DNS Hostname-cert.pem  
ManagementPortal\etc\Certificates\Master-fully qualified  
DNS Hostname-prvkey.pem  
ManagementPortal\etc\Certificates\Master-fully qualified  
DNS Hostname-request.pem
```

Subordinate CM Portal

```
ManagementPortal\etc\CACertificates\cacert.pem  
ManagementPortal\etc\Certificates\Subordinate-fully  
qualified DNS Hostname-cert.pem  
ManagementPortal\etc\Certificates\Subordinate-fully  
qualified DNS Hostname-prvkey.pem  
ManagementPortal\etc\Certificates\Subordinate-fully  
qualified DNS Hostname-request.pem
```

- 5 Add the references to the newly created `cacert.pem` file to the `httpd-managementportal.rc` file.

The revised configuration section will resemble the following.

```
Overrides Config {  
  
SSL_CERTFILE "ManagementPortal/etc/Certificates/Subordinate-  
fully qualified DNS Hostname-cert.pem"  
  
SSL_KEYFILE "ManagementPortal/etc/Certificates/Subordinate-  
fully qualified DNS Hostname-prvkey.pem"  
  
HTTPS_PORT 4433  
  
PORT 3466
```

```
LOG_LEVEL 3
SSL_CADIR "ManagementPortal/etc/CACertificates"
SSL_CAFILE "cacert.pem"
}
```



By setting `PORT` to `-1` the non-secure port will be disabled.

This will lock down the CM Portal non-secure port and prevent it from accepting any RMA registrations.

- 6 Add the setting `RMP_SECURE_RMP 1` to the `etc/rmp.cfg` file, as shown in the following example.

This will enable all CM Portal-to-CM Portal communications as *secure*.

```
rmp::init {
    URL /
    RMP_SECURE_RMP 1
}
```

- 7 Place the `tls.tkd` file into the `modules` directory.

Closing Steps

- After completing all of the SSL configurations, start the CM Portal.
- Add the Directory Service in the master CM Portal—specifying the subordinate CM Portal—according to the instructions in the *HP OpenView Configuration Management Portal Installation and Configuration Guide*.
- The information that is needed for mounting the subordinate CM Portal using a secure DSML connection differs from that for mounting a CM Portal with a non-secure connection in that the URL that is specified must use the HTTPS protocol and the port that is specified must be the secure port of the subordinate CM Portal.

The following is an example of an acceptable URL.

`https://subrmp:4443/proc/dsml`

where...

- **subrmp** is the *subordinate CM Portal hostname*
- **4443** is the *secure port*

CM Application Usage Manager

This section details **HTTPS** configuration procedures for CM Application Usage Manager.

This section details how to configure the CM Application Usage Manager Agent to use an SSL-secured CM Integration Server as its **collection point**. See CM Application Usage Manager Agent in a CM Environment, starting below.



The collection point is a share point—created by the CM Integration Server—from which the CM Application Usage Manager transfers usage data.

Additionally, CM Application Usage Manager Agent can run in a non-CM environment, as detailed in CM Application Usage Manager Agent in a Non-CM Environment, starting below.

CM Application Usage Manager Agent in a CM Environment

The collection point for the CM Application Usage Manager Agent to use an SSL-secured CM Integration Server in a CM environment is:

```
https://xxx.xxx.xxx.xxx:443/KB_Mgr1_Usage/
```

This can be set in the CM Admin Configuration Server Database Editor (CSDB Editor).

CM Application Usage Manager Agent in a Non-CM Environment

- 1 Stop HP OpenView CM Application Usage Manager Agent service.
- 2 In *SystemDrive*:\ProgramFiles\Hewlett-Packard\CM create a new directory called Agent.
- 3 From the Usage Manager\Agent Install\Setup\CACertificates on the Configuration Management media, copy the CACertificates folder and paste it in *SystemDrive*:\ProgramFiles\Hewlett-Packard\CM\Agent.
- 4 From IntegrationServer\etc\CACertificates\Server-*hostname.netcert.pem*, copy the lines

-----BEGIN CERTIFICATE-----

Thru

-----END CERTIFICATE-----



If you are using the CM Portal, modify the path in step 4 as follows. Replace

IntegrationServer\etc\CACertificates

with

ManagementPortal\etc\CACertificates.

- 5 On CM agent machine, open the `cacert.pem` file that is in the `CACertificates` directory and, at the end of it, paste the lines that were copied in step 3.
- 6 In the Registry, change the collection point to **`https://xxx.xxx.xxx.xxx:443/KB_Mgr1_Usage/`**.
- 7 Start the HP OpenView CM Application Usage Manager Agent service.

CM Agents

Secure (SSL) communications are supported on the following Configuration Management agents:

- HP OpenView Configuration Management Application Manager agent (CM Application Manager agent)
- HP OpenView Configuration Management Application Self-service Manager agent (CM Application Self-service Manager agent), see CM Application Self-service Manager Agent on page 51
- HP OpenView Configuration Management Inventory Manager agent (CM Inventory Manager agent)
- HP OpenView Configuration Management Patch Manager agent (CM Patch Manager agent)

To enable SSL communications with a CM Configuration Server for these CM agents, pass **SSLMGR** and **SSLPORT** with the appropriate values on a **RADSKMAN** command line, as in:

```
Radskman sslmgr=host,sslport=443
```

CM Application Self-service Manager Agent

For the CM Application Self-service Manager agent, setup **sslmanager** and **sslport** tags in the `ARGS.XML` file, as in:

```
<SSLMANAGER>localhost</SSLMANAGER>
```

```
<SSLPORT>443</SSLPORT>
```


A Troubleshooting



IMPORTANT NOTE:

Before troubleshooting SSL using the information in this section, HP recommends always checking the HP documentation web site for the latest version of this document and the 5.00 Release Notes.

To check for recent updates and to verify that you are using the most recent edition, go to http://ovweb.external.hp.com/lpe/doc_serv/.

- In the **Product** list, click the product name (**CM** *product name* (**Radia**)).
- In the **Version** list, click the version number.
- In the **OS** list, click the OS type.
- In the **Document** field, click the document title.
- To retrieve the document, click **Open** or **Download**.

Certificate Authorities

The file, `cacert.pem`, contains the CA root certificate (the public key) for the following Certificate Authorities: Entrust, VeriSign, Inc. and G.E. If you are not using one of these CAs, the CA root certificate must be obtained using one of the following methods.

CM Agents

- Obtain the certificate from your CA and substitute it for `cacert.pem` in the `CACertificates` sub-directory of the CM agent `IDMSYS` location.
- Use CM agent self-maintenance to download the certificate to the CM agent.

CM Portal (HTTPS and LDAPS)

- Obtain the certificate from your CA and substitute it for `cacert.pem` in the `/etc/CACertificates` sub-directory of the directory in which the

CM Portal is installed. If multiple CA root certificates are required, the contents of the public keys can be added at the beginning of the `cacert.pem` file.

Existing Certificate or Private Key

If the Certificate Generation Utility program is run on a CM server that already houses a version of the Certificate Generation Utility, the following message might appear.

“A certificate or private key already exists for the specified server name. Choose another server name.”

Do either of the following:

- In the Review and Password window, change the name in the text box Server to Generate For and try again. (This generates a new server certificate request for the server that is identified in this text box.)
- or
- Cancel the installation (since a server certificate request and private key already exist for this server).

SSL Port is Not Enabled

- Verify that the correct port is specified.
- Be sure that the signed certificate is set. If not, the following message will appear in the `httpd-PORT.log` on the CM Integration Server.

```
20050621 21:49:11 Warning: TLS startup failed: Certificate
"D:\Program Files\Hewlett-
Packard\CM\IntegrationServer\etc\Certificates\
server.HP.comcert.pem" not found
```

- If the port is already in use by another application, the following message will appear in the `httpd-PORT.log` on the CM Integration Server.

```
20050621 22:10:08 Warning: TLS startup failed: LAVENEL1:443
couldn't open socket: address already in use
```

B Product Name Changes

If you have used Radia in the past, and are not yet familiar with the newly rebranded HP terms and product names, Table 4 below will help you identify naming changes that have been applied to the Radia brand.

Table 4 Product Name and Term Changes

New Name/Term	Old Name/Term
CM agents	Radia clients
HP OpenView Configuration Management	Radia
HP OpenView Configuration Management Application Manager	Radia Application Manager, RAM
HP OpenView Configuration Management Application Self-service Manager	Radia Software Manager, RSM
HP OpenView Configuration Management Application Usage Manager	Radia Usage Manager, RUM
HP OpenView Configuration Management Configuration Server	Radia Configuration Server, RCS
HP OpenView Configuration Management Distributed Configuration Server	Radia Distributed Configuration Server, Radia DCS, DMA
HP OpenView Configuration Management Configuration Server Database	Radia Configuration Server Database, Radia Database
HP OpenView Configuration Management Inventory Manager	Radia Inventory Manager, RIM
HP OpenView Configuration Management Patch Manager	Radia Patch Manager, RPM
<i>No longer a stand-alone product in the Configuration Management suite.</i>	Radia Inventory Manager Server
HP OpenView Configuration Management Portal	Radia Management Portal, RMP
HP OpenView Configuration Management Policy Server	Radia Policy Manager, Radia Policy Server, RPS

New Name/Term	Old Name/Term
HP OpenView Configuration Management Messaging Server	Radia Messaging Server, RMS
HP OpenView Configuration Management Reporting Server	Radia Reporting Server
HP OpenView Configuration Management Proxy Server	Radia Proxy Server

Index

A

args.xml file, 49

C

CA. *See* Certificate Authority

CA root certificate, 53
adding, 44

CA_FILE setting, 37

cacert.pem file, 30, 34, 36, 42, 44, 45, 46, 49, 53

ca-cert.pem file, 23

cert.pem file, 24, 25, 36, 40, 41, 43, 45, 46

Certificate Authority, 13, 24

CERTIFICATE_FILE setting, 37

certificates, 13

CM Agents, 49

CM Application Self-service Manager Agent, 49

CM Application Usage Manager, 48

CM Configuration Server, 37

CM Configuration Server Database Editor, SAP
settings, 41

CM Distributed Configuration Server, 37

CM Integration Server, 38, 40, 54

HTTPS, 40

LDAPS, 40

CM Messaging Server, 34

CM Policy Server, 40

LDAPS, 42

CM Portal, 40

HTTPS, 42, 48

LDAPS, 42, 48

CM Proxy Server, 40, 41

dynamic upstream request, 41

preload, 41

Common Name, 22

D

directory service connection, adding for LDAPS, 44

Distinguished Name, 22

dmabatch.rc file, 37, 38

dynamic upstream request, CM Proxy Server, 41

E

edmprof file, 36, 37, 38

MGR_ATTACH_LIST section, 36

MGR_SSL section, 36, 38

zsslmgr setting, 37

H

httpd.rc file, 38, 40

Overrides Config section, 40

httpd-managementportal.rc file, 43, 46

Overrides Config section, 43

httpd-PORT.log, 54

HTTPS, 35, 40, 43

CM Portal, 42

HTTPS_PORT setting, 40

K

key pair, 12

KEY_FILE setting, 37

keystore.jks file, 33

L

LDAPS, 40

adding directory service connection, 44

CM Policy Server, 42

CM Portal, 42
ldaps82.dll file, 42

M

MGR_ATTACH_LIST section, 36
MGR_SSL section, 36, 38
settings, 37

N

netcert.pem file, 48

O

Overrides Config section of httpd.rc file, 40

P

PEM. *See* Private Enhanced Mail
pm.cfg file, 42
preload, CM Proxy Server, 41
Private Enhanced Mail format, 21, 37, 40
private key, 12, 15
private key file, 26
prvkey.pem file, 21, 26, 36, 40, 41, 43, 46
public key, 12, 13
adding, 44
crypto-system, 27

R

RADSKMAN, 49
request.pem file, 24, 25, 46
rmp.cfg file, 47
rmp.tkd file, 43
rms.cfg file, 34, 35
root certificate, 15

rps.cfg file, 41
rrs.cfg file, 30
RSA crypto system, description, 27

S

SAP. *See* Server Access Profile
Server Access Profile, 41
server certificate, 15
Server Certificate Request file, 24
returned, 25
signed, 25
signer.pem file, 24
SSL_CERTFILE setting, 40
SSL_KEYFILE setting, 40
SSL_PORT setting, 37
sslmanager, 49
SSLMGR, 49
sslport, 49
SSLPORT, 49

T

tls.tkd file, 35, 43, 47
troubleshooting
CA authorities, 53
CM agents, 53
CM Portal
HTTPS, 53
LDAPS, 53
existing certificate or private key, 54
SSL port not enabled, 54
truststore.jks file, 34

Z

zsslmgr setting, 37