HP OpenView Adapter for SSL Using Radia

for the AIX, HP-UX, Linux, Solaris, and Windows operating systems*

Radia Release Version: 4.2i

Software Version: 2.1.1

Installation and Configuration Guide

*Information in this guide can be used for all supported platforms except where indicated for a specific platform only.

Document Release Date: January 2006

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

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.

Documentation Updates

This manual's title page contains the following identifying information:

- Version number, which indicates the software version.
- Print date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition, visit the following URL:

http://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.

Table 1 indicates the changes that were made to this document since the last released edition.

Table 1 Document Changes

Chapter	Version	Changes
Chapter 1	2.1.1	Page 10, The section, Supported Products, has been revised.
Chapter 1	2.1.1	Page 12, Figure 1 has been updated for LDAPS.
Chapter 2	2.1.1	Page 15, In Step 5 of the Adapter for SSL installation, a new note regarding LDAPS support has been included.
Chapter 4	2.1.1	Page 29, Management Portal (LDAPS) is a new topic that details how to configure and enable the Management Portal to connect to a Directory Service using LDAPS.
Chapter 4	2.1.1	Page 38, The section, CA Authorities, has a new sub-section, Management Portal (HTTPS and LDAPS), which details the placement of the CA Authority's certificate.

Support

Please visit the HP OpenView support web site at:

http://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 valuable 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:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

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

Contents

1 Introduction

At the end of this chapter, you will:

- Be familiar with the cipher suite that is used by the HP OpenView Adapter for SSL Using Radia (Adapter for SSL).
- Be aware of the issues when using a Radia client, version 1.0, with version 2.0 of the Adapter for SSL.
- Be familiar with the products that can be used in conjunction with the Adapter for SSL.
- Be familiar with the Adapter for SSL pre-installation requirements.
- Have had the chance to review the various communications relationships that are possible in an HP OpenView Using Radia environment.

Overview

This document describes how to install and configure the HP OpenView Adapter for SSL Using Radia (Adapter for SSL) to support SSL and HTTPS communications between Radia servers and the Radia client. HP OpenView Using Radia 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.

Important Upgrade Information

Radia clients that are using the Adapter for SSL, version 1.0 will reject a certificate from an Adapter for SSL, version 2.0-enabled server, and the client will abort the secure client connection. Therefore, Radia clients must be upgraded to Adapter for SSL, version 2.0 before the servers are upgraded.

The Adapter for SSL installation copies the files that are necessary to support SSL communications, and collects data to generate a **certificate request** and a **private key**, and then creates the appropriate files.

Supported Products

The following is a list of products in the HP OpenView Using Radia suite that can be used in conjunction with the Adapter for SSL.

For this version of the Adapter for SSL, these products must be at the *minimum* version levels that are documented in this section.

- HP OpenView Application Manager Using Radia (Application Manager), version 4.0 and greater
- HP OpenView Inventory Manager Using Radia (Inventory Manager), version 4.0 and greater
- HP OpenView Software Manager Using Radia (Software Manager), version 4.0 and greater
- HP OpenView Patch Manager Using Radia (Patch Manager), version 2.0 and greater
- HP OpenView Configuration Server Using Radia (Configuration Server), version 4.5.4 and greater

- HP OpenView Proxy Server Using Radia (Proxy Server), version 2.0 and greater
- HP OpenView Policy Server Using Radia (Policy Server), version 4.0 and greater
- HP OpenView Management Portal Using Radia (Management Portal), version 2.0.1 and greater to enable HTTPS; version 2.1.1 and greater to enable LDAPS
- HP OpenView Messaging Server Using Radia (Messaging Server), version 3.1 and greater
- HP OpenView Distributed Configuration Server Using Radia (Distributed Configuration Server), version 4.6 only.

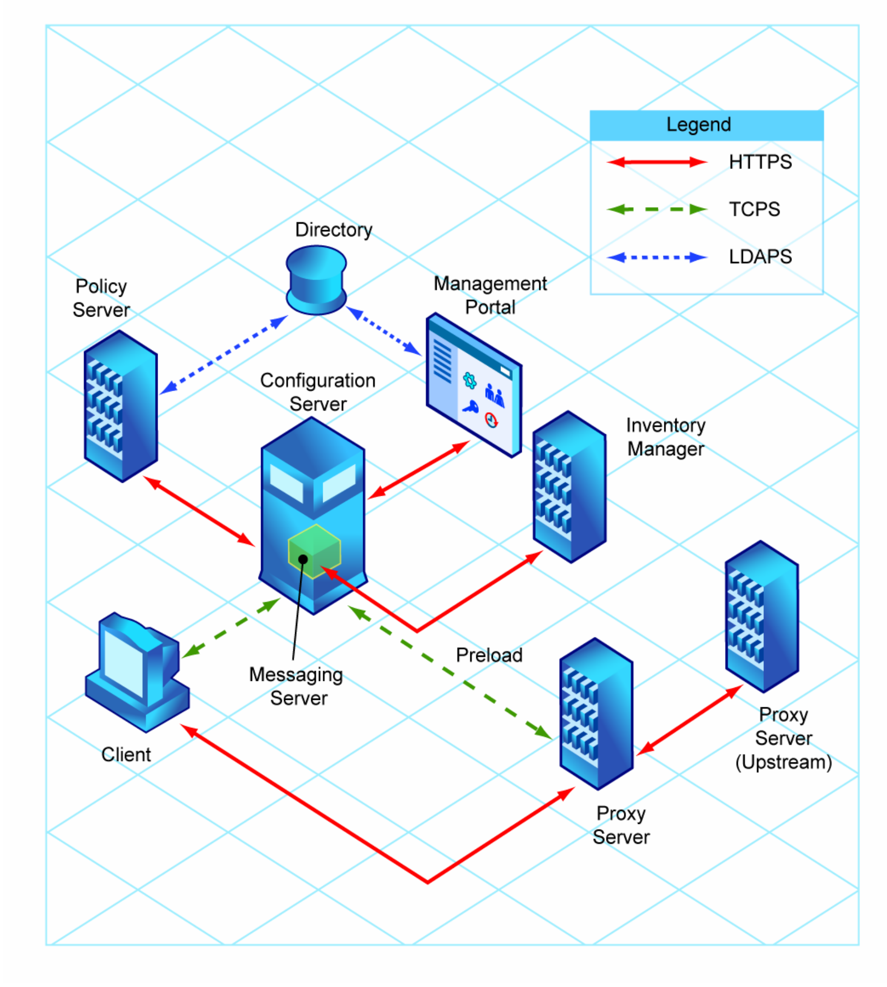
Requirements and Prerequisites

- You must be licensed for SSL.
- Radia clients and servers must have a **Certificate Authority** (**CA**) root certificate.
- Radia servers must have a **server certificate** and a **private key**.

Communications in an HP OpenView Using Radia Environment

Figure 1 below presents an overview of the various types of communications and relationships that are possible in an HP OpenView Using Radia environment.

Figure 1 Communications Overview



2 Installing the Adapter for SSL

At the end of this chapter, you will have:

- Installed the HP OpenView Adapter for SSL Using Radia (Adapter for SSL) and:
  - Selected to (optionally) enable SSL support for:
    - Infrastructure Server components
    - Configuration Server components
    - Messaging Server components
  - Chosen whether to generate a new certificate request or use an existing certificate

Adapter for SSL Installation

The Adapter for SSL must be installed on each Radia server that is to be configured for SSL communications.

Installing the Adapter for SSL

This section documents the installation of the Adapter for SSL.

To install the Adapter for SSL

1. If the Radia server is running, shut it down.
2. Insert the HP OpenView Management Solutions Radia 4.2 Infrastructure CD into the CD-ROM drive, and navigate to

   `\managementextensions\adapter_for_ssl\`*`operatingsystem`*

   where *`operatingsystem`* is the operating system on which the Adapter for SSL is being installed.

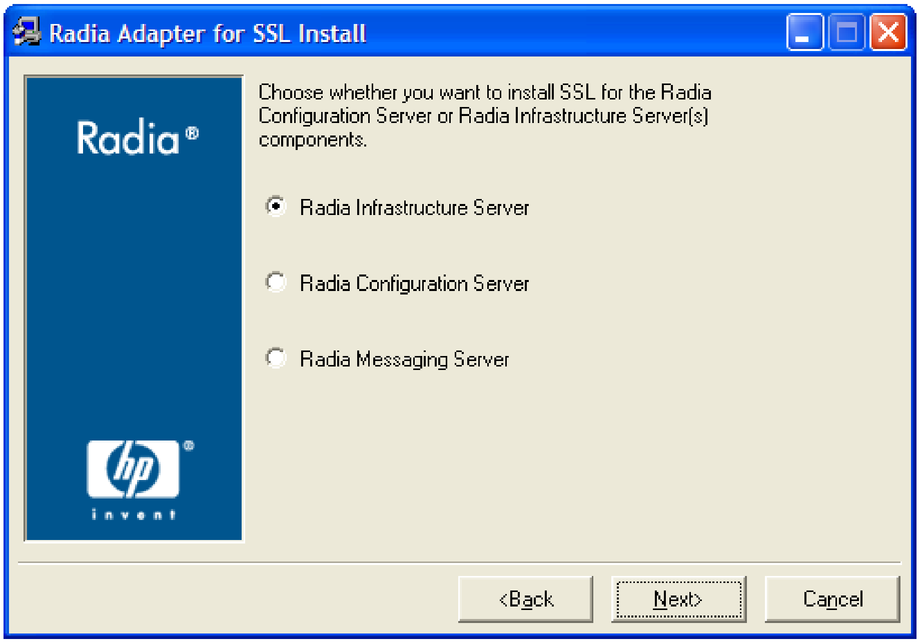
   — For Windows, double-click `setup.exe`.

   — For UNIX, use the file `./install`.

   The Welcome window opens.
3. Click **Next**.

   The End User Licensing Agreement opens.
4. Review the terms and click **Accept**.

   The Components Selection window opens.



Choose whether you want to install SSL for the Radia Configuration Server or Radia Infrastructure Server(s) components.

● Radia Infrastructure Server

○ Radia Configuration Server

○ Radia Messaging Server

In this window:

5 Select either of the following components for which SSL support is to be enabled.

- Select **Radia Infrastructure Server** to enable all Integration Server-based components to accept a secure connection. The Infrastructure Server components are:
  - Management Portal
  - Policy Server
  - Inventory Manager server
  - Proxy Server

  Selecting Radia Infrastructure Server on a machine that is hosting the Management Portal enables secure-LDAP (LDAPS) directory connections.

- Select **Radia Configuration Server** to enable the Configuration Server for SSL support.
- Select **Radia Messaging Server** to enable the Messaging Server for SSL support.

6 Click **Next**.

If Radia Infrastructure Server is selected, SSL will be enabled for the Integration Server (HTTPS), and the following additional options can be selected.

— Enable secure Policy Server directory connection

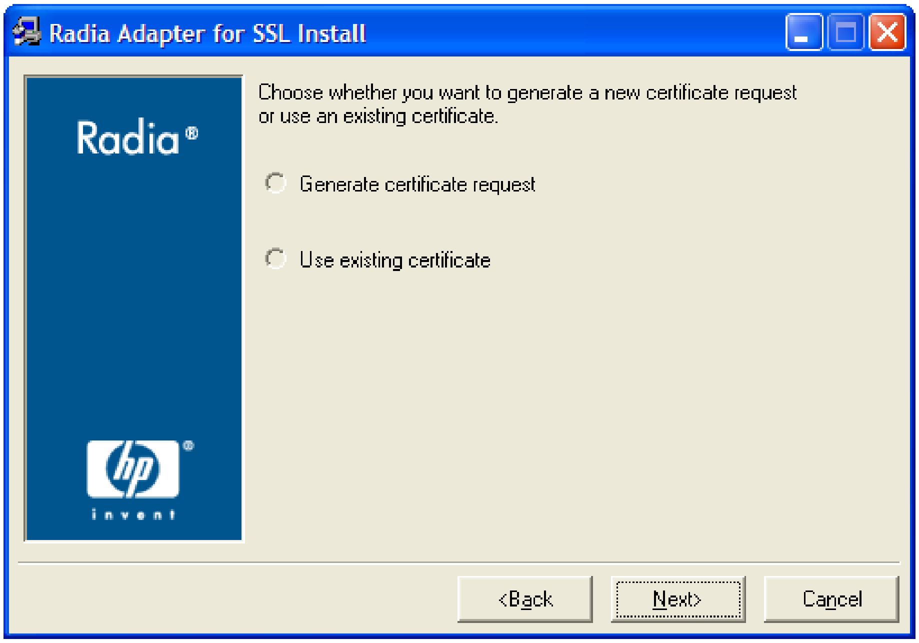
— Enable Secure Radia Proxy Server preload

If Radia Configuration Server had been selected the following options would have been available:

- Enable secure policy methods to enable secure HTTPS transactions
- Enable secure inventory methods (to enable secure HTTPS transactions)
- Enable secure portal methods (to enable secure HTTPS transactions)
- Enable secure RCS TCP task (Configuration Server TCP task)

7 Click **Next**.

The Certificate Selection window opens.



Choose whether you want to generate a new certificate request or use an existing certificate.

○ Generate certificate request

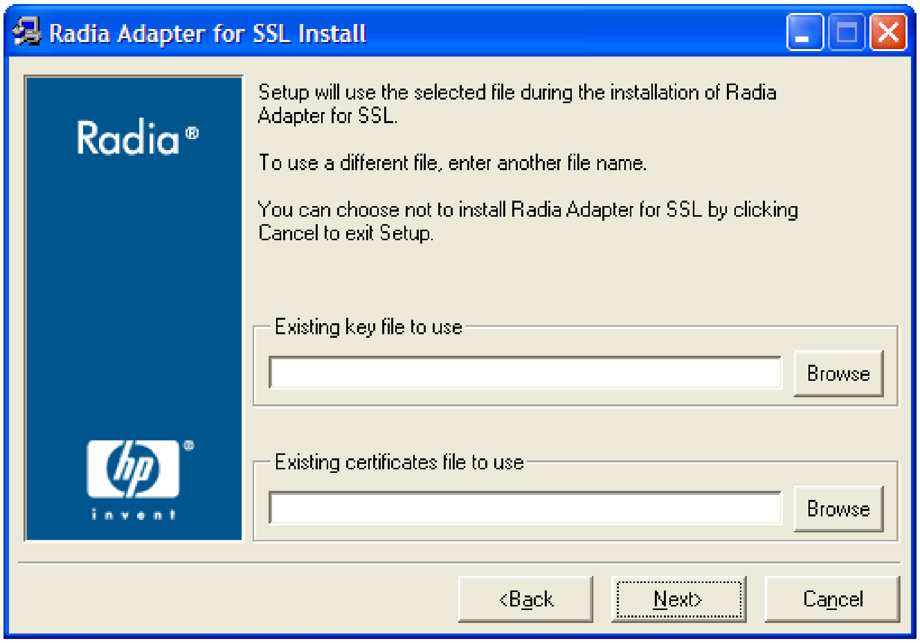
○ Use existing certificate

In this window:

8 Select whether to generate a new certificate request or to use an existing certificate, and click **Next**.

If Generate certificate request is chosen, skip to step 9 on page 18.

If Use existing certificate is chosen, specify the location for the existing key file and certificates file.



Setup will use the selected file during the installation of Radia Adapter for SSL.

To use a different file, enter another file name.

You can choose not to install Radia Adapter for SSL by clicking Cancel to exit Setup.

a Click **Next**.

Specify where the Adapter for SSL is to be installed.

- If the location displayed in the RCS Configuration File Location field is correct, click **Next**. Otherwise,
- Specify the correct location, or click **Browse** to navigate to the license file.

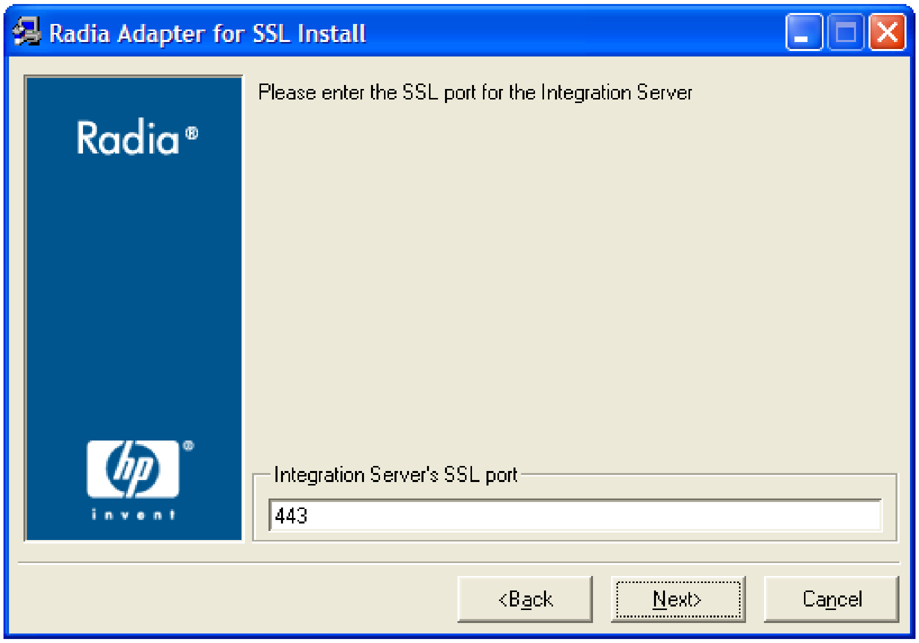
b Click **Next**.

A message indicates that the selected directory will be updated. The location might vary based on the components that were selected in step 5.

c Click **OK** to continue with Step 11 on page 18.

9 If Generate certificate request was chosen at step 8, you will be prompted to specify where you want to place the new key file and certificates file.

If the Infrastructure Server option was selected in step 4, the Integration Server's SSL Port window opens.



Please enter the SSL port for the Integration Server

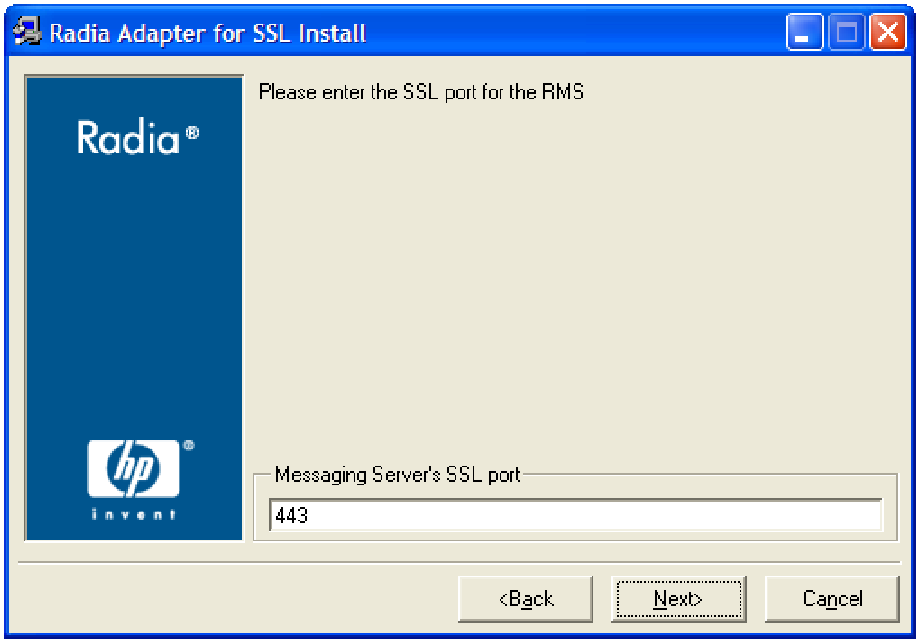
Integration Server's SSL port

443

10 Specify the SSL port (the default is **443**) on which the Radia components should listen for requests.

Click **Next**.

If the Messaging Server option was selected, the Messaging Server's SSL Port window opens.



Please enter the SSL port for the RMS

Messaging Server's SSL port

443

11 Click **Next**.

The next six windows request environment-specific server-certificate and private-key information:

- Company
- Department
- Country Code
- State/Province
- City
- Fully Qualified Host Name of the Server Domain

12 Specify the requested information and click **Next**.

The Summary window opens.

This window presents all the information that was specified during the Adapter for SSL installation. This is the final opportunity to review and modify the specified settings.

- If you discover any errors, or wish to modify any of the entries, click **Back** until you reach the appropriate windows, and make the necessary changes.

The information that was entered in the other windows will not be affected. After making the changes, click **Next** repeatedly, until you arrive back at the Summary window.

13 Click **Install**.

The files that are needed to support SSL communications are copied. This takes only a few moments and progress bars display activity as it occurs.

When the files have been copied, the Review window opens.

14 Review the data that will be used to generate the server certificate request and private key, and click **Next**.

The installation program will take a few moments to generate the server certificate request and private key. When it's finished, a confirmation message appears.

15 Click **OK**.

Send the identified server certificate request to your CA authority. Follow its instructions for having the server certificate request signed and returned to you. Store the signed server certificate request in the appropriate (operating system-specific) Configuration Server directory:

`bin\Certificates\requests` (Windows) or
`exe/Certificates/requests` (UNIX).

The Installation Successful window opens.

16 Click **Finish**.

The Adapter for SSL is successfully installed.

To enable SSL, the Configuration Server or the Integration Server component must be re-started.

3 Certificate Authority Files

At the end of this chapter, you will:

- Have the Server Certificate Request File signed and returned.
- Renamed the (signed and returned) Server Certificate Request File and place it in the proper directory.
- Know more about the Private Key File.

The Server Certificate Request File

The HP OpenView Adapter for SSL Using Radia (Adapter for SSL) installation program generates a **server certificate request file**, for example,

`host.HP.comcert.pem`.

To have the server certificate request signed and returned, follow the procedure that is required by your public **Certificate Authority** (**CA**). Typically, the server certificate request 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.

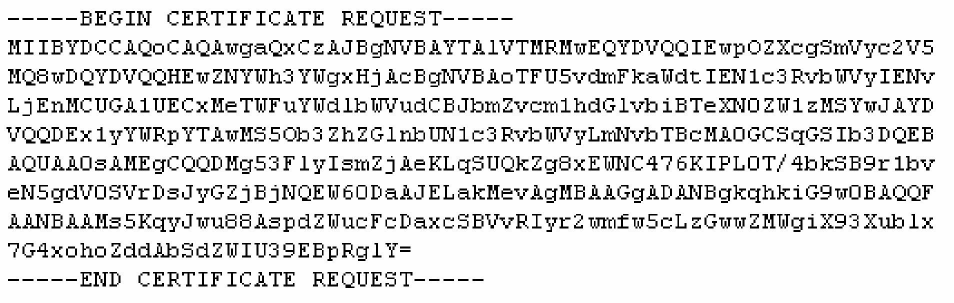
To issue a signed certificate, the CA signing authority will also require proof-of-identity and authority—such as your company's DUNS number, Articles of Incorporation, Partnership Papers, or Business License.

➤ 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 Server Using Radia (Configuration Server) the server certificate request file is located in:
  - `bin\Certificates\requests` (Windows)
  - `exe/Certificates/requests` (UNIX).
- For the HP OpenView Integration Server Using Radia (Integration Server) the server certificate request file is located in:
  - `\etc\Certificates` (Windows)
  - `exe/Certificates` (UNIX).

If the server certificate request 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 opened with a text editor



```
-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCCAQoCAQAwgaQxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpOZXcgSmVyc2V5
MQ8wDQYDVQQHEwZNYWh3YWgxHjAcBgNVBAoTFU5vdmFkaWdtIEN1c3RvbWVyIENv
LjEnMCUGA1UECxMeTWFuYWdlbWVudCBJbmZvcm1hdGlvbiBTeXNOZW1zMSYwJAYD
VQQDEx1yYWRpYTAwMS5Ob3ZhZGlnbUN1c3RvbWVyLmNvbTBcMAOGCSqGSIb3DQEB
AQUAAOsAMEgCQQDMg53FlyIsmZjAeKLqSUQkZg8xEWNC476KIPLOT/4bkSB9r1bv
eN5gdVOSVrDsJyGZjBjNQEW6ODaAJELakMevAgMBAAGgADANBgkqhkiG9wOBAQQF
AANBAAMs5KqyJwu88AspdZWucFcDaxcSBVvRIyr2wmfw5cLzGwwZMWgiX93Xublx
7G4xohoZddAbSdZWIU39EBpRglY=
-----END CERTIFICATE REQUEST-----
```

The Signed Server Certificate Request File

When the signed server certificate request file is returned from the public CA:

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

    `host.HP.comreq.pem`

    to

    `host.HP.comcert.pem`.

    The server certificate request file might have a different name when it is returned from the CA.

2 Place the renamed certificate request file (`host.HP.comcert.pem`) in the appropriate folder, as below.

    — For the Configuration Server, place the file in:

        `bin\Certificates` (Windows)

        `exe/Certificates` (UNIX).

    — For the Integration Server, place the file in:

        `\etc\Certificates` (Windows)

        `exe/Certificates` (UNIX).

3 Restart the Configuration Server or 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

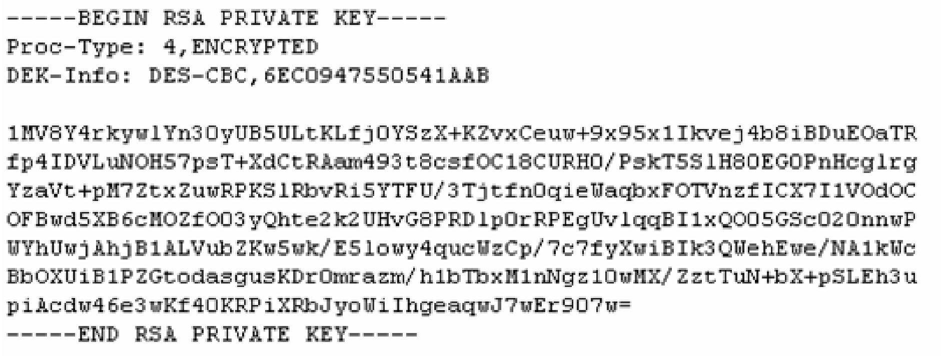
The installation program also generates a **private key file**, for example,

`host.HP.comprvk.pem`.

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

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

Figure 3 Private key file opened with a text editor



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

1MV8Y4rkyw1Yn3OyUB5ULtKLfjOYSzX+KZvxCeuw+9x95x1Ikvej4b8iBDuEOaTR
fp4IDVLuNOH57psT+XdCtRAam493t8csfOC18CURHO/PskT5S1H8OEGOPnHcglrg
YzaVt+pM7ZtxZuwRPKS1RbvRi5YTFU/3TjtfnOqieWaqbxFOTVnzfICX7I1VOdOC
OFBwd5XB6cMOZfO03yQhte2k2UHvG8PRD1pOrRPEgUv1qqBI1xQO05GSc02OnnwP
WYhUwjAhjB1ALVubZKw5wk/E5lowy4qucWzCp/7c7fyXwiBIk3QWehEwe/NA1kWc
BbOXUiB1PZGtodasgusKDrOmrazm/h1bTbxM1nNgz10wMX/ZztTuN+bX+pSLEh3u
piAcdw46e3wKf40KRPiXRbJyoWiIhgeaqwJ7wEr907w=
-----END RSA PRIVATE KEY-----
```

In order to maintain compatibility with current 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 file shown above the key type (**RSA**) is indicated at the beginning and end of the file.

4 Configuration and Use

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

- Configure SSL for Configuration Server connections (TCPS).
- Configure SSL for Configuration Server methods (RADISH).
- Configure SSL for the Integration Server components:
  - Management Portal (HTTPS and LDAPS)
  - Proxy Server (HTTPS, SSL for preload, and upstream request)
  - Inventory Manager (HTTPS)
  - Policy Server (HTTPS and LDAPS)
- Configure SSL for the Messaging Server.
- Setup a Radia client to use SSL.

Configuration Server (TCPS)

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

- The MGR_ATTACH_LIST section has been revised and now contains the `zsslmgr CMD_LINE`, as shown:

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

- The MGR_SSL section has been added, as shown:

```
[MGR_SSL]
CA_FILE = C:/Novadigm/ConfigurationServer/bin/CACertificates/
cacert.pem
CERTIFICATE_FILE = C:/Novadigm/ConfigurationServer/bin/
Certificates/host.HP.comcert.pem
KEY_FILE = C:/Novadigm/ConfigurationServer/bin/Certificates/
host.HP.comprvk.pem
SSL_PORT = 443
```

The following table describes the 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 Radia 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.

Setting	Usage
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.

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

- The MGR_SSL section has been added, as shown:

```
[MGR_POLICY]
HTTP_HOST = Policy_host
HTTP_PORT =
USE_HTTPS = 1
HTTPS_PORT = 443

[MGR_RIM]
HTTP_HOST = rim_host
HTTP_PORT =
USE_HTTPS = 1
HTTPS_PORT = 443

[MGR_RMP]
HTTP_HOST = rmp_host
HTTP_PORT =
USE_HTTPS = 1
HTTPS_PORT = 443
```

Integration Server (HTTPS & LDAPS): Management Portal, Proxy Server, Inventory Manager, Policy Server

To confirm that the Integration Server is configured for SSL support, 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 D:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comcert.pem
SSL_KEYFILE D:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comprvk.pem
HTTPS_PORT 443
```

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

Table 2 Overrides Config section Settings

Setting	Usage
SSL_CERTFILE	This setting is used to identify and locate the server certificate of the Radia 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 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:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comcert.pem
SSL_KEYFILE D:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comprvk.pem
HTTPS_PORT 443
PORT -1
```

Upgrading an Integration Server

If version 2.1 of the Adapter for SSL was installed on an Integration Server, follow the steps below to upgrade to version 2.1.1.

➤ To obtain LDAPS support on a Management Portal, it must be at version 2.1.1.

1 Stop the Integration Server service (`httpd`).

2 Remove any copies of `ldap82.dll` from the `IntegrationServer` directory and/or its subdirectories. (This ensures the use of the latest version of `ldaps82.dll` that is packed inside of `tls.tkd`.)

3 Replace the `tls.tkd` that is in the `IntegrationServer\modules` directory with the version that is in

`\management_extensions\adapter_for_ssl\infra\`

on the Radia 4.2 media.

4 Restart the Integration Server service (`httpd`).

To configure the new LDAPS support, see the next section, Management Portal (LDAPS).

Management Portal (LDAPS)

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

1. The ldaps82.dll is in the root IntegrationServer directory.

   The ldaps82.dll file is unpacked by the Adapter for SSL module tls.tkd when the Management Portal service starts. If ldaps82.dll is missing, stop the Management Portal service, delete any existing ldap82.dll file in the IntegrationServer directories or path, and restart the Management Portal service.

2. A CA Certificate file containing the LDAP server's CA root certificate (public key) is in a local directory on the Management Portal.

   The Adapter for SSL installs a default CA Certificate file, cacert.pem, which includes the public keys for Entrust, VeriSign, and G.E, and is located in C:/Novadigm/IntegrationServer/etc/CACertficates.

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

If the server that is hosting the LDAP directory is using a certificate authority other than Entrust, VeriSign, or G.E., obtain and place the CA root certificate on a local directory of the Management 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 cacert.pem file.

  or

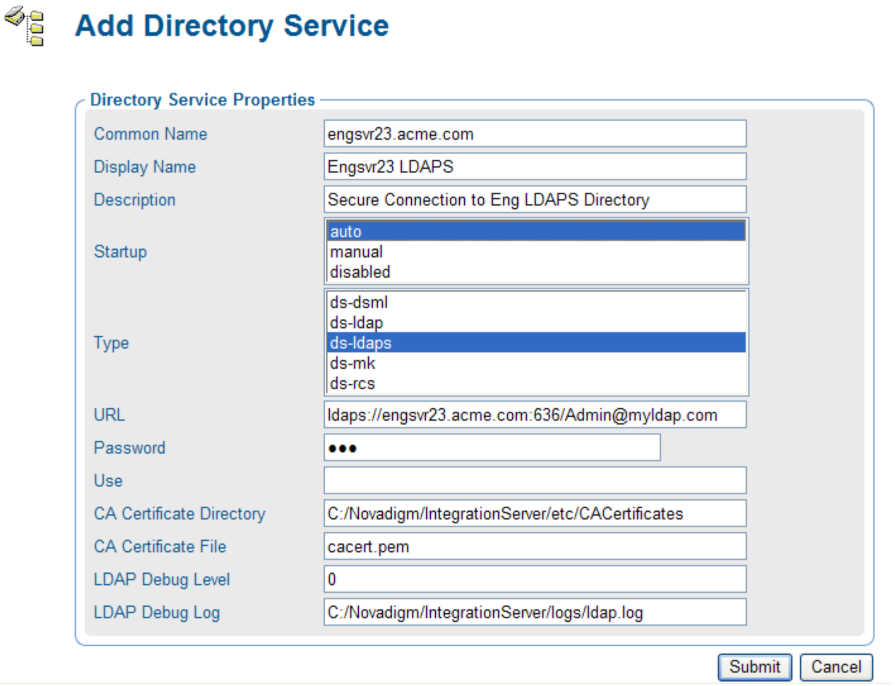
- Copy the CA root certificate file to a local directory on the Management Portal host machine.

To add a directory service connection for LDAPS

1. To enable the Management Portal to connect to an LDAP directory using SSL, log on to the Management 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-lsaps**.

   The following figure shows sample entries for adding an LDAPS Directory Service.



Add Directory Service

Directory Service Properties

Common Name	engsvr23.acme.com
Display Name	Engsvr23 LDAPS
Description	Secure Connection to Eng LDAPS Directory
Startup	[✓ auto] manual disabled
Type	ds-dsml ds-ldap [✓ ds-ldaps] ds-mk ds-rcs
URL	ldaps://engsvr23.acme.com:636/Admin@myldap.com
Password	●●●
Use	
CA Certificate Directory	C:/Novadigm/IntegrationServer/etc/CACertificates
CA Certificate File	cacert.pem
LDAP Debug Level	0
LDAP Debug Log	C:/Novadigm/IntegrationServer/logs/ldap.log

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 doesn't 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>
Specify the LDAP secure port; the default LDAPS port 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 Adapter for SSL 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 *Installation and Configuration Guide for the HP OpenView Management Portal Using Radia.* 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.

Proxy Server Preload

To confirm that the Proxy Server preload 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
```

Proxy Server Upstream Request

To confirm that the 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
```

Policy Server (LDAPS)

To confirm that Policy Server LDAP is configured for SSL (LDAPS) support, use a text editor to open the `rpm.cfg` file, which is located in the `IntegrationServer` directory, and confirm that it has the following settings.

```
dap::init {
   TYPE   ldaps
   ...
```

Messaging Server

To confirm that the Messaging Server is configured for SSL support, use a text editor to open the `rms.cfg` file, which is located in the `MessagingServer\etc` directory, and confirm that it has the following settings.

```
package require nvd.httpd
Overrides Config {
SSL_CERTFILE D:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comcert.pem
SSL_KEYFILE D:\Novadigm\IntegrationServer\etc\Certificates\
host.HP.comprvk.pem
HTTPS_PORT 443
}
```

To enable SSL for the Messaging Server receiver, update the `rms.cfg` file as described below:

```
msg::register httpd {
   TYPE   HTTPD
   PORT   3461
   HTTPS_PORT   443
  }
```

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 Messaging Server environment.

```
msg::register secure1 {
   TYPE   HTTPS

   ADDRESS  {
     PRI  10
     URL  https://localhost:443/proc/inventory
   }
}
```

Radia Clients (RADSKMAN)

SSL is supported on:

- HP OpenView Application Manager Using Radia (Application Manager),
- HP OpenView Inventory Manager Using Radia (Inventory Manager),
- HP OpenView Software Manager Using Radia (Software Manager),
- HP OpenView Patch Manager Using Radia (Patch Manager)

To enable SSL communication with a Configuration Server for Radia clients, pass SSLMGR and SSLPORT on a RADSKMAN command line, as in:

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

Software Manager

For the Software Manager, setup sslmanager and sslport tags in the `ARGS.XML` file, as in:

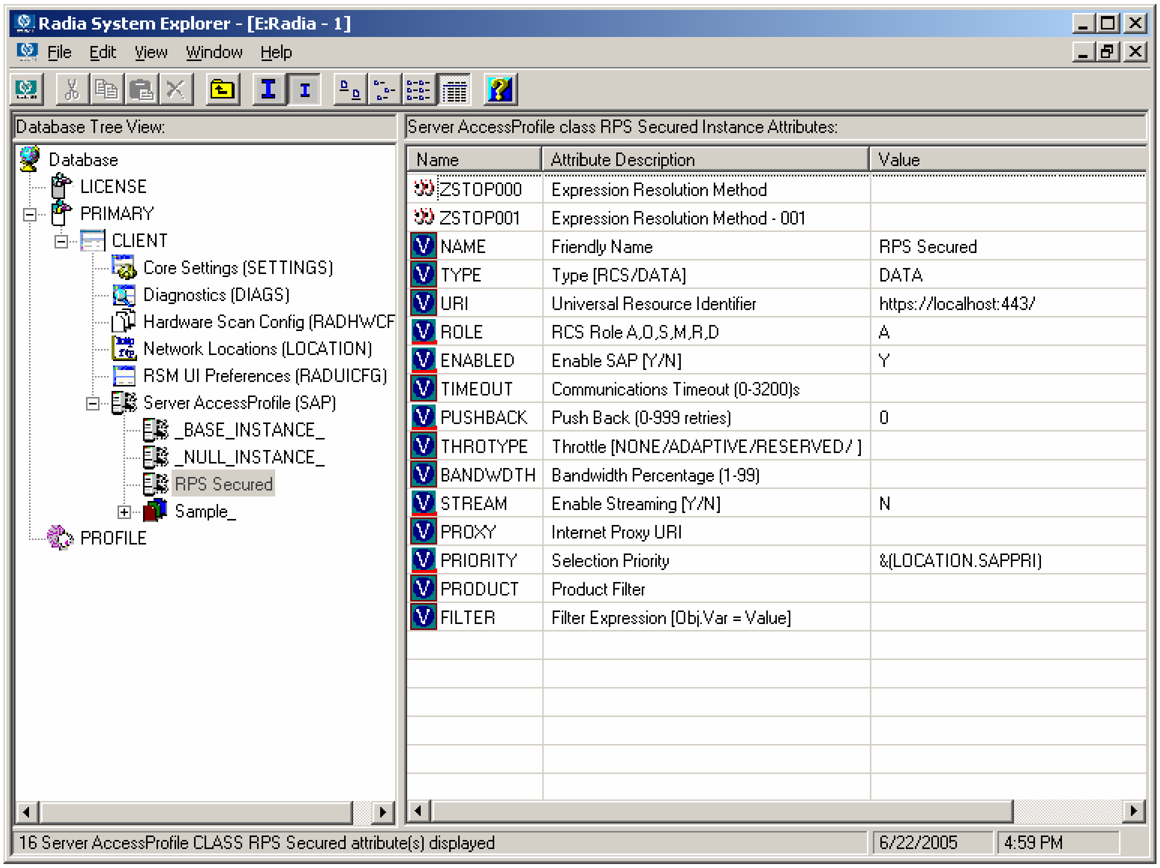
```
<SSLMANAGER>localhost</SSLMANAGER>

<SSLPORT>443</SSLPORT>
```

Proxy Server

To enable SSL communication with a Proxy Server, set up a Service Access Point (SAP) in Radia database via the HP OpenView System Explorer Using Radia (System Explorer), as shown in the following figure.

Figure 4 Enable SAP setting in System Explorer



Server AccessProfile class RPS Secured Instance Attributes:

Name	Attribute Description	Value
ZSTOP000	Expression Resolution Method	
ZSTOP001	Expression Resolution Method - 001	
NAME	Friendly Name	RPS Secured
TYPE	Type [RCS/DATA]	DATA
URI	Universal Resource Identifier	https://localhost:443/
ROLE	RCS Role A,O,S,M,R,D	A
ENABLED	Enable SAP [Y/N]	Y
TIMEOUT	Communications Timeout (0-3200)s	
PUSHBACK	Push Back (0-999 retries)	0
THROTYPE	Throttle [NONE/ADAPTIVE/RESERVED/]	
BANDWDTH	Bandwidth Percentage (1-99)	
STREAM	Enable Streaming [Y/N]	N
PROXY	Internet Proxy URI	
PRIORITY	Selection Priority	&(LOCATION.SAPPRI)
PRODUCT	Product Filter	
FILTER	Filter Expression [Obj.Var = Value]	

16 Server AccessProfile CLASS RPS Secured attribute(s) displayed | 6/22/2005 | 4:59 PM

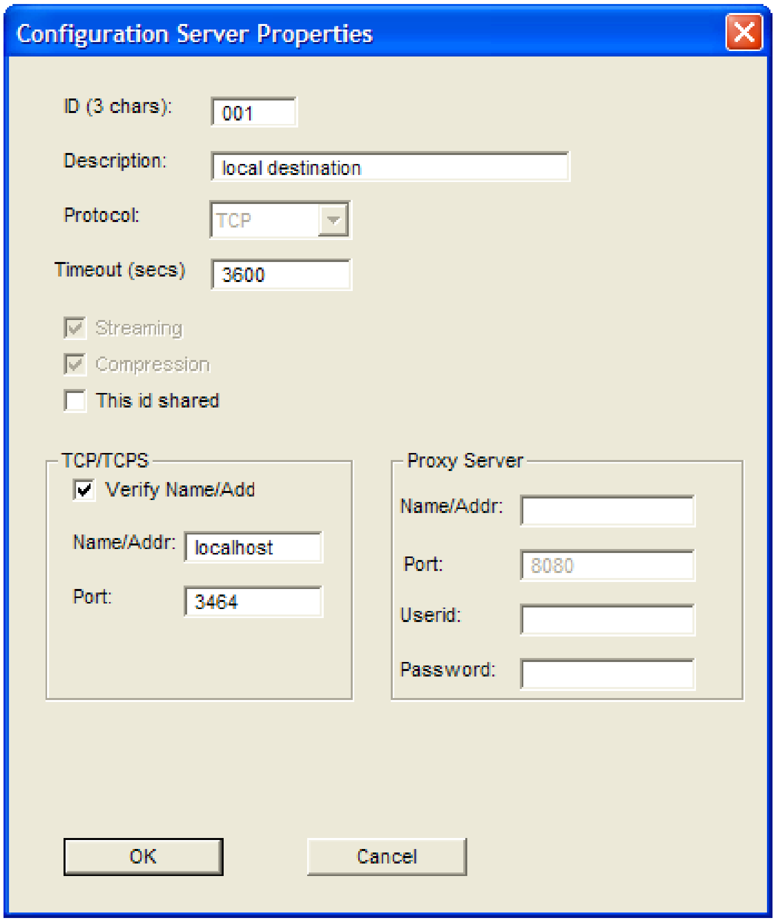
For more information on configuring Radia clients, refer to the HP OpenView Using Radia documentation.

Distributed Configuration Server

SSL support is provided only in the version 4.6 release of Distributed Configuration Server.

To specify SSL for the Configuration Servers in Distributed Configuration Server, open the Configuration Server Properties window (Figure 5) in the Distributed Configuration Server configuration panel, and set SSL as the Protocol.

Figure 5 Configuration Server Properties window



Configuration Server Properties

ID (3 chars): 001

Description: local destination

Protocol: TCP

Timeout (secs) 3600

☑ Streaming

☑ Compression

□ This id shared

TCP/TCPS

☑ Verify Name/Add

Name/Addr: localhost

Port: 3464

Proxy Server

Name/Addr:

Port: 8080

Userid:

Password:

Troubleshooting

Logs

The Adapter for SSL installation program creates a log file, `setup.log`, in the folder `TEMP\SETUP` (Windows), and `$HOME/tmp/setup.log` (UNIX).

CA Authorities

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

Radia Clients

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

Detailed instructions for packaging and deploying Radia client self-maintenance can be found on the HP OpenView web site.

Management Portal (HTTPS and LDAPS)

- Obtain the certificate from your CA authority and substitute it for `cacert.pem` in the `/etc/CACertificates` sub-directory of where the Management Portal is installed. If multiple CA root certificates are required, the contents of the public keys can be added to the top of the `cacert.pem` file.

Existing Certificate or Private Key

If the Adapter for SSL installation program is run on a Radia server that already houses a version of the Adapter for SSL, 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 Integration Server.

  ```
  20050621 21:49:11 Warning: TLS startup failed: Certificate
  "D:/Novadigm/IntegrationServer/etc/Certificates/server.HP.comc
  ert.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 Integration Server.

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

Index