

HP OpenView Adapter for SSL Using Radia

Radia SSL Adapter Guide

Software Version: 2.0

for the UNIX and Windows operating systems



Manufacturing Part Number: T3424-90064

August 2004

© Copyright 2004 Hewlett-Packard Development Company, L.P.

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 1998-2004 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.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Acknowledgements

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

Technical Support

Please select Support & Services from the following web site:

<http://www.hp.com/managementsoftware/services>

There you will find contact information and details about the products, services, and support that HP OpenView offers.

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Introduction	7
Requirements/Prerequisites	7
About the Server Certificate Request File	19
Signing the Server Certificate Request	19
About the Private Key File	20
Confirming the Installation	21
Radia Configuration Server	21
Radia Integration Server	22
Troubleshooting	23

Introduction

This document describes how to install and configure the Radia Adapter for SSL to support SSL and HTTPS communications between Radia Servers and the Radia Client. 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 using the SSL adapter 1.0 will reject the certificate from an SSL adapter 2.0-enabled server and abort the secure client connection. Therefore, you must upgrade your clients to SSL adapter 2.0 *before* upgrading your servers.

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

Requirements/Prerequisites

- License strings must be SSL-enabled. If the license string is not SSL-enabled, contact Product Fulfillment for a new set of license strings.
- Radia Clients and Radia Servers must have a Certificate Authority (CA) root certificate.
- Radia Servers must have a server certificate and a private key.
- Radia Client version 3.0 or higher
- Radia Integration Server build 69

Installing the Radia Adapter for SSL

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

To install the Radia Adapter for SSL

1. If the Radia Server is running, shut it down.
2. Insert the Radia Adapter for SSL CD-ROM into the CD-ROM drive, and go to `\managementExtensions\adapter_for_ssl\operatingsystem`.
 - For Windows, double-click **setup.exe**.
 - For UNIX, use the file **.install**.

The **Welcome** window opens.



Figure 1 ~ The Welcome window.

3. Click **Next**.
The **End User Licensing Agreement** opens.

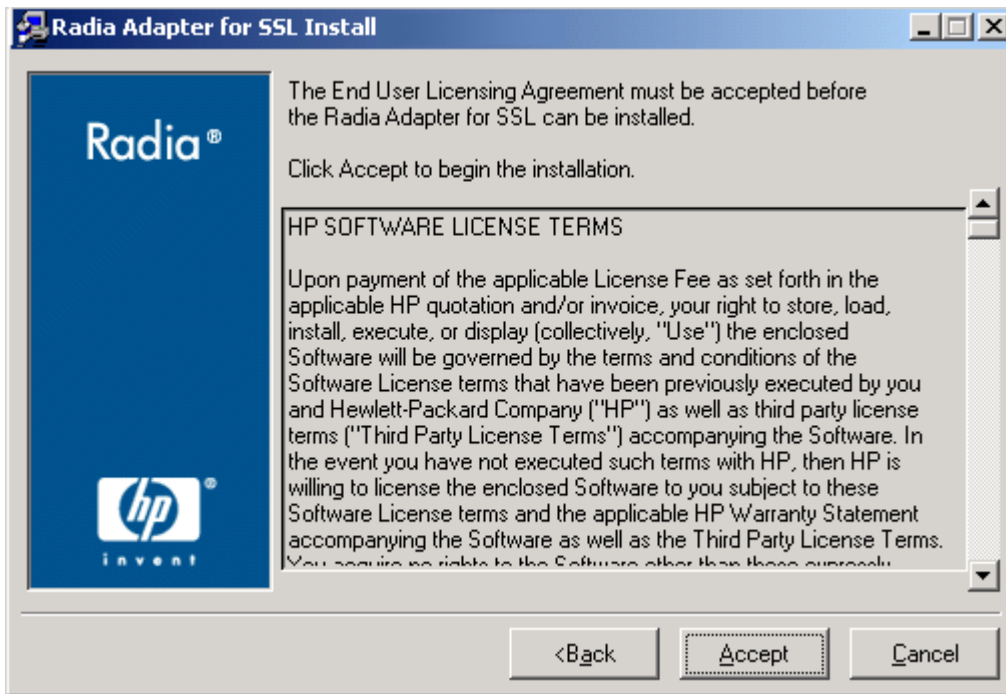


Figure 2 ~ End User Licensing Agreement window.

4. Review the terms and click **Accept**.
The **Product Selection** window opens.

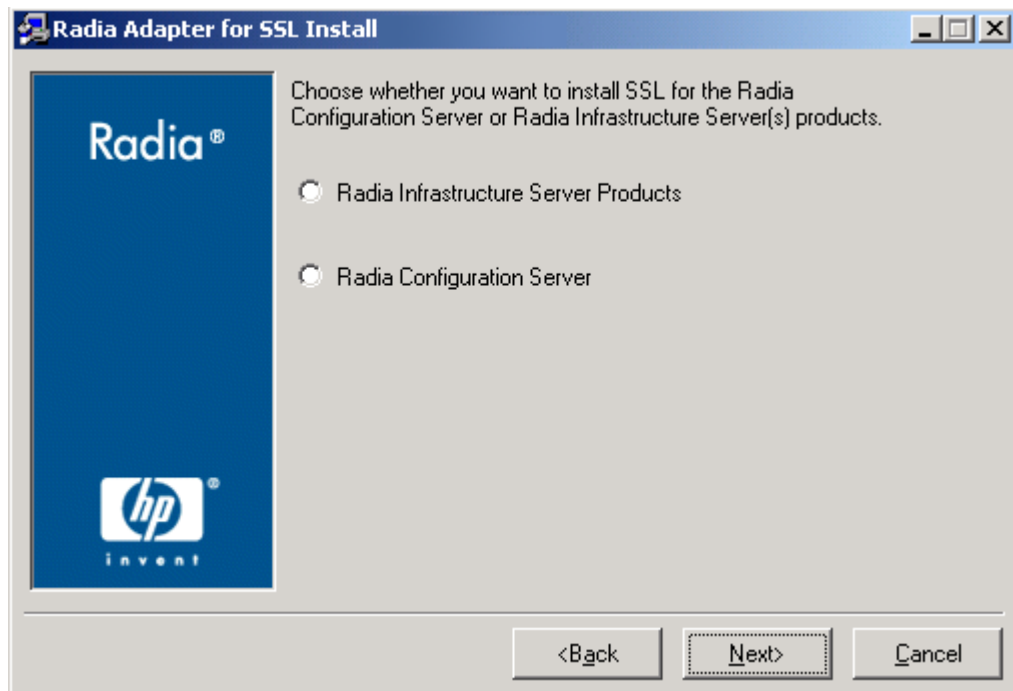


Figure 3 ~ Product selection window.

5. Select the product for which you want to enable SSL.
 - Select **Radia Infrastructure Server Products** to configure all RIS-based products to accept a secure connection.
 - Select **Radia Configuration Server** to configure the RCS for SSL support.
6. Click **Next**.

If you selected **Radia Infrastructure Server Products** you can select the following options:

 - **Enable secure Policy Server directory connection.**
 - **Enable secure RPS preload.**

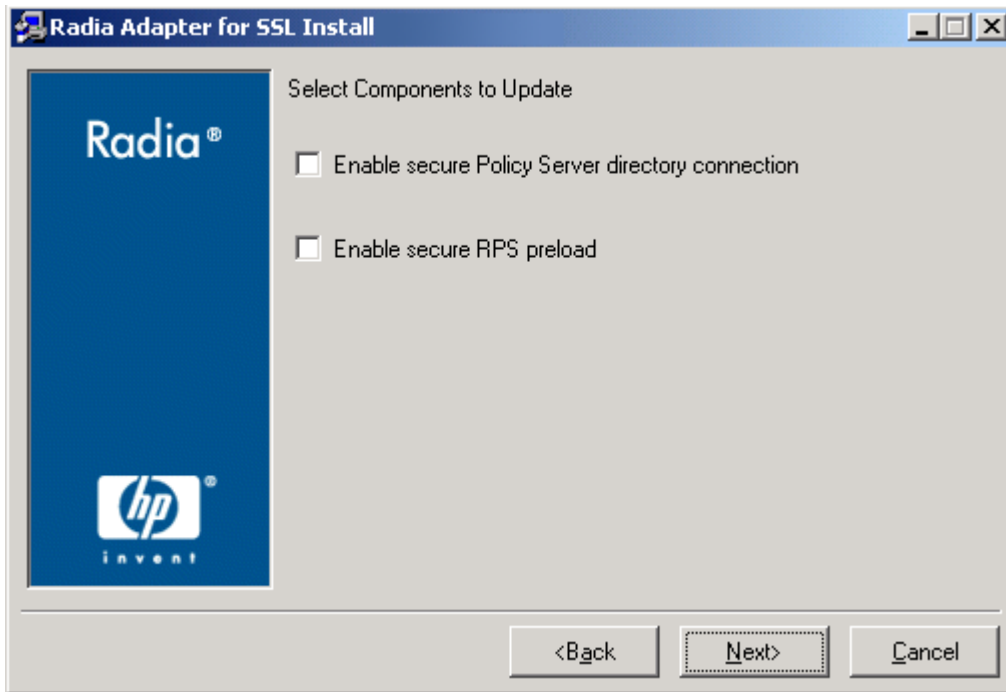


Figure 4 ~ RIS components to update.

If you selected **Radia Configuration Server** you can select the following options:

- **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.**

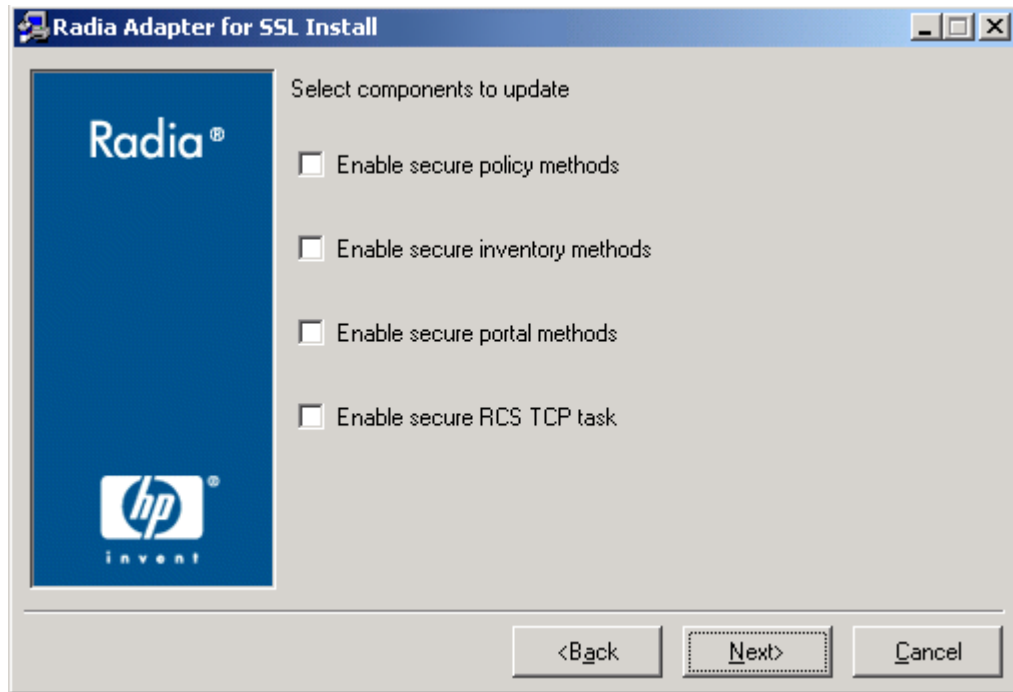


Figure 5 ~ RCS components to update.

7. Click Next.

Select whether to generate a new certificate request or to use an existing certificate.

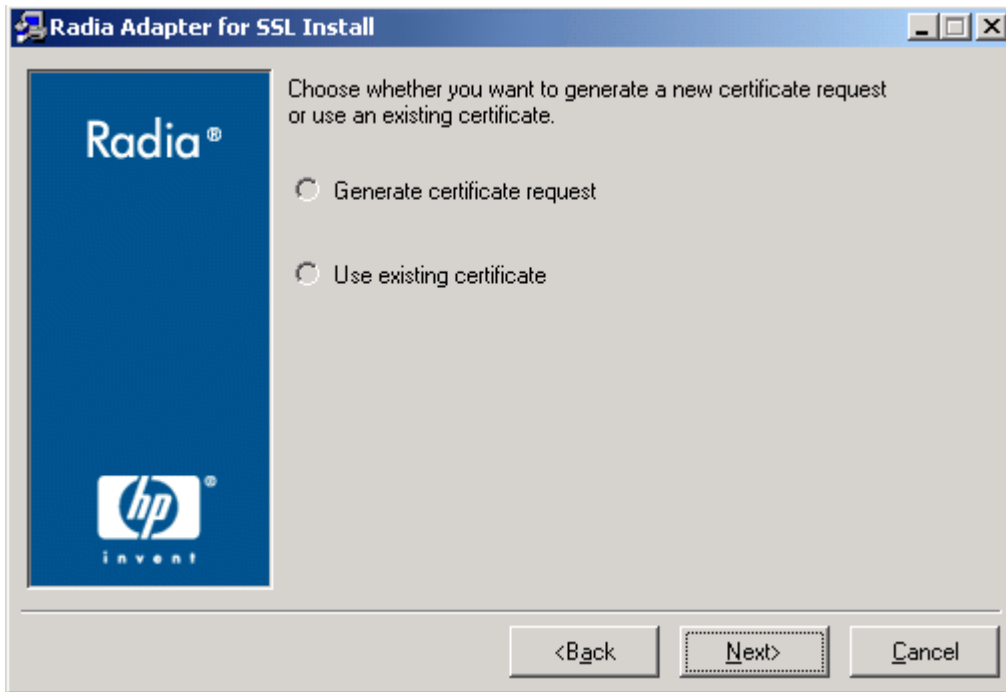


Figure 6 ~ Generate certificate or use existing certificate?

8. Click Next.

If you chose to use an existing certificate, specify the location for the existing key file and certificates file.

9. Click Next.

Specify where you want the Radia Adapter for SSL to be installed.

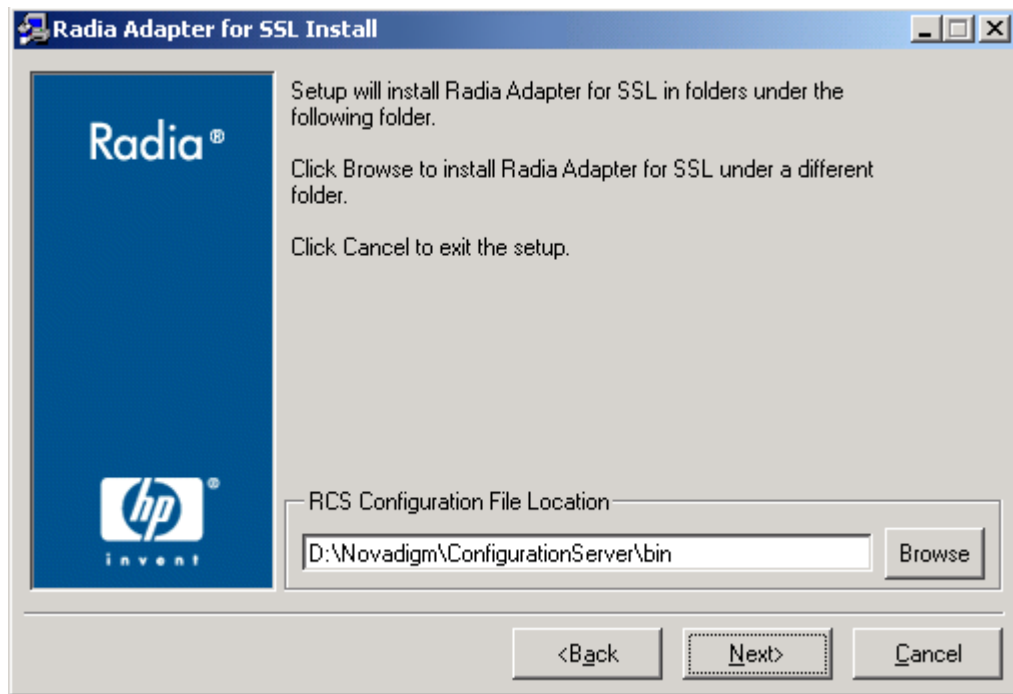


Figure 7 ~ File Location for SSL Adapter.

10. A message indicates that the selected directory will be updated. Click **OK** to continue.
11. If prompted, type the SSL port (default, 443) where the Radia Server should listen for requests.

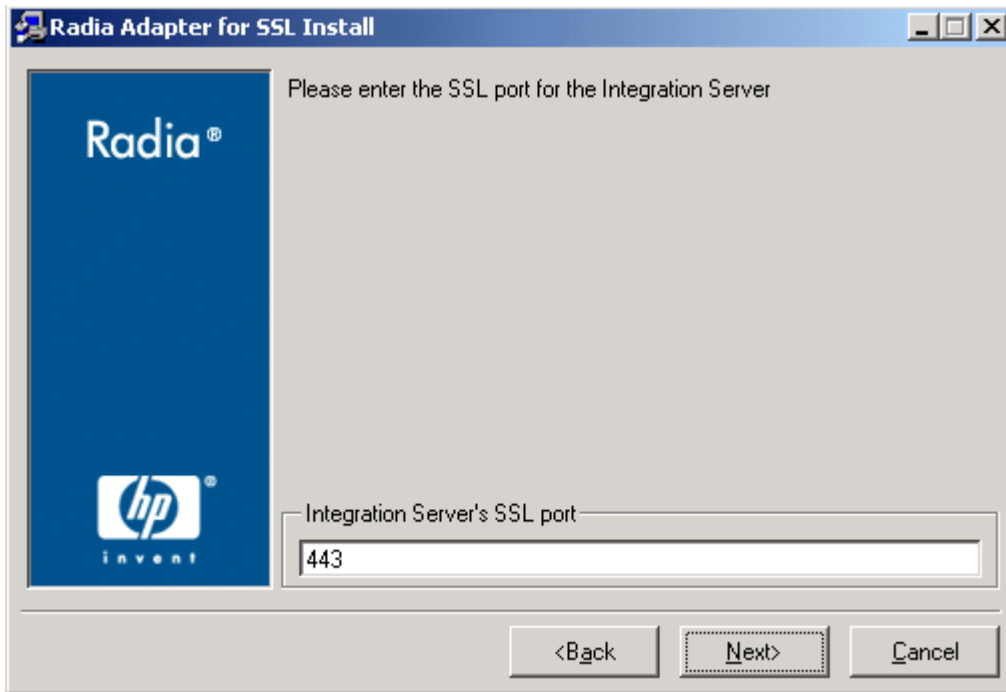


Figure 8 ~ RIS port.

- 12.** Click **Next**.
- 13.** If you choose to generate a certificate request, you will be prompted for information used to generate the request.
- 14.** Click **Next**.

The **Summary** window opens.

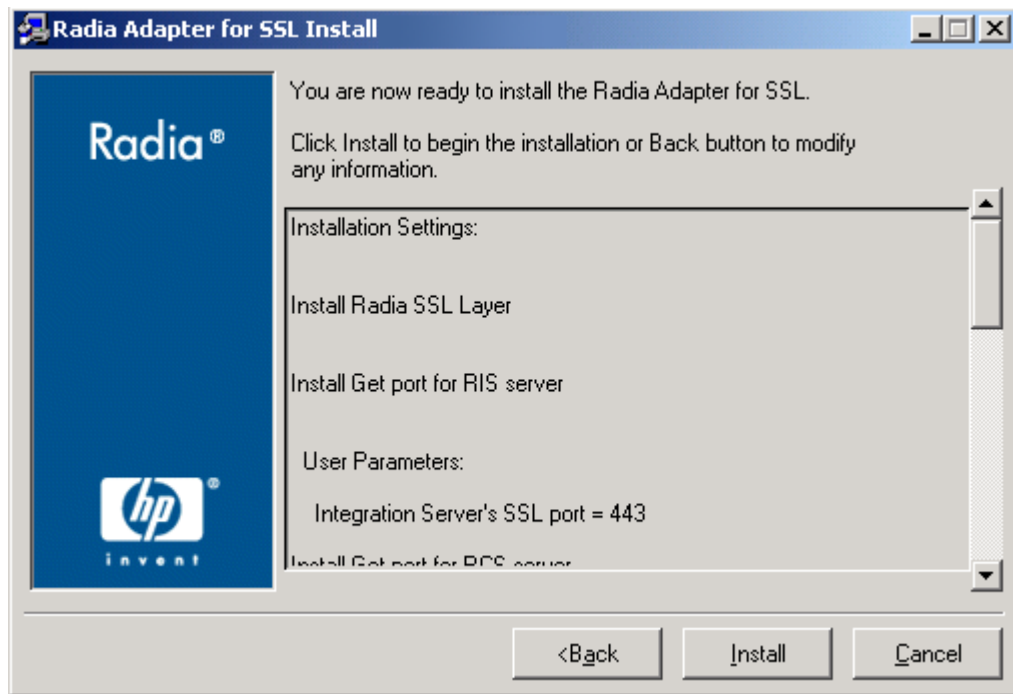


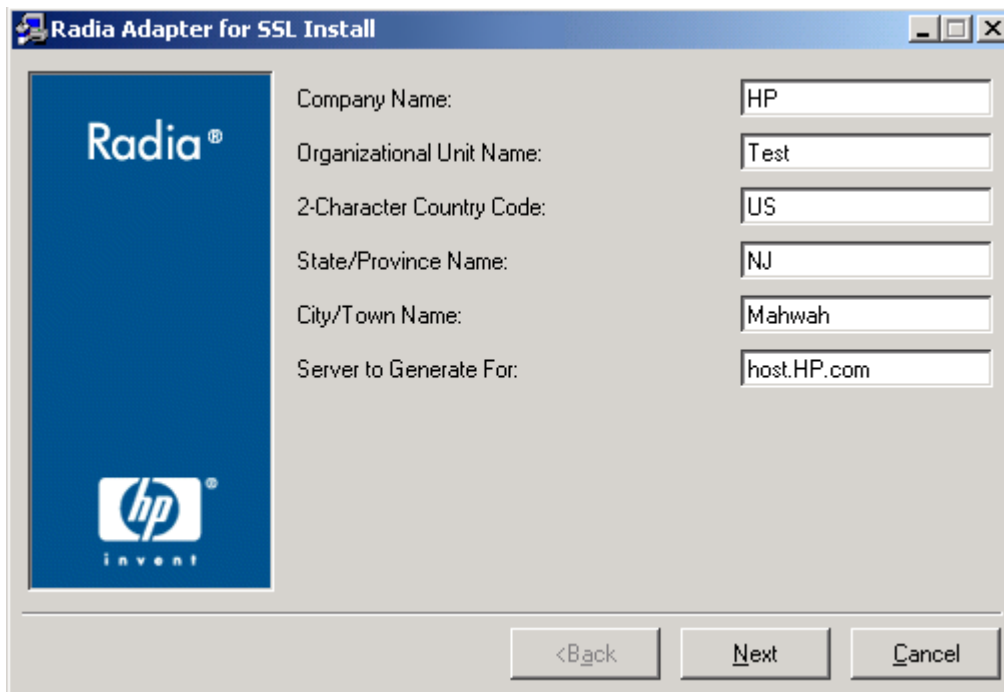
Figure 9 ~ The Summary window.

Review the settings you've specified. If necessary, click the Back button to make any changes.

15. Click Install.

The files necessary 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 successfully copied, the **Review** window opens.



Company Name:	<input type="text" value="HP"/>
Organizational Unit Name:	<input type="text" value="Test"/>
2-Character Country Code:	<input type="text" value="US"/>
State/Province Name:	<input type="text" value="NJ"/>
City/Town Name:	<input type="text" value="Mahwah"/>
Server to Generate For:	<input type="text" value="host.HP.com"/>

<Back Next Cancel

Figure 10 ~ Review window.

16. Review the data that will be used to generate the server certificate request and the private key.
17. Click **Next** to continue. The installation program will take a few moments to generate the server certificate request and private key. A confirmation message, similar to the following, opens.

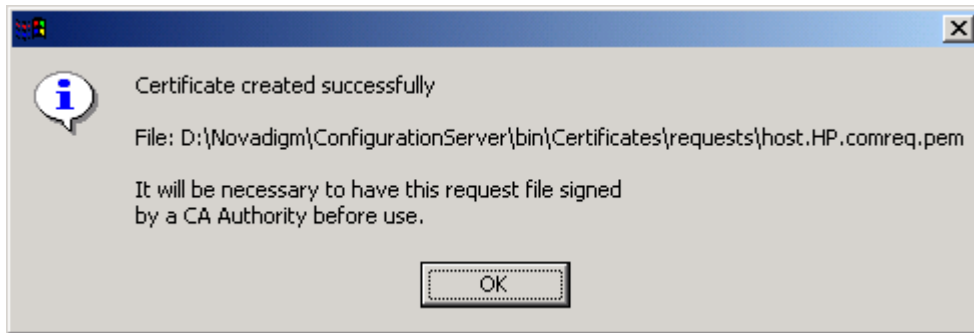


Figure 11 ~ Certificate created successfully message.

18. Click **OK**.

Note

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 Radia Configuration Server's **BIN\Certificates\requests** folder (Win32), and in the **exe/Certificates/requests** folder (UNIX).

The **Installation Successful** window opens.

19. Click **Finish**.

You have successfully installed the Radia Adapter for SSL.

About the Server Certificate Request File

The installation program generates a server certificate request—*filename.pem*. Follow the procedure required by your chosen public certificate authority to have the request signed and returned. Typically, you must open the certificate request in a text editor, copy the certificate request text to a clipboard, and paste it into a text entry field on the signing authority's Web page. The signing authority will also require proof of identity and authority to obtain a signed certificate (such as your company's DUNS number, Articles of Incorporation, Partnership Papers, or Business License).

- **For the Radia Configuration Server**

This file is located in the Radia Configuration Server's `BIN\Certificates\requests` folder (Windows), and `exe/Certificates/requests` folder (UNIX).

- **For the Radia Integration Server**

This file is located in the Radia Integration Server's `\etc\Certificates` folder (Windows), and `exe/Certificates` (UNIX)

If you open the file with a text editor, it will appear similar to the following.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBYDCCAQoCAQAwwgaQxCzAJBgNVBAYTA1VTMRMwEQYDVQIQIEwPOZXcgSmVyc2V5
MQ8wDQYDVQQHEwZNYWh3YWgXhJAcBgNVBAoTFU5vdmFkaWdtIEN1c3RvbWVyeIENv
LjEnMCUGA1UECXMtTWFuYWdlbWVudCBJbmZvcmlhdG1vb1BTeXNOZW1zMSYwJAYD
VQQDEx1yYWRpYTAwMS5Ob3ZhZG1nbUN1c3RvbWVyeLmNvbTBcMAOGCSqGSIb3DQEB
AQUAAOsAMEgCQQDMg53F1yIsmZjAeKLqSUQkZg8xEWNC476KIPL0T/4bkSB9r1bv
eN5gdVOSVrDsJyGZjBjNQEW60DaAJELakMevAgMBAAAGgADANBgkqhkiG9wOBAQQF
AANBAAMs5KqyJwu88AspdZWucFcDaxcSBVvRIyr2wmfw5cLzGwwZMwgiX93XublX
7G4xohoZddAbSdZWIU39EBpRglY=
-----END CERTIFICATE REQUEST-----

```

Figure 12 ~ Server certificate request file.

Signing the Server Certificate Request

When the server certificate request file is returned from the public certificate authority:

1. Change **req** (request) in the server certificate's name to **cert** (certificate). For example, the server certificate request file may be changed from:

```
host.HP.comreq.pem
```

to

```
host.HP.comcert.pem
```

2. Place the signed certificate file in the appropriate folder.

- **For the Radia Configuration Server**
Place the signed certificate file in the Radia Configuration Server's **BIN\Certificates** folder (Windows), and **exe/Certificates** folder (UNIX).
 - **For the Radia Integration Server**
Place the signed certificate file in the Radia Integration Server's **\etc\Certificates** folder (Windows), and **exe/Certificates** (UNIX)
3. (Optional) Delete the copy of the **req** file.

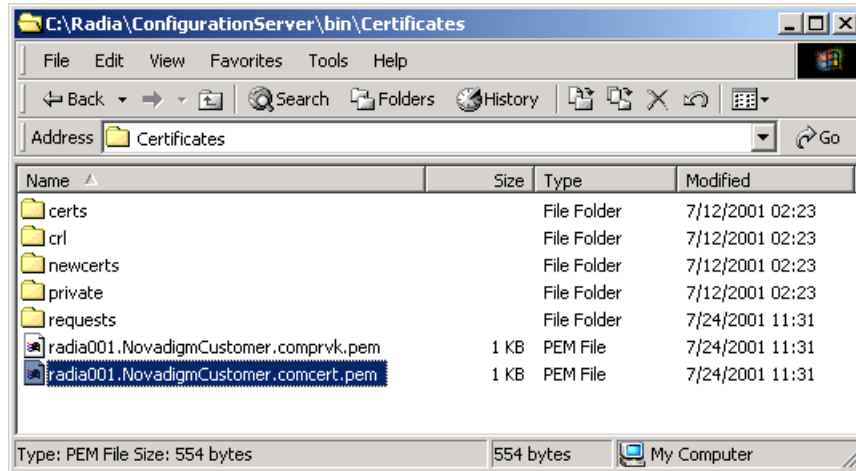


Figure 13 ~ Certificates directory.

4. Restart the Radia Server, and then examine the Server's log to verify that the SSL Manager task starts correctly and successfully verifies the CA certificate and server certificate.

About the Private Key File

The installation program generates a private key file (such as host.HP.comprvk.pem).

- **For the Radia Configuration Server**
This file is located in the Radia Configuration Server's **BIN\Certificates** folder (Windows), and **exe/Certificates** folder (UNIX).
- **For the Radia Integration Server**
This file is located in the Radia Integration Server's **\etc\Certificates** folder (Windows), and **exe/Certificates** (UNIX)

If you open the file with a text editor, it will appear similar to the following.

```

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

1MV8Y4rkyw1Yn30yUB5ULtKLfjOYSzX+KZvxCeuw+9x95x1Ikvej4b8iBDuEOaTR
fp4IDVLuNOH57psT+XdCtRAam493t8csfOC18CURHO/PskT5S1H80EGOPnHcgIrg
YzaVt+pM7ZtxZuwRPKS1RbvRi5YTFU/3TjtfnOqieWaqbxFOTVnzfICX7I1VodOC
OFBwd5XB6cMOZf003yQhte2k2UHvG8PRDlpOrRPEgUvlqqBI1xQ005GSc02OnnwP
WYhUwjAhjB1ALVubZKw5wk/E5lowy4qucWzCp/7c7fyXwiBIk3QWehEwe/NA1kWc
BbOXUiB1PZGtodasgusKDrOmrazm/h1bTbxM1nNgz10wMX/ZztTuN+bX+pSEh3u
piAcdw46e3wKf40KRPiXRbJyoWiIhgeaqwJ7wEr907w=
-----END RSA PRIVATE KEY-----

```

Figure 14 ~ Private key file.

In order to maintain compatibility with current industry standards, we have 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). The private key file presented in Figure 14 (above) begins and ends with the key type (RSA) indicated.

Confirming the Installation

Radia Configuration Server

If you want to confirm that the Radia Configuration Server is configured for SSL support, use a text editor to open <SystemDrive>:\Novadigm\ConfigurationServer\bin\edmprof.dat to confirm that the MGR_SSL section has been added, as shown below.

```

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

```

Figure 15 ~ [MGR_SSL] section in edmprof.dat

The table below 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 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 (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.
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.

Radia Integration Server

If you want to confirm that the Radia Integration Server is configured for SSL support, use a text editor to open `<SystemDrive>:\Novadigm\IntegrationServer\httpd.rc` to 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

```

Figure 16 ~ Overrides Config section in httpd.rc.

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

Table 2 ~ MGR_SSL 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.

Table 2 ~ MGR_SSL Settings

Setting	Usage
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.

Troubleshooting

■ Logs

The Radia Adapter for SSL installation program creates a log file, **setup.log**, in a **SETUP** sub-folder of the folder identified by the **TEMP** setting in your environment (Win32), 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 methods described below.

- 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.

Note

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

■ Existing certificate or private key

If you accidentally use the SSL installation program on a server where you have already installed the SSL Adapter, you may receive the following message “A certificate or private key already exists for the specified server name. Choose another server name.” You can:

- Change the name in the **Server to Generate For** text box (in the **Review and Password** window) and try again. (This generates a new server certificate request for the server identified in this text box).

OR

- Cancel the installation (since a server certificate request and private key already exist for this server).

