

Novell Volera Secure Excelerator

1.1

www.novell.com

ADMINISTRATION GUIDE



Novell®

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1997-2003 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,870,739; 5,873,079; 5,884,304; 6,330,605. U.S. and Foreign Patents Pending.

Novell, Inc.
1800 South Novell Place
Provo, Utah 84606
U.S.A.

www.novell.com

Volera Secure Excelerator 1.1 Administration Guide

May 2003

Online Documentation: To access the online documentation for this and other Volera products, and to get updates, see www.novell.com.

Novell Trademarks

Volera and Novell are trademarks of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

	About This Guide	3
1	Overview of Secure Excelerator	5
	How Secure Excelerator Works	5
	What Secure Excelerator Can Do for Your Network	6
	Offloading Secure Connection Overhead	6
	Opening Up Firewalls	8
	How Secure Excelerator Transforms Links	10
	A Visual Summary	13
2	Planning Your Secure Excelerator Installation	15
	Deciding Which Content to Secure	15
	Identifying Each Web Server	15
	Ensuring that Each Web Server Has an Acceleration Service	15
	Obtaining Trusted Root Certificates	15
	Accessing the Certificate Chain	16
	Storing Trusted Root Certificate Files	16
	Obtaining Appliance Certificates for Each Web Server	17
	Identifying Authentication Sources for Users	17
3	Setting Up Secure Excelerator	19
	Preparing the Appliance	19
	Installing a Secure Excelerator License	19
	Purchasing a Secure Excelerator License	20
	Installing the License from Floppy Disk	20
	Installing the License Using FTP	20
	Installing Secure Excelerator	20
	Downloading the Secure Excelerator Patches	21
	Updating the Appliance's Backup System Image	21
	Backing Up Your License	21
	Establishing Secure Connections with Browsers	22
	Preparing a Certificate Signing Request (CSR)	22
	Sending the CSR	23
	Storing the Certificate	24
	Backing Up Your Certificates	25
	Setting Up Authentication Profiles	25
	Configuring the Web Server Acceleration Services	25
	Opening the Web Server Acceleration Service	26
	Specifying an SSL Listening Port and Selecting a Certificate	26
	Selecting an Authentication Profile	26
	Configuring the Service to Use Secure Excelerator	26
	Importing the Trusted Root Certificates	27

About This Guide

Use this guide to install and configure the Volera™ Secure Excelsator.

For information about Volera Excelsator 2.x, see the documentation accompanying your product.

NOTE: The term *appliance* as used in this guide refers to both appliances from Volera partners and Volera-approved hardware, including server-class machines.

1

Overview of Secure Excelerator

Volera™ Secure Excelerator is a special-purpose module for the Volera Excelerator appliance which secures content as it is being accelerated by one or more appliance Web server acceleration services.

Secure Excelerator was designed for e-businesses, enterprises, and other organizations that want to conduct business using the Web.

Secure Excelerator uses SSL version 3 technology to protect your sensitive data. It does not require any additional software or special configuration of either your Web servers or the browsers accessing your Web site.

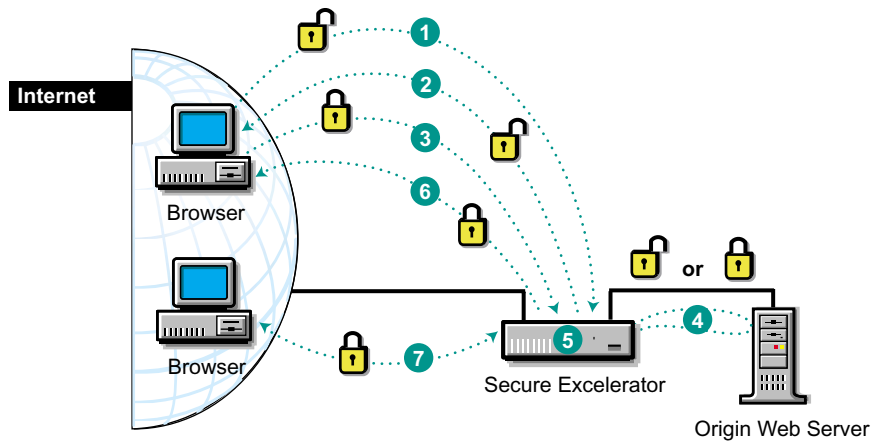
Secure Excelerator:

- ♦ Provides secure external access to both secure and non-secure internal Web servers
- ♦ Eliminates the need to implement SSL services on non-secure internal Web servers
- ♦ Offloads CPU-intensive SSL transactions from internal Web servers
- ♦ Accelerates the Web servers by caching their content
- ♦ Eliminates the need to install special software, such as virtual private networking (VPN) solutions
- ♦ Eliminates the need to manually change links
- ♦ Uses multiple processors to provide very high scalability as secure connection requirements increase
- ♦ Leverages Excelerator's authentication services to verify all users on the Web who request content

How Secure Excelerator Works

Figure 1 illustrates the basic steps that occur when a browser on the Web establishes a secure connection with Secure Excelerator. It also illustrates how Secure Excelerator works with the Excelerator appliance to cache secure content.

Figure 1



- 1 A Browser requests content using HTTP.
- 2 Secure Excelsator sends a redirect to force a secure request (HTTPS).
- 3 The Browser requests content using HTTPS.
- 4 Secure Excelsator fills the request from the Web server using HTTP or HTTPS.
- 5 Secure Excelsator caches the content and converts all HTTP links to HTTPS.
- 6 Secure Excelsator encrypts the content and returns it to the browser.
- 7 Secure Excelsator fills subsequent requests for secure content from cache.

What Secure Excelsator Can Do for Your Network

By adding the Secure Excelsator module to your Excelsator appliances, you can:

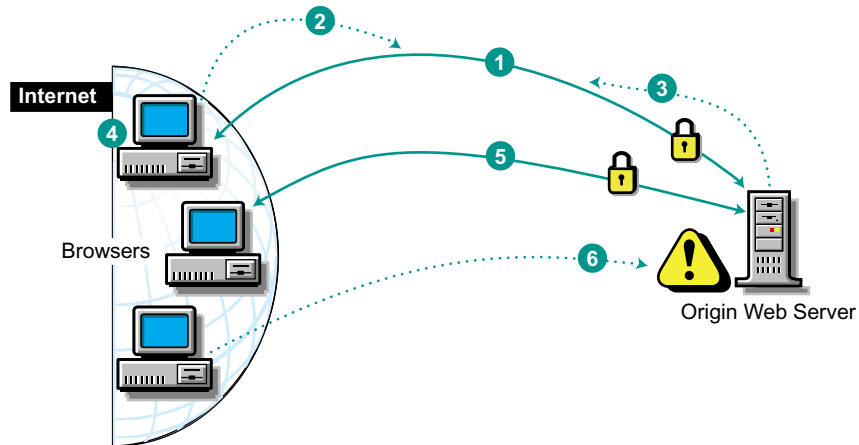
- ♦ Offload secure connection overhead
- ♦ Open firewalls

Offloading Secure Connection Overhead

Establishing and maintaining secure connections between a Web server and the browsers it services takes more processing power than any other Web server tasks. The work required to encrypt and decrypt data is especially taxing.

As additional browsers request connections, the Web server's processor load increases. When the upper limits of processing resources are reached, requests bog down as they wait their turn. Eventually, as illustrated in [Figure 2](#), the Web server has to refuse browser requests.

Figure 2



- 1 The browser and Web server establish a secure connection through a process that is CPU-intensive for the Web server.
- 2 The browser requests content from the Web server using the secure connection.
- 3 The secure Web server sends encrypted content to the browser using the secure connection.
- 4 The browser decrypts the content and displays it.
- 5 Other browsers establish secure connections, thus increasing the load on the server's CPU.
- 6 As requests multiply, the Web server's CPU gets overloaded, causing processing delays and refused connections.

Much of the content sent through secure connections is the same for each browser request. This means that a secure Web server must use its processing cycles to repeatedly encrypt the same content.

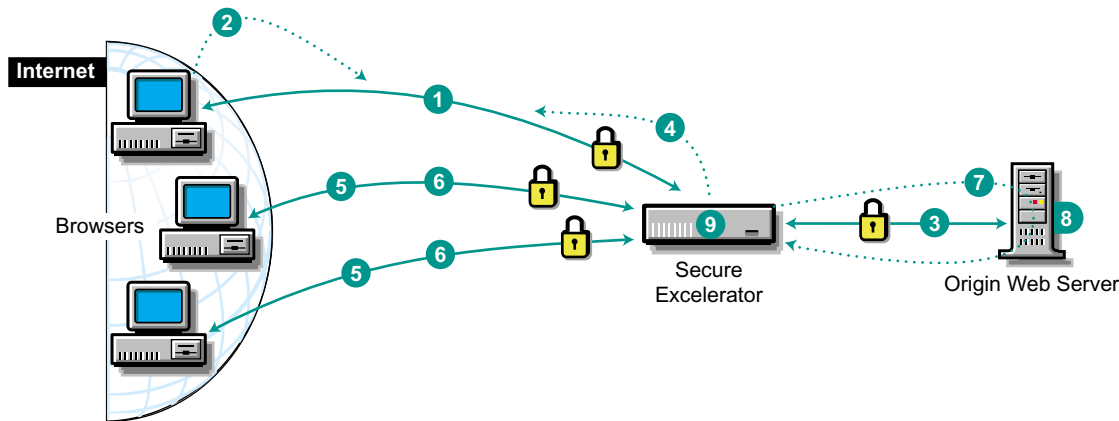
Just as Excelerator appliances cache content and offload redundant content requests from Web servers, Secure Excelerator offloads the repeated encryption of the content.

As a result, the Web server's processor is freed up for one-time, non-cacheable events, such as finalizing online purchases and providing account or credit balance information.

Secure Excelerator also works with multiple processors on a single appliance. This means that you can scale the appliance to handle very heavy secure-connection loads as the demand for secure content increases.

Figure 3 illustrates how Secure Excelerator offloads the secure connection overhead from the Web server.

Figure 3



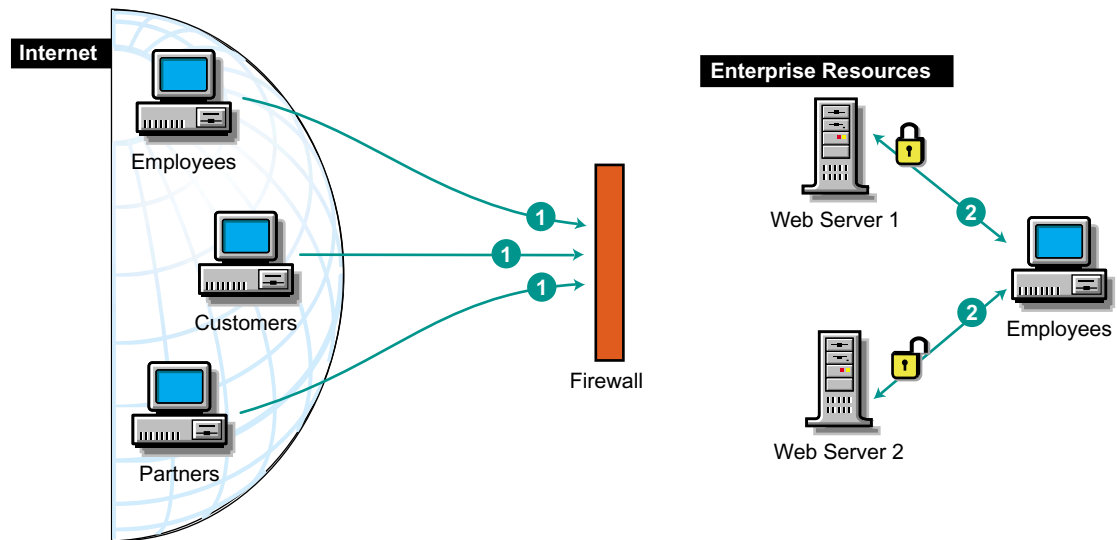
- 1 The browser and Web server establish a secure connection.
- 2 The browser requests Web server content using the secure connection.
- 3 Secure Excelsator establishes a secure connection with the Web server, obtains the requested data, decrypts the data, and, if the data is cacheable, caches the data as clear text.
- 4 Secure Excelsator encrypts the data and sends it to the requesting browser using the secure connection.
- 5 Secure Excelsator establishes secure connections for subsequent fill requests.
- 6 Secure Excelsator fills most secure requests from cache.
- 7 Secure Excelsator obtains uncached data from the Web server using the secure connection.
- 8 Web server CPU cycles are used only for non-redundant tasks because Secure Excelsator handles all redundant content requests and practically all of the encryption.
- 9 Secure Excelsator's multi-processor support eliminates processing delays and supports more connections.

Opening Up Firewalls

Companies with enterprise networks have traditionally erected strong firewalls to protect the data on their network.

However, changes in business dynamics have created a need to provide access through the firewall (see [Figure 4](#)).

Figure 4



1 Employees, customers, and partners on the Web can't conduct business on the enterprise's internal network.

2 Employees on the enterprise's network are restricted to conducting business with only those who can access the network.

Opening Firewalls Without Secure Excelerator

Opening access through the firewall usually requires that you address the following issues:

- ♦ **Authentication:** Ensuring that each secure connection is with someone who is authorized to access the network.

Each Web server must ensure that every user seeking access is verified by a trusted authentication source. Also, each Web server must work with all the authentication sources that are used.

- ♦ **Encryption:** Encrypting all content passing through the firewall.

All data must be encrypted before it is transmitted on the Internet. This ensures that only the intended receiver can decrypt and view the content.

- ♦ **Secure Connections:** Obtaining SSL certificates for each of the Web servers being accessed from the Web, including any servers that are cross referenced in any content being served.
- ♦ **Link Modifications:** Enabling the protocol schemes in all content links to work with SSL.

This requires one of the following actions:

- ♦ Replacing all absolute URL links with relative links

Or

- ♦ Changing all absolute URL links to use HTTPS

- ♦ **DNS Modifications:** Accommodating the use of internal and external DNS hostnames.

For security and other reasons, organizations normally use internal DNS hostnames for their intranet Web servers. They use different DNS hostnames for the same servers when they expose intranet content to the outside world.

Using different hostnames for internal and external access requires two things:

- ♦ Obtaining SSL certificates that match the DNS hostnames that external browsers will use for the Web servers
- ♦ Enabling links to work in both internal and external browsers

Opening Firewalls Using Secure Excelsator

Volera Secure Excelsator doesn't require you to change your existing Web servers or their content to provide secure access through a firewall.

- ♦ **Streamlining Authentication:** You can leverage Excelsator's authentication services so that users log in once for your entire domain.

You enable Excelsator's authentication services by defining one or more authentication profiles and enabling each Web Server Acceleration service to use an authentication profile.

This ensures that only those who are authorized can access your secure content. For more information, see [“Identifying Authentication Sources for Users” on page 17](#) and [“Setting Up Authentication Profiles” on page 25](#).

- ♦ **Transforming Links:** In addition to encrypting and securing all content that is sent to browsers on the Web, Secure Excelsator can eliminate the manual rewriting of URL links within the content on your Web servers. For more information, continue with the next section, [How Secure Excelsator Transforms Links](#).

How Secure Excelsator Transforms Links

If you understand the process Secure Excelsator uses to determine which links to transform, you can ensure that:

- ♦ All the content you are serving to the Web is secure
- ♦ People accessing your Web site won't receive browser warnings regarding the mixing of secure and non-secure content

Only Absolute Links Are Transformed

Only absolute links that include the protocol scheme (HTTP) and a full DNS hostname can be transformed.

For example, Secure Excelsator would rewrite the following link if all other conditions for transforming links are met:

```
<A HREF="http://Inhouse1.foo.org/products/describe.htm">Click here.</A>
```

NOTE: Relative links do not need to be transformed.

Links Must Reference Content on Accelerated Web Servers

If an absolute link references content on a Web server that the Excelsator appliance is securely accelerating, the link can be transformed.

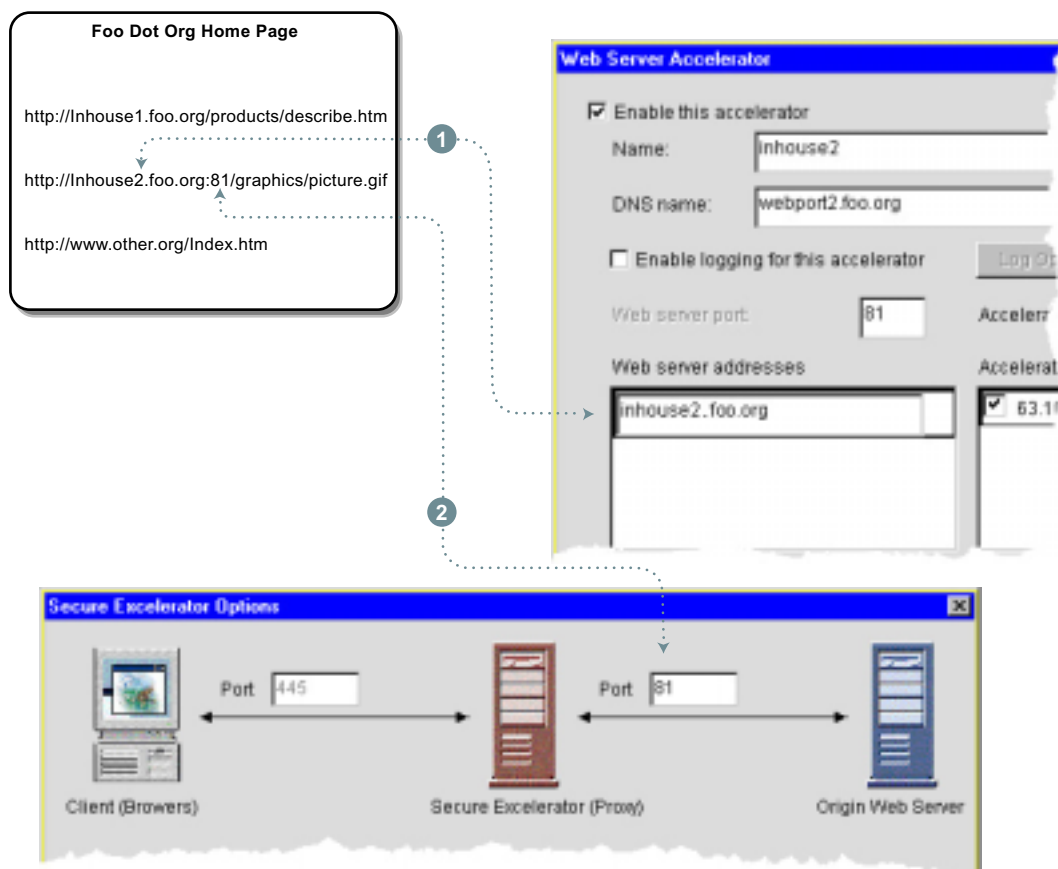
For example, the following table shows which links to Web servers on a given network could be transformed:

Web Server DNS Hostname	Is the Excelerator appliance securely accelerating the Web server?	Can links to the Web server be transformed?
Inhouse1.foo.org	Yes	Yes
Inhouse2.foo.org	Yes	Yes
Inhouse3.foo.org	No	No

Hostnames and Ports Must Match

If the requirements in “Only Absolute Links Are Transformed” on page 10 and “Links Must Reference Content on Accelerated Web Servers” on page 10 are met, Secure Excelerator will transform non-secure links that meet the requirements illustrated in Figure 5.

Figure 5



- 1 The hostname in the link must match the hostname of one of your securely accelerated Web servers.

To access the Web Server Accelerator dialog box, click Cache > Web Server Accelerator > Insert or Modify in the browser-based management tool.

- 2 The port in the link must match the Origin Web Server Port specified in the Secure Excelerator Options dialog box.

To access the Secure Excelerator Options dialog box from the Web Server Accelerator dialog box, check Enable Secure Excelerator and click Secure Excelerator Options.

Information on setting the Web Server Address and Port shown in [Figure 5](#) is contained in [“Configuring the Web Server Acceleration Services” on page 25](#).

What Secure Excelerator Does to Link Content

Secure Excelerator does the following to qualified absolute URLs:

- ◆ It automatically changes the hostname of the origin server to the DNS name specified in the Web Server Accelerator definition.

For example, the DNS hostname `inhouse1.foo.org` might be changed to `webport1.foo.org`.

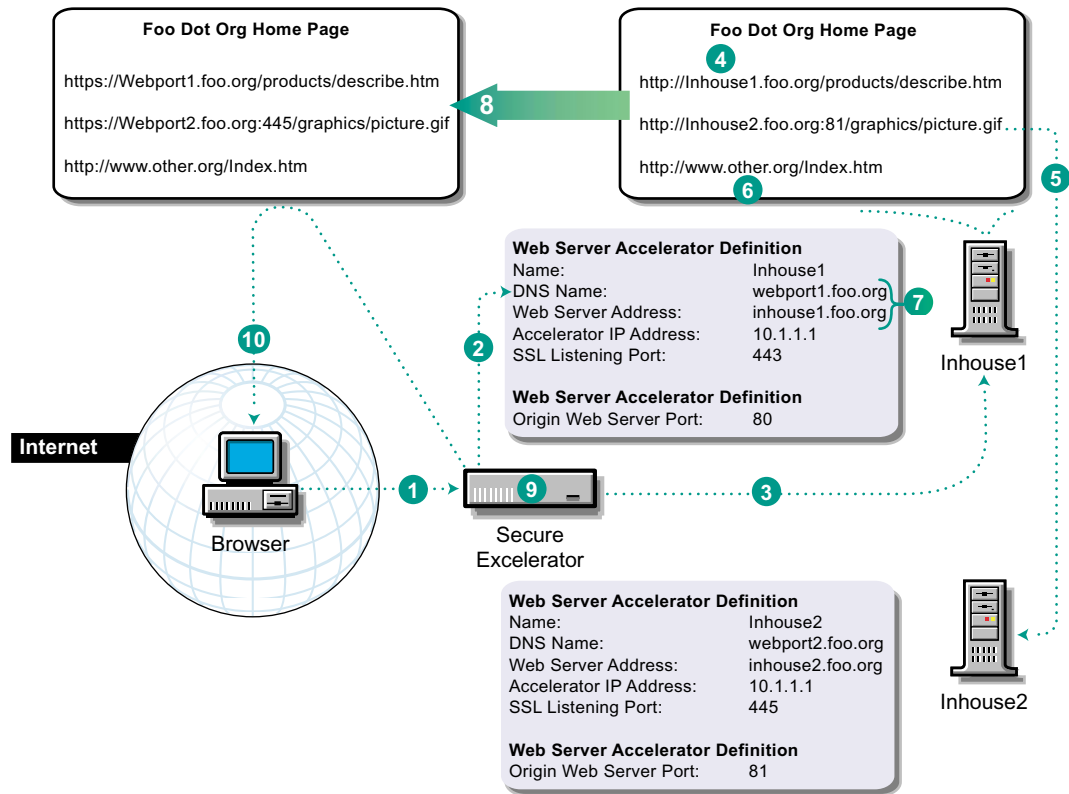
- ◆ It changes the protocol scheme as appropriate in all cached content.

HTTP becomes HTTPS.

- ◆ It automatically inserts any non-standard (non-443) SSL listener port overrides you specify.

[Figure 6](#) illustrates the Secure Excelerator content transformation process.

Figure 6

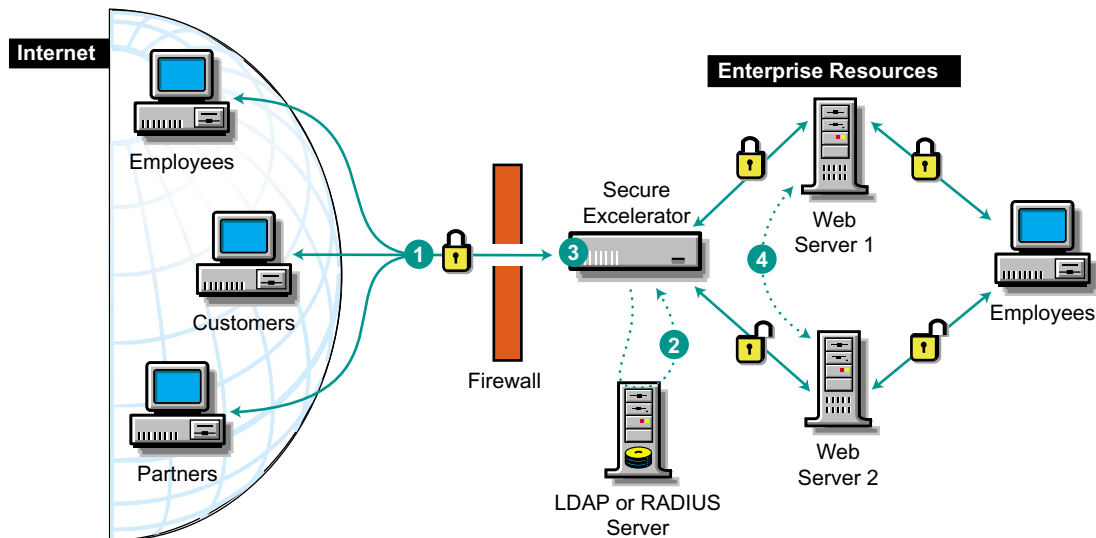


- 1 A browser requests the Foo Dot Org home page using the URL `https://webport1.foo.org/index.htm`.
 - 2 Secure Excelsator matches the hostname in the request with the DNS name in the Web server accelerator definition.
 - 3 Secure Excelsator requests the home page from the Inhouse1 Web server.
 - 4 The Foo Dot Org home page contains links to content on the Inhouse1 Web server.
 - 5 Some links are to the Inhouse2 Web server.
 - 6 Other links are to external Web servers.
 - 7 Because Foo Dot Org uses different DNS hostnames for content served on the Web (webport instead of inhouse [see Item 1]), DNS servers on the Web won't be able to resolve links that use inhouse hostnames.
 - 8 Secure Excelsator transforms links to all securely accelerated inhouse Web servers (both Inhouse1 and Inhouse2) so that the links use the correct protocol scheme, hostname, and SSL port for the Web environment.
 - 9 Secure Excelsator caches the home page.
 - 10 Secure Excelsator sends the transformed home page to the requesting browser.
- Because all the links (items 4, 5, and 6) use the HTTP protocol scheme, browsers on the Web will not generate SSL requests when links are selected. Unless HTTPS is used, the browsers will warn users about non-secure connections.

A Visual Summary

Figure 7 is a visual summary of how Secure Excelsator can connect your internal network to the Web.

Figure 7



- 1 Secure Excelsator ensures that the connections between each Web server accelerator service and each browser are secure.
- 2 Excelsator authentication services ensure that only authorized users can access the Web server acceleration services.
- 3 Secure Excelsator encrypts all data sent to external browsers.
- 4 Secure Excelsator automatically transforms all the absolute links that point to any securely accelerated Web servers on your network.

2 Planning Your Secure Excelerator Installation

Deciding Which Content to Secure

As you plan your Volera™ Secure Excelerator installation, you must first determine what content needs to be secured.

We generally recommend that you secure all content that can conceivably pass through your firewall. In addition to helping prevent security breaches, this will ensure that users don't receive any disconcerting warnings from their browsers regarding non-secure content.

Identifying Each Web Server

To ensure that all content passing through your firewall is secure, you must identify

- ♦ The primary Web servers from which users can request content
- ♦ All other Web servers referenced through links on the primary servers

This generally requires you to perform a methodical analysis of all the Web pages that users can access from your site, including all pages accessible through links on your site.

Ensuring that Each Web Server Has an Acceleration Service

Secure Excelerator works in conjunction with appliance Web acceleration services. Each Web server from which browsers can request content must be associated with an appliance Web server acceleration service. We recommend you compare your list of Web servers identified the previous section, [Identifying Each Web Server](#), with your appliance's Web server acceleration definitions to ensure that each Web server is being accelerated.

If any of the servers are not being accelerated, you should either create services for them or add them to existing services. For more information, see [Accelerating Web Servers](#) in the [Volera Excelerator 2.3 Administration Guide](#).

Obtaining Trusted Root Certificates

If you use Secure Excelerator to accelerate a secure Web server, you will need to provide the Secure Excelerator service with the trusted root certificates for the certificate authority (CA) that issued the Web server's SSL certificate.

NOTE: Trusted root certificates are also known as CA certificate chains because they often consist of two or more certificates that link together to certify a CA's identity.

By identifying the trusted root certificates in advance for each CA, you will ensure that your Secure Excelerator setup happens quickly and efficiently.

IMPORTANT: Each CA has only one set of trusted root certificates. Therefore, you will need only one set of files for each CA you use.

You must copy the trusted root certificates as you set up Secure Excelerator for an acceleration service that fills from secure Web servers on your network. The appliance must have the trusted root certificates to establish secure connections with the secure Web servers from which it is filling browser requests.

You might already have trusted root certificate files (*.CER) from the certificate authorities who issued certificates for your secure Web servers. If you have the files, skip to [“Obtaining Appliance Certificates for Each Web Server” on page 17](#).

If you don’t have the trusted root certificate files for one of your CAs, you must extract them from a Web server whose certificate was issued by the CA.

Complete the steps in [“Accessing the Certificate Chain” on page 16](#) and [“Storing Trusted Root Certificate Files” on page 16](#) for each CA you use.

Accessing the Certificate Chain

Complete the following steps:

- 1 Using Internet Explorer, access a secure Web server with a certificate issued by the CA whose trusted root certificates you need.
- 2 Double-click the lock icon at the bottom of the browser window.
- 3 Click Certification Path.

The last certificate shown in the chain is the Web server certificate. The CA certificate chain is represented by the certificates above this certificate. Therefore, you need to save only the certificates above the Web server certificate.

- 4 Select the certificate above the last certificate in the chain, then click > View Certificate > Details.
- 5 Continue with [Storing Trusted Root Certificate Files](#).

Storing Trusted Root Certificate Files

A CA’s trusted root certificate files usually form a chain consisting of more than one certificate. Each certificate is contained in an ASCII text file.

Repeat the following steps until you have saved each certificate file in the certificate chain.

- 1 Click Copy to File > Next.

When Copy to File is not available, all certificates in the chain have been saved.

- 2 Select Base-64 Encoded x.509 (.CER).
- 3 Click Next > Browse.
- 4 Select a location for the file.

If you have multiple servers, you might want to create a folder for each server.

- 5 In the Filename field, type a unique name to identify the CA and the certificate.

The name can contain up to 8 alphanumeric characters. Do not include the .CER extension.

- 6 Click Save > Next > Finish > OK.

7 Click Certification Path.

8 Select the next certificate upward in the chain and continue with [Step 9](#).

If there are no more certificates above the one you last saved, the chain has been saved. Click OK, click OK again, then close the browser window.

9 Click View Certificate > Details.

10 Repeat this procedure, starting with [Step 1](#).

You will use these files in [“Configuring the Service to Use Secure Excelerator” on page 26](#).

Obtaining Appliance Certificates for Each Web Server

During the setup process, you prepare the appliance to act as a proxy for each Web server being accelerated. This means that you need an SSL certificate chain for each Web server (both secure and non-secure) being accelerated by Secure Excelerator.

Normally, you request the certificates from third-party certificate authorities (such as VeriSign) using the appliance’s certificate maintenance feature. After obtaining the certificates, you install them on the Excelerator appliance.

Because obtaining certificates usually requires up to two weeks, you should take this process into account in the installation timeline.

NOTE: You also have the options of auto-generating certificates or of manually generating certificates using the Excelerator appliance’s CA. However, requesting browsers won’t automatically recognize these certificates. You must set up each browser manually to avoid browser warnings regarding unknown certificate authorities.

You will use these certificates in [“Storing the Certificate” on page 24](#).

Identifying Authentication Sources for Users

Establishing and using secure connections with requesting browsers ensures that no one except the person using the requesting browser can read the content sent from the appliance.

However, having a secure connection does not ensure that the person using the browser is someone who should be accessing your confidential data. The user’s identity must be verified by a trusted authentication source.

You must plan how to verify, or authenticate, the identity of each user requesting access to secure content.

You can eliminate most of the overhead of authentication by using existing databases. Excelerator authentication can leverage both LDAP-compliant and RADIUS databases.

For help in creating authentication profiles, see [“Setting Up Authentication Profiles” on page 25](#).

3

Setting Up Secure Excelerator

IMPORTANT: When you install Volera™ Secure Excelerator, the appliance must be running Excelerator version 2.0 or higher. If you need to upgrade your appliance, visit [Volera's product Web pages on Novell.com](http://support.novell.com/volera) (<http://support.novell.com/volera>).

You must also install a Secure Excelerator patch from the Web. For more information, see ["Downloading the Secure Excelerator Patches" on page 21](#).

You install Secure Excelerator on your appliance by completing the following basic steps:

1. Prepare each appliance on which you are installing Secure Excelerator.
2. Purchase a Secure Excelerator activation license for each Excelerator 2.x appliance that will have Secure Excelerator installed.
3. Download the required Secure Excelerator product patches to each appliance.
4. Set up Secure Excelerator services on each appliance.

Preparing the Appliance

Complete the following instructions for each appliance on which you are installing Secure Excelerator:

- 1 Start a browser on your workstation and connect to the appliance using the browser-based management tool.

For help using the browser-based tool, see [Using the Browser-Based Management Tool](#) in the [Volera Excelerator 2.3 Administration Guide](#).

- 2 Ensure the appliance's backup system image is current by clicking System > Actions > Update Clone > Update Clone.
- 3 If you haven't already done so, restart the appliance without a system CD in the CD tray.

In the browser-based tool, click System > Actions > Restart.

Installing a Secure Excelerator License

You must purchase and install a Secure Excelerator license for each appliance on which you are installing Secure Excelerator.

Three levels of Secure Excelerator licenses are available. The license you need depends on the number of processors on your appliances and how many of those processors you want Secure Excelerator to use:

- ♦ The base license supports one processor.
- ♦ The first-level multiprocessor license supports up to four processors.
- ♦ The second-level multiprocessor license supports up to eight processors.

Purchasing a Secure Excelerator License

To purchase a license, complete the following steps:

- 1 Contact your Novell Authorized Reseller or visit the [Volera product Web pages on Novell com \(http://support.novell.com/volera\)](http://support.novell.com/volera).
- 2 If so instructed, download the Secure Excelerator product and associated license files.
- 3 Install the license on the appliance using one of the following methods:
 - ♦ If you have direct access to the appliance, you can use a floppy disk and the command line interface to install the license. Continue with the instructions in [Installing the License from Floppy Disk](#).
 - ♦ If you do not have direct access to the appliance, you can install the license using FTP. See the instructions in [“Installing the License Using FTP” on page 20](#).

Installing the License from Floppy Disk

Complete the following steps:

- 1 Insert the floppy disk containing the license file in the appliance’s floppy disk drive.
For more information, see [“Purchasing a Secure Excelerator License” on page 20](#).
- 2 At the system prompt, enter
`importlicense floppy`
- 3 Remove the diskette and store it in a safe location.
- 4 Continue with [“Installing Secure Excelerator” on page 20](#).

Installing the License Using FTP

If you have not used an FTP connection to manage your appliance, you should review the information in [FTP Services](#) in the [Volera Excelerator 2.3 Administration Guide](#).

Complete the following steps:

- 1 Launch your FTP application and enter an appliance IP address that is enabled for FTP access.
For instructions on enabling FTP access, see [Setting Up Appliance FTP Services](#) in the [Volera Excelerator 2.3 Administration Guide](#).
- 2 Log in to the appliance using the Config username.
- 3 If you have set a Config username password, enter it when prompted. Otherwise, press Enter.
- 4 FTP the license file from your workstation to the appliance’s /ETC/PACKAGE directory.
- 5 Continue with [Installing Secure Excelerator](#).

Installing Secure Excelerator

Complete the steps in the following sections for each appliance on which you are installing Secure Excelerator.

Downloading the Secure Excelerator Patches

IMPORTANT: Volera provides URLs to the latest product patches with each license purchased. The URLs must be applied in the order listed in the Thank You page and in the confirmation e-mail.

You must always install all product patches before configuring and using an Excelerator product.

Complete the following steps.

- 1 In the browser-based tool, click System > click Upgrade > check Enable Download.
- 2 In the Install from URL field, type the Download URL received from Volera support.
- 3 Double-check the URL to ensure you typed it correctly.
- 4 Click the Download Time drop-down list > select the time you want the download to occur > check Enable Install.
- 5 Click the Install Time drop-down list > select the time you want the upgrade installed.
- 6 Click Apply.

The upgrade process always restarts the appliance, temporarily disconnecting the browser-based tool.

- 7 After the appliance restarts, reconnect to the appliance using the browser-based management tool and repeat this process for any other URLs received on the Thank You page and in the confirmation e-mail.
- 8 After all product patches have been applied, continue with [Updating the Appliance's Backup System Image](#).

Updating the Appliance's Backup System Image

You should update the appliance's clone image as soon as possible after an upgrade is completed.

- 1 Reconnect to the appliance using the browser-based management tool.
- 2 Click System > Actions > Update Clone > Update Clone.

This prevents the system from being overwritten by an earlier version.

Backing Up Your License

You should always save a backup copy of each Excelerator license you purchase. You might choose to store the floppy diskettes used to install the licenses, or you might want to keep the files in a secure location on your network. The method you use is not important. It is important, however, that you have the license files for each appliance in case you need to restore them in the future.

If you prefer, you can periodically copy all the licenses installed on your appliance to a floppy disk and archive them in a safe location.

To copy the license files from an appliance, complete the following steps:

- 1 Insert a blank, formatted floppy disk in to the appliance's diskette drive.
- 2 At the system prompt, enter the following command:

```
exportlicense floppy
```
- 3 Remove the diskette and store it in a safe location.
- 4 Continue with [Establishing Secure Connections with Browsers](#).

Establishing Secure Connections with Browsers

For the appliance to establish secure connections with browsers, it must have certificates installed that were issued by certificate authorities which the browsers recognize.

You will want to purchase certificates from third party certificate authorities (CAs) for most Secure Excelerator installations. A list of trusted CAs is included in your browser. For example, in Internet Explorer 5.5, you can view the list by clicking Tools > Internet Options > Content > Certificates > Trusted Root Certification Authorities.

NOTE: As explained in [Authentication Services](#) in the [Volera Excelerator 2.3 Administration Guide](#), you can have the appliance automatically generate certificates, or you can create them manually. However, both of these options utilize the appliance's internal CA and will result in browser messages indicating that the CA is unknown. Eliminating this message requires manually importing the appliance's trusted root certificate chain into each browser, an impractical requirement for most situations.

Preparing a Certificate Signing Request (CSR)

IMPORTANT: You must obtain a separate appliance certificate for each Web server the appliance is accelerating.

Because obtaining certificates usually requires up to two weeks, make sure your installation timeline takes the certificate request process into account.

Prepare a CSR for each certificate by completing the following steps:

- 1 In the browser-based management tool, click System > Timezone and verify that the system's timezone settings are correct.
 - 2 Click System > Date/Time and verify that the appliance's date and time settings are correct.
- The appliance's system time must be correct when you prepare the CSR. Errors usually indicate a discrepancy between the appliance's system time and your CA's system time.
- 3 Click Home > Certificate Maintenance > Create.
 - 4 Type a certificate name that you easily associate with the accelerated Web server.

The name must contain only alphanumeric characters and no spaces.

- 5 In the Subject Name field, type the Web server's DNS hostname.
- 6 Click the Signature Algorithm drop-down list > select the algorithm used by the original certificate (if applicable).

NOTE: If the Web server is not a secure server, there is, of course, no original certificate algorithm to match.

- 7 Click the RSA Key Size drop-down list > select the RSA key size used by the original certificate (if applicable).

You cannot select a key size larger than the maximum key size on the appliance.

- 8 Click Use External Certificate Authority.

- 9 If you are requesting a VeriSign certificate, check the VeriSign CA checkbox. Otherwise, leave the box unchecked.

- 10 If desired, type a name for your organization or division.

This is commonly referred to as the Organizational Unit and is used to differentiate organizational divisions or to describe departments or divisions.

- 11 Type the city or town where your organization does business.

This is commonly referred to as the Locality.

- 12 Type the unabbreviated name of the state or province where the organization does business.

This is commonly referred to as the State.

- 13 Type the ISO country code for the country where the organization does business.

This is commonly referred to as the Country and must be a valid, two-character ISO country code.

- 14 Click OK.

- 15 Look at the Action and Status fields.

The Action field should have red arrows on the left and the word Request displayed on a green background. The Status should be Building.

The red arrows and green background indicate that you need to click Apply.

- 16 Click Apply.

If any errors occur during the certificate creation process, they are displayed in the Error field on a red background.

- 17 If an error occurs, click Modify.

- 18 In the Modify Certificate dialog box, make the changes necessary to resolve the errors > click OK.

IMPORTANT: You must ensure that the appliance's system time is correct both when you prepare the CSR and when you store the certificate. Errors can indicate a date/time discrepancy between the appliance and your CA.

To check the system time in the browser-based tool, click System > Timezone and/or Date/Time.

- 19 Click Apply and repeat the modification process until the Status field displays the words CSR in Progress on a yellow background.

Sending the CSR

After you have created a certificate signing request for each required certificate, you must send each request in a separate e-mail to the appropriate CA.

For each certificate, complete the following steps:

- 1 To open a new browser window that displays the CSR contents, click View CSR.

- 2 If you are using Internet Explorer, press F5 to reformat the window.

IMPORTANT: The header and trailer must be on lines separate from the body of the CSR.

The header line will be similar to the following:

```
----- BEGIN NEW CERTIFICATE REQUEST-----
```

The trailer line will be similar to the following:

```
-----END NEW CERTIFICATE REQUEST-----
```

If required, you must use hard returns to separate these two lines from the body of the CSR.

- 3 Select and copy the complete CSR text into your workstation's clipboard.
- 4 Paste the CSR text from the workstation's clipboard to the e-mail message or HTML form as required by your CA.

The method for sending the CSR will vary, depending on the authority. VeriSign, for example, uses a web page interface.

NOTE: If you are using Internet Explorer and the paste operation does not work in your browser, you must download and install the Microsoft virtual machine on your workstation. To obtain this component, search for Microsoft VM on the [Microsoft Web site \(http://www.microsoft.com/downloads/search.asp?\)](http://www.microsoft.com/downloads/search.asp?).

- 5 Complete the application process required by your CA.

IMPORTANT: You must ask the CA to issue your certificates in Base-64 Encoded x.509 (.CER) format. Otherwise, the certificate installation instructions that follow will fail.

- 6 Wait for the certificates to be returned from the external CAs.

Storing the Certificate

After the external CAs respond with the certificates for each Web server, complete the following steps for each certificate you have received:

- 1 In the browser-based management tool, click System > Timezone and verify that the system's timezone settings are correct.
- 2 Click System > Date/Time and verify that the appliance's date and time settings are correct.

The appliance's system time must be correct when you store the certificates. Errors usually indicate a discrepancy between the appliance's system time and your CA's system time.

- 3 In the browser-based tool, click Home > Certificate Maintenance > the name of the certificate you want to store > Store Certificate.

NOTE: If you requested a VeriSign certificate and you checked the VeriSign box on **Step 9** under "**Preparing a Certificate Signing Request (CSR)**" on **page 22**, you will not need to paste the VeriSign CA certificate because VeriSign certificates are already stored on the appliance. Skip to **Step 7**.

- 4 Using Notepad, open the CA certificate you received from the CA.

If you are using multiple CAs, ensure you use the CA certificate for the CA who issued the certificate you are storing (the name selected in **Step 3**).

- 5 Copy the file contents to the workstation's clipboard by clicking Edit > Select All > Edit > Copy.
- 6 In the browser-based tool, paste the CA certificate in the CA Certificate Contents box.
- 7 Using Notepad, open the Web server certificate you received that matches the name of the certificate you are storing (the name selected in **Step 3**).
- 8 Copy the file contents to the workstation's clipboard by clicking Edit > Select All > Edit > Copy.
- 9 In the browser-based tool, Click the Server Certificate Contents box.
- 10 Paste the Web server certificate from the clipboard to the Server Certificate Contents box.
- 11 Click Create.
- 12 Look at the Action and Status fields.

The Status should be CSR in Process.

The Action field should have red arrows on the left and the word Create displayed on a green background. The red arrows and green background indicate that you need to click Apply.

- 13 Click Apply.
- 14 Check to ensure there are no errors displayed on a red background in the Error field.

- 15 If the Status field displays Active and there are no errors indicated, the certificate is ready to use. Return to [Step 3](#) and repeat the process for the next Web server certificate you need to store.
- 16 If the Error field displays an error, one of the following conditions has probably occurred:
- ♦ The appliance's system time is incorrect.
 - ♦ One of the certificates doesn't match the CSR.
- Do the following:
- 16a Verify that the appliance's system time is correct by clicking System > Timezone and/or Date/Time.
- The appliance's system time must be correct both when you prepare the CSR and when you store the certificate. Errors usually indicate a discrepancy between the appliance's system time and your CA's system time.
- 16b Return to [Step 3 on page 24](#) and ensure the following:
- ♦ The CA certificate you pasted in the CA Certificate Contents box ([Step 6](#)) matches the CA who issued the certificate you have selected in the Certificate Name list ([Step 3](#)).
 - ♦ The Web server certificate you pasted in the Server Certificate Contents box ([Step 10](#)) is the certificate received in response to the CSR request that created the entry you have selected in the Certificate Name list ([Step 3](#)).

Backing Up Your Certificates

You should always ensure that you have backup copies of all the SSL certificates used on your network. The Excelerator appliance lets you back up any certificates after you have stored them. For more information, see [Backing Up a Certificate](#) in the [Volera Excelerator 2.3 Administration Guide](#).

Setting Up Authentication Profiles

To use authentication in conjunction with Secure Excelerator, you must create one or more authentication profiles and enable one of the profiles for each Web server acceleration service. You can use the same authentication profile for all Web server acceleration services, or you can define and select profiles that meet specific acceleration service needs.

Complete the following steps:

- 1 In the browser-based management tool, click Cache > Authentication.
- 2 Create the LDAP and/or RADIUS authentication profiles required by your authentication needs.

Information regarding the various dialog boxes and their fields and options is contained in the [Authentication Tab](#) section in the [Volera Excelerator 2.3 Administration Guide](#).

Configuring the Web Server Acceleration Services

NOTE: Prior to completing the instructions in this section, you should have received and installed all the certificates requested in ["Preparing a Certificate Signing Request \(CSR\)" on page 22](#).

Opening the Web Server Acceleration Service

For each of the acceleration services you identified in [“Ensuring that Each Web Server Has an Acceleration Service” on page 15](#), complete the following steps:

- 1 If the service doesn't exist, you must create it by completing the instructions in [Web Server Accelerator Setup](#) in the [Volera Excelerator 2.3 Administration Guide](#).

IMPORTANT: Two fields specified in the Web server accelerator definitions you create are critical to Secure Excelerator's link transformation feature.

These fields are the DNS name specified in the Web Server Addresses list and the Web Server Port specified in the Secure Excelerator Options dialog box. Their role in link transformation is explained in [Figure 5 on page 11](#).

- 2 In the browser-based management tool, click Cache > Web Server Accelerator > the target Web Server Acceleration service > Modify.
- 3 Continue with [Specifying an SSL Listening Port and Selecting a Certificate](#).

Specifying an SSL Listening Port and Selecting a Certificate

Complete the following steps:

- 1 In the Web Server Accelerator dialog box, check Enable Secure Excelerator.
- 2 In the SSL Listening Port field, type the SSL port number for the service.

The default SSL port is 443.

IMPORTANT: If you are using the same acceleration IP address for multiple Web server accelerators, you must ensure that each definition uses a unique SSL port for its Secure Excelerator service.

- 3 In the Certificate drop-down list, select the certificate you obtained for the Web server being accelerated.

NOTE: As explained in [“Obtaining Appliance Certificates for Each Web Server” on page 17](#) and [“Establishing Secure Connections with Browsers” on page 22](#), you can have the appliance automatically generate SSL certificates, you can manually create them, or you can purchase them from third-party CAs. For most installations, the third-party CA option works best.

- 4 Continue with [Selecting an Authentication Profile](#).

Selecting an Authentication Profile

Complete the following steps:

- 1 In the Web Server Accelerator dialog box, check Enable Authentication > click Authentication Options.
- 2 In the Existing Profiles list, select the profile you want this service to use.
- 3 Click Add > OK.
- 4 Continue with [Configuring the Service to Use Secure Excelerator](#).

Configuring the Service to Use Secure Excelerator

Complete the following steps:

- 1 In the Web Server Accelerator dialog box, check Enable Secure Excelerator > click Secure Excelerator Options.

- 2 If the content being served from this accelerator should not be cached by requesting browsers, ensure that the Mark Pages Non-Cacheable on the Browser option is checked.
- 3 If the Web server being accelerated doesn't require a secure connection with the appliance, click OK > click OK > click Apply > return to "Opening the Web Server Acceleration Service" on page 26.

Otherwise, continue with **Importing the Trusted Root Certificates**.

Importing the Trusted Root Certificates

If a secure connection between the Web server and Secure Excelerator is required, you must import the certificate files you identified in "Obtaining Trusted Root Certificates" on page 15.

Complete the following steps:

- 1 Using Notepad, open the first certificate file you saved in "Storing Trusted Root Certificate Files" on page 16.
- 2 In Notepad copy the file contents to the clipboard by clicking > Edit > Select All > Edit > Copy.
- 3 In the Secure Exceleration Options dialog box (accessed in "Configuring the Service to Use Secure Excelerator" on page 26), check Enable Secure Access between Secure Excelerator and Web Server.
- 4 Click Insert > Import Trusted Root.
- 5 In the Imported Filename field, type the root name of the certificate you opened in Notepad and include the extension .DER in the filename.
- 6 Click the Insert Trusted Root Contents box > press Ctrl+V to copy the clipboard contents into the box.

NOTE: If you are using Internet Explorer and the paste operation does not work (nothing is copied), you must download and install the Microsoft virtual machine on your workstation. To obtain this component, search for Microsoft VM on the [Microsoft Web site \(http://www.microsoft.com/downloads/search.asp?\)](http://www.microsoft.com/downloads/search.asp?).
- 7 Click OK.
- 8 Using Notepad, open the next certificate file and repeat the process from **Step 2** until all CA certificates have been imported.
- 9 When the entire chain has been imported, click OK > OK > Apply.
- 10 Repeat the accelerator configuration process by returning to "Opening the Web Server Acceleration Service" on page 26 until all the services have been configured to use Secure Excelerator.

