Web Security Deployment

Web Security Deployment - Client Site Proxy and Remote Connect

Client Site Proxy and Remote Connect Deployment Guide

Documentation version: 1.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Clients are advised to seek specialist advice to ensure that they use the Symantec services in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include (but is not limited to) data protection law, privacy law, telecommunications regulations, and employment law. In many jurisdictions, it is a requirement that users of the service are informed of or required to give consent to their email being monitored or intercepted for the purpose of receiving the security services that are offered by Symantec. Due to local legislation, some features that are described in this documentation are not available in some countries.

Configuration of the Services remains your responsibility and entirely in your control. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec advises you to always check local legislation prior to deploying a Symantec service. You should understand your company’s requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. Symantec can accept no liability for any civil or criminal liability that may be incurred by you as a result of the operation of the Service or the implementation of any advice that is provided hereto.

The documentation is provided "as is" and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Symantec Corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information that is contained in this documentation is subject to change without notice.

Symantec may at its sole option vary these conditions of use by posting such revised terms to the website.

Technical support

If you need help on an aspect of the security services that is not covered by the online Help or administrator guides, contact your IT administrator or Support team. To find your Support team's contact details in the portal, click **Support** > **Contact us**.

Contents

Section 1

Overview of Web Security deployment

Chapter 1

Introducing Web Security deployment

This chapter includes the following topics:

Overview to deploying Web Security

To enable Web traffic to be directed through the the Web Security infrastructure, configure your network to direct Web traffic into your organization using proxy settings. The proxy settings are provided in your confirmation email. They comprise the following:

- Web Security Proxy Address: for example, proxy*X.XX*.webscanningservice.com (where *X* is variable)
- Web Security Proxy Port

You can configure the proxy settings in the following ways:

- Configure the proxy settings directly within the settings of your Internet browser (Internet Explorer and Mozilla Firefox are described in this guide).
  See "Configuring proxy server settings in Internet Explorer" on page 79.
- Use a PAC (Proxy Auto-Configuration) file is to define the proxy settings. This file can be pushed out across your network. Use WPAD (Web Proxy Autodiscovery Protocol) to locate the PAC file automatically.
  See "Deploying the use of PAC / WPAD files" on page 85.

- The CSP captures information specific to the user computer making requests to the Internet.

Initial planning and key decisions

The overall process of setting up Web Security involves some initial planning, based on the existing setup of your network, and your requirements.

There are several key decisions to be made about the installation including:

- Whether to implement the same settings for all users or require Web URL Filtering control and reporting at the user or group level
- Whether to download details of users and groups from your existing Active Directory setup or create custom users and groups within Web Security manually
- Whether to integrate the operation of Web Security with Microsoft's ISA Server.

See "Setting up Web Security with user/group configuration and synchronizing users/groups with the Active Directory" on page 75.

See "Setting up Web Security without user/group configuration or only custom users/groups (no Active Directory synchronization)" on page 76.

Deploying Web Security within a local area network step by step

When you deploy Web Security within your local area network, you direct your users' web traffic through a Client Site Proxy. The Client Site Proxy then forwards the web traffic to the Web Security infrastructure. The table shows the main tasks.

Table 1-1 Phases to deploy Web Security within a local area network

Phase	Description	Action
Phase 1	Install and configure the Client Site Proxy	See "About the Client Site Proxy for Web Security services" on page 14. See "Installing the Client Site Proxy for standalone server step by step" on page 17. or See "Installing the Client Site Proxy for ISA server step by step" on page 44. or See "Installing the Client Site Proxy for TMG server step by step" on page 60.
Phase 2	Configure the proxy server in users' web browsers	See "Overview to deploying Web Security" on page 9. See "Setting up Web Security with user/group configuration and synchronizing users/groups with the Active Directory" on page 75.
Phase 3 (optional)	Set up web roaming	See "About web roaming" on page 94. See "Deploying Remote Connect step by step" on page 95. or See the *Smart Connect Deployment Guide*

Other guidance on Web Security

These help topics provide further guidance on the Web Security Services.

Table 1-2 Help on Web Security

	Help page
Click to open the help page	Web Security Configuration Smart Connect Deployment Web Firewall Configuration Web Security Deployment

Section 2

Set up the Client Site Proxy server

Chapter 2

Introduction to the Client Site Proxy Tool for Web Security

This chapter includes the following topics:

About the Client Site Proxy for Web Security services

The Client Site Proxy (CSP) is the component of Web Security which captures information specific to the user machine making requests to the internet. To accomplish this, the CSP authenticates the user making a web request against the local domain, captures and encrypts details of the domain name, username and local IP address and adds them to the HTTP request as custom HTTP headers. This information is used in conjunction with information on users held by the service to then apply the policy specifically to the user as defined in the portal.

The CSP acts as an authenticated web proxy for internal computer workstations. In outline, workstations are configured to use the CSP as their http proxy server rather than the external Web Security proxy. When a web page is requested, the CSP authenticates the user against the local domain and captures the local IP information of the requesting computer. It then securely passes this information and the original request to Web Security. Web Security then evaluates which rules should be applied to the request. Once the rules have been processed, the page is requested from the web server and then passed back to the CSP and then onto the requesting workstation.

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

Choosing the right Client Site Proxy for you

There are currently three implementations of the Client Site Proxy (CSP) for Web Security.

The CSP has been designed to integrate into your existing infrastructure. If you already use Microsoft's ISA server 2004 or 2006, then use the appropriate CSP version for TMG.

For all other infrastructures, use the standalone version of the CSP.

Table 2-1 Current implementations of CSP

CSP implementation	Description
CSP, Standalone version	Installs on an existing or new Microsoft Windows server and acts as standalone proxy server . See "Installing the Client Site Proxy for standalone server step by step" on page 17.
CSP for ISA server	A plug-in for Microsoft ISA server 2004 and 2006. The plug-in adds the CSP functionality to the ISA server See "Installing the Client Site Proxy for ISA server step by step" on page 44.
CSP for TMG	A plug-in which adds CSP functionality to the Microsoft Forefront Threat Management Gateway. See "Installing the Client Site Proxy for TMG server step by step" on page 60.

Downloading the Client Site Proxy

To download the Client Site Proxy, in the portal click **Tools** > **Downloads** and click the **Download** button in the **Client Site Proxy** section.

Chapter 3

Client Site Proxy for Standalone Server

This chapter includes the following topics:

- Troubleshooting - checking the CSP (standalone server)

Installing the Client Site Proxy for standalone server step by step

The following table provides an overview of the tasks involved in installing and using the Client Site Proxy (CSP) for standalone server.

Table 3-1 Overview of tasks

Task	More information
CSP Request flow	See “Request flow for Client Site Proxy for standalone server” on page 19.
Planning to install the CSP	See “Planning to install the CSP for standalone server” on page 20. See “About installing CSP to multiple sites (for standalone server)” on page 20. See “Building in redundancy for CSP (standalone server)” on page 20.
Requirements for installing the CSP	See “Requirements for the Client Site Proxy for standalone server” on page 24.
Chaining two CSPs together between the LAN and DMZ	See “Client Site Proxy for Standalone Server version 1.00.028 Release Notes” on page 18.
Installing the CSP	See “Installing the Client Site Proxy for standalone server” on page 25.
Configuring the CSP	See “Configuring the Client Site Proxy for standalone server” on page 26.
Stopping and starting the CSP	See “Stopping and starting the Client Site Proxy for standalone server” on page 27.
CSP logs	See “Logs for the Client Site Proxy for standalone server” on page 27.
Upgrading the CSP	See “Upgrading the Client Site Proxy for standalone server” on page 28.
Removing the CSP	See “Removing the Client Site Proxy for standalone server automatically” on page 29.

See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.

See “Troubleshooting - checking the CSP logs (standalone server)” on page 30.

See “Troubleshooting - checking the CSP client computers (standalone server)” on page 31.

See “Troubleshooting - checking the CSP (standalone server)” on page 31.

Client Site Proxy for Standalone Server version 1.00.028 Release Notes

Version 1.00.028 of the CSP for Standalone Server introduces a new configuration parameter, *keep_username_xsaucer*. The parameter allows an organization to chain two CSPs together, where the first CSP is in an internal network and a second CSP is in the DMZ.

In this setup, the internal CSP has access to the organization's Active Directory server and authenticates user requests. The DMZ CSP does not have access to the internal network. Normally, when the internal CSP receives traffic with X-saucer and X-teacup headers, the internal CSP removes them in case they are spoofed. The internal CSP re-adds the X-saucer and X-teacup headers once the user authentication has been completed.

The DMZ CSP is not able to complete the user authentication because it has no access to the internal network or Active Directory. Therefore, the DMZ CSP is not able to add the X-saucer or X-teacup headers, and so it should not remove them to begin with. The *keep_username_xsaucer* configuration parameter was implemented to instruct the CSP to not remove these headers. Note that the administrator needs to configure the DMZ CSP to bypass authentication, which is pre-existing CSP functionality.

The valid values for this new parameter are "**on**" or "**off**".

Installation instructions

1. Back up your current configuration file, located at C:\ClientSiteProxy\etc\squid.conf.
2. Uninstall the current Client Site Proxy package.
3. Run the CSP installer.
4. Merge your previous custom configuration settings into the new configuration file.
5. Restart the CSP service.

Request flow for Client Site Proxy for standalone server

The request flow shows the environment where Web Security is deployed with the CSP installed. It is worth noting that NTLM authentication is per connection not per request.

Note: The first request will follow all steps but future requests for this TCP session will be replaced by a simple one step request for the web page.

CSP request flow for standalone server

1. Client sends unauthenticated request to the CSP
2. CSP responds with "Authentication required" of type NTLM
3. Client sends the user name to the server (in plain text, base-64 encoded).
4. CSP generates a 16-byte random number, called a challenge, and sends it to the client.
5. The client encrypts this challenge with the hash of the user's password and returns the result to the CSP. This is called the response.
6. The CSP sends the following three items to the domain controller: User name, Challenge sent to the client and Response received from the client
7. The domain controller uses the user name to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge. The domain controller compares the encrypted challenge it computed to the response computed by the client. If they are identical, authentication is successful.
8. CSP adds the custom HTTP headers that contain the domain\username and local IP encrypted, CSP requests page from Web Security
9. Web Security decrypts the headers and evaluates the request against rules in the portal. Rules can now be applied to groups and client IP. If allowed the page is now requested from the original web server
10. Web Security receives web page and evaluates the request against rules in the portal.
11. Web Security returns page to the CSP
12. CSP returns web page to the client.

Planning to install the CSP for standalone server

The standalone CSP is straight forward to install and configure. We recommend that you secure the CSP behind a firewall. The CSP needs to be member of the domain that the users authenticate against. All workstations that use the CSP must be able to access the server.

See “Building in redundancy for CSP (standalone server)” on page 20.

About installing CSP to multiple sites (for standalone server)

If you have multiple sites with Internet access, you must consider some additional points.

Two scenarios are possible:

- Each site is connected through a WAN and each site has Internet access.

  You can have a CSP at each site. The advantage to have the CSP at each site is that it reduces WAN traffic and each site is independent. You can still choose to have only one CSP at the main site. You simplify the installation if you have the CSP at the main site, however, you do not take advantage of the Internet access at each site.
- Each site is connected through a WAN and you have one access point to the Internet. We recommend that you install the CSP at the site that has Internet access. Because the CSP only acts as a proxy server and not as a caching proxy, you have no additional benefit to have a CSP that is installed at each site, as the WAN traffic would be the same in either case

See “Planning to install the CSP for standalone server” on page 20.

Building in redundancy for CSP (standalone server)

You can ensure failover and load-sharing of the HTTP proxy between two or more CSP servers without third-party products. Browsers can be configured automatically by using a configuration file known as "proxy.pac" file

The following code sample shows an example proxy.pac that uses one possible method to do load sharing and failover. After the code sample, the logic within the code is explained. This example must be customized for your organization.

```
// Sample proxy.pac
```

```
function FindProxyForURL(url,host)
{
// set p1 and p2 to the 2 proxies
var p1="10.90.193.213"
var p2="10.90.193.211"
//find the 4th octet - if even, is p1/p2 else p2/p1
var myip=myIpAddress()
var ipbits=myip.split(".")
var myseg=parseInt(ipbits[3])
if(myseg==Math.floor(myseg/2)*2) {
  var proxone=p1
  var proxtwo=p2
}
else {
  var proxone=p2
  var proxtwo=p1
 }

//if name has no dots, or is our domain, or starts 10., or if my
//current address does not start 10. don't use proxy
if(isPlainHostName(host)  ||
dnsDomainIs(host,".mydomain.co.uk") ||
myip.substring(0,3)!=="10." ||
host.substring(0,3)=="10." )

//
{
// alert("direct")
return "DIRECT";
}
else {
//  alert("proxy")
return "PROXY "+proxone+":8080; PROXY "+proxtwo+":8080" ;
}
}
```

Dissecting the Routine

For this example the company uses the class A "10" address range for all internal IP addresses, and the internal DNS domain is "mydomain.co.uk".

```
function FindProxyForURL(url,host)
{
```

This marks the start of the function. The function is always called `FindProxyForURL`. The browser passes the full URL (e.g. http://www.google.com/index.html) and the host name (e.g. www.google.com). The final closing "`}`" at the end of the script denotes the end of the function.

```
// set p1 and p2 to the 2 proxies
var p1="10.90.193.213"
var p2="10.90.193.211"
```

The first line is a comment. The next two lines set the values of the two variables to use. Putting them here at the start of the routine makes it easier to find them, if you want to change them.

To take down one of the proxies, change these variables so that they both refer to the same server. Once everyone has reloaded their browser, they only talk to one proxy. You can easily take down the second without any effect whatsoever.

```
//find the 4th octet - if even, is p1/p2 else p2/p1
var myip=myIpAddress()
var ipbits=myip.split(".")
var myseg=parseInt(ipbits[3])
if(myseg==Math.floor(myseg/2)*2) {
  var proxone=p1
  var proxtwo=p2
}
else {
  var proxone=p2
  var proxtwo=p1
 }
```

Here, you store the IP address of your workstation into a variable (`myip`). You then automatically divide it into the four octets (splitting at the "."). Then you store each octet into an element of an array (`ipbits`). You extract the last octet, and call it "myseg". Divide the number by 2, discarding any remainder. Then multiply the result by 2. If the result is the same as the original number, it was even. If not, it was odd. Then populate the variables "proxone" and "proxtwo" accordingly.

```
//if name has no dots, or is our domain, or starts 10., or if my
//current address does not start 10. don't use proxy
if(isPlainHostName(host)  ||
  dnsDomainIs(host,".mydomain.co.uk") ||
  myip.substring(0,3)!=="10." ||
  host.substring(0,3)=="10." )
```

Now you apply logic to decide whether to try to talk to your proxy or not. The line `if(isPlainHostName(host)` means "if the name typed in does not contain any dots". That is, if the user has typed in a single word, assume that they are referring to a web server inside the DNS domain, and expect DNS resolution to supply the rest of the address. For example, if you use a workstation at your company where the DNS domain is mydomain.co.uk, and at a command prompt you enter **Ping www**, it pings www.mydomain.co.uk. This line performs a similar function for web browsing.

Note: The two vertical bars (||) represent `OR`.

The line `dnsDomainIs(host,".mydomain.co.uk")` means "if the domain of the specified host matches .mydomain.co.uk". So if you try to talk to a web server within the firewall, do not contact the proxy.

The line `myip.substring(0,3)!=="10." ||` means "if my current IP address does not begin 10.". That is if the user is not within our firewall, go directly to the web server.

The line `host.substring(0,3)=="10." )` means "if the IP address you are trying to reach begins 10.". That is if you have entered the IP address of the web server instead of the DNS name, and it is inside the firewall, go directly.

```
// alert("direct")
return "DIRECT";
}
  else {
//  alert("proxy")
  return "PROXY "+proxone+":8080; PROXY "+proxtwo+":8080" ;
}
```

The `alert` lines are commented out, but you can uncomment them for troubleshooting. The other lines mean "if the following test result in a TRUE value, return the value "DIRECT" to make the browser bypass the proxy. Otherwise, return a string containing the two proxies in the order you specified earlier".

Workstations on even IP addresses try to use the first named Proxy server (p1), and failover to the second (p2). Workstations with odd IP addresses try to use the second named proxy server (p2), and failover to the first (p1).

See "Planning to install the CSP for standalone server" on page 20.

Requirements for the Client Site Proxy for standalone server

The following table describes the requirements for installing the Client Site Proxy (CSP) for a standalone server.

Table 3-2 Requirements for CSP for a standalone server

Type of requirement	Description
Domain Membership	The CSP server needs to be a member of the domain that users will be authenticated against.
Firewall Access	The CSP server needs to have the following access to the Internet. These ports may need to be allowed on your firewall: ■ 53/TCP,UDP DNS (Domain Name System) Allow to all external addresses ■ [Port]/TCP HTTP used by [Proxy Address] Only allow Web Security IP ranges. See your provisioning documentation for this information In the list, the proxy address is shown as [Proxy Address] and the Port is shown as [Port]. Replace these entries with the proxy details included in your provisioning documentation. The CSP server must also be able to resolve names on the Internet. Ensure that the DNS setting are correct; these can be obtained from your Internet service provider .
Upstream Proxy Configuration	The proxy address and port details are included in your provisioning documentation.

Table 3-2 Requirements for CSP for a standalone server *(continued)*

Type of requirement	Description
Supported Operating Systems	■ Windows Server 2003 Service Pack 1 ■ Windows Server 2003 R2 Service Pack 2 ■ Windows XP Professional Service Pack 3 ■ Windows Server 2008 R2 Service Pack 1 (SP1) ■ Windows Server 2012 Although the CSP is supported on desktop operating systems, we recommend that you install the CSP on a server class operating system.
Hardware requirements	■ *Memory*—256 MB over OS requirement ■ *Disk*—500 MB free in C:drive ■ *Processor*—2 cores with 1GHz + **Note:** These are the minimum hardware requirements.

See “About performance sizing and the CSP for Standalone Server” on page 34.

Installing the Client Site Proxy for standalone server

In order to install CSP, you should have administrator permission because the CSP will stop/start the MS Windows service.

To install the standalone CSP

1. Double-click on **setup.exe**.

   You are presented with the installer.

2. Click **Next**
3. Read the license agreement, and if you accept, click **Next**.
4. Select whom the application is installed for, click **Next**.
5. Click **Install**
6. On the Completion page, click **Finish.**

See “Configuring the Client Site Proxy for standalone server” on page 26.

See “Stopping and starting the Client Site Proxy for standalone server” on page 27.

See “Logs for the Client Site Proxy for standalone server” on page 27.

Configuring the Client Site Proxy for standalone server

The file *c:\ClientSiteProxy\etc\squid.conf* contains the configuration options for your site. There are two sections that may need changing. After any configuration changes, the Client Site Proxy server needs to be restarted.

You need to configure the upstream proxy - the correct details for your site will be contained in your provisioning documentation. Any additional lines referencing different proxy details should be commented out (with '#' at the beginning of the line) or deleted.

```
#  TAG: cache_peer
cache_peer [Proxy Address] parent [Port] 0000 default no-query
```

Note: The proxy address is shown as [Proxy Address] and the Port is shown as [Port]. - replace these entries with the proxy details included in your provisioning documentation.

The second section defines the local networks. The standard configurations has all private network configured but if you wish to refine this to only your internal networks or add another network you may change this line. These networks are defined in RFCs 1918, 3330 and 3927 (RFCs are available at http://www.ietf.org/rfc.html). Only clients from these subnets will be able to use the CSP.

```
#  TAG: acl
acl our_networks src 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8 169.254.0.0/16
```

See "Installing the Client Site Proxy for standalone server" on page 25.

See "Stopping and starting the Client Site Proxy for standalone server" on page 27.

See "Logs for the Client Site Proxy for standalone server" on page 27.

Stopping and starting the Client Site Proxy for standalone server

The Installation automatically starts the proxy service, but for maintenance and fault finding it may be necessary to start or stop the service.

To start and stop the proxy service

1. **Start** > **Run** > **compmgmt.msc**
2. Open **Services and Applications** > **Services**
3. Right click on the service **Client Site Proxy**, select **Stop**. (Takes 30 seconds to stop)
4. Right click on the service and select **Start**.

See “Installing the Client Site Proxy for standalone server” on page 25.

See “Configuring the Client Site Proxy for standalone server” on page 26.

See “Logs for the Client Site Proxy for standalone server” on page 27.

Logs for the Client Site Proxy for standalone server

The following logs are available:

`c:\ClientSiteProxy\var\logs\access.log` Most log file analysis programs are based on the entries in *access.log*. Currently, there are two file formats possible for the log file, depending on your configuration for the *emulate_httpd_log* option. By default, Squid logs on in its native log file format. If the *emulate_httpd_log*option is enabled, Squid logs on in the common log file format as defined by the CERN web daemon.

`c:\ClientSiteProxy\var\logs\cache.log` The *cache.log* file contains the debug messages and error messages that Squid generates. Look in this file for automated error reports, when testing or searching for reasons of a perceived misbehavior, etc.

`c:\ClientSiteProxy\var\logs\store.log`	As caching is disabled on the CSP, this log file is redundant. The *store.log* file covers the objects currently kept on disk or removed ones. As a kind of transaction log it is usually used for debugging purposes. A definitive statement about whether an object resides on your disks is only possible after analyzing the *complete* log file. The release (deletion) of an object may be logged at a later time than the swap out (save to disk).

See “Installing the Client Site Proxy for standalone server” on page 25.

See “Configuring the Client Site Proxy for standalone server” on page 26.

See “Stopping and starting the Client Site Proxy for standalone server” on page 27.

Upgrading the Client Site Proxy for standalone server

Upgrades can be grouped into two kinds:

A patch or point upgrade	This is a minor release. This is the type of upgrade that is released to resolve outstanding issues and would not typically have additional features.
A version upgrade	This is a major release. This type of release has enhanced functionally and more features. Each release includes instructions on how to install the release.

The procedure below is a guide to approaching an upgrade.

For the major and minor releases of the standalone CSP, all upgrades should be treated the same.

Warning: Upgrading the CSP will cause the service to be unavailable while the upgrade is in progress.

To upgrade the Client Site Proxy for standalone server

1. Take a backup of all the configuration files **C:\ClientSiteProxy\etc\*.conf**
2. Stop the SquidNT service
3. Run the installer

4 Once the new installer has run compare the *squid.conf* files from the backup and the new install. Ensure that any custom settings that you had are re-entered into the new install. Enter the new settings if needed, and restart the SquidNT service.

5 Test the functionality of the CSP.

See "Troubleshooting - testing the Client Site Proxy with web Security policy rules" on page 29.

Removing the Client Site Proxy for standalone server automatically

To automatically remove the CSP

◆ Use **Control Panel** > **Add/Remove Programs** and remove the CSP.

Troubleshooting - testing the Client Site Proxy with web Security policy rules

Once the CSP is installed, the best way to ensure that the CSP service works is to create two policy rules in the portal. Then test that the CSP works using the procedure below.

Define two policy rules in the portal:

- A policy rule that denies a known web site for a particular user.
- A policy rule for the same web site that denies a local IP address.

For further information on defining Web Security policy rules, see the Online Help.

To test your firewall rules

1 Identify the following for testing:

   - 2 x user accounts (A and B)
   - 2 x workstations and their local IP address (X and Y)
   - 1 x web site for testing.

2 In the portal

3 Ensure that the domain and the user names exist

4 Ensure that the Local IP address exits

5 Create a custom URL group for the selected URL

6 Create a deny rule for user account A for this URL group

7 Create a deny rule for address X for this URL group

Once the rules have been applied, the expected test results should be:

	Workstation X	Workstation Y
User A	Web site is denied	Web site is denied
User B	Web site is denied	Web site is allowed

This set of rules can be used at any time to test the correct operation of the CSP.

Troubleshooting - checking the CSP logs (standalone server)

By default, both the cache_store_log and access_log are disabled. You can enable either by commenting out the following two lines in the *C:\ClientSiteProxy\etc\squid.conf*. Then restart the proxy service.

Table 3-3 Interpreting the CSP logs

Log file	Interpretation
c:\ClientSiteProxy\var\access.log	You should be able to see the requests to the web sites that your clients request. On each line you should be able to see the domain and the user name of each user making the request. See the example log below.
c:\ClientSiteProxy\var\cache.log	In normal operation there should be no entries that are generated in the log file apart from startup and shutdown information

Example c:\ClientSiteProxy\var\access.log

```
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
    "GET http://www.mozilla.org/images/header_tab.gif HTTP/1.0"
    200 4816 TCP_MISS:NONE
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
    "GET http://www.mozilla.org/images/header_br.gif HTTP/1.0"
    200 1064 TCP_MISS:NONE
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
```

```
    "GET http://www.mozilla.org/images/header_tr.gif HTTP/1.0"
    200 984 TCP_MISS:NONE
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
    "GET http://www.mozilla.org/images/key-point_back.gif HTTP/1.0"
    200 610 TCP_MISS:NONE
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
    "GET http://www.mozilla.org/images/header_tl.gif HTTP/1.0"
    200 1354 TCP_MISS:NONE
192.168.0.11 - company\administrator [11/Oct/2006:12:34:18 +1300]
    "GET http://www.mozilla.org/images/header_logo.gif HTTP/1.0"
    200 5682 TCP_MISS:NONE
```

Troubleshooting - checking the CSP client computers (standalone server)

The following detailed checks can be performed on the client server computers:

- Common errors—if your workstations have problems contacting the Internet through Web Security, perform the common connection checks on the client computers and on the Client Site Proxy server
- User Proxy Settings—Check that the user has the correct proxy setting for the CSP server, including the port number that the CSP listens on.

Note: If you use an internal DNS name for the CSP, ensure that the client system can resolve this name. Test whether the client computer can resolve the DNS name by performing an `nslookup` of the name of the CSP.

Troubleshooting - checking the CSP (standalone server)

The two main issues that may occur with the Client Site Proxy for a standalone server are:

- Service Hanging - Cannot contract upstream proxy
- Service does not respond to client requests

Use the following checks to troubleshoot these issues:

- *Service Hanging - Cannot contract upstream proxy*—The service does not respond to client requests.

1. On the CSP server open a **cmd** prompt.
2. Run **nslookup**.
3. Enter the host name of your **proxy address**.

The proxy address details for your site are included in your provisioning documentation.

Four lines are returned: the name of the DNS server name, the IP address, the ‘proxy address’ name, and its IP address. If the **nslookup** does not resolve, check the CSP DNS settings and your firewall. Ensure that this server is allowed DNS access to the Internet. When the issue is resolved, restart the SquidNT service.

Example error in log:

```
c:\ClientSiteProxy\var\logs\cache.log
2006/09/22 15:58:12| Performing DNS Tests...
FATAL: ipcache_init: DNS name lookup tests failed.
```

- *Service is not responding to client requests*—This issue can happen if the CSP service cannot contact the upstream proxy server. Ensure that the CSP system can resolve the upstream name, and that it can access this address on port 3128. When the issue is resolved, restart the SquIdNT service.

  Another cause of this issue is that the IP address is not provisioned for the service. Check whether it is provisioned in the portal.

  Example error in log:

```
2006/09/25 13:40:59| TCP connection to [Proxy Address]/[Port] failed
2006/09/25 13:40:59| Detected DEAD Parent: [Proxy Address]/[Port]/0
2006/09/27 09:46:29| Failed to select source for ‘http://www.google.com/’
2006/09/27 09:46:29|   always_direct = 0
2006/09/27 09:46:29|    never_direct = 1
2006/09/27 09:46:29|        timedout = 0
```

In the log example, the proxy address is shown as [Proxy Address] and the Port is shown as [Port]. These entries are replaced with the details included in your provisioning documentation.

Example client errors (displayed in web browser):

```
ERROR
The requested URL could not be retrieved
--------------------------------------------------------------------------------
While trying to retrieve the URL: http://www.examplewebsite.com/isapi/redir.dll?
```

```
The following error was encountered:
Connection to [Proxy Address] Failed
The system returned:
   (10060) WSAETIMEDOUT, Connection timed out.
The remote host or network may be down. Try the request again.
```

In the log example, the proxy address is shown as [Proxy Address]. This entry is replaced with the proxy details included in your provisioning documentation.

```
ERROR
The requested URL could not be retrieved
--------------------------------------------------------------------------------
While trying to retrieve the URL: http://www.examplewebsite.com/
The following error was encountered:
Unable to forward this request at this time.
This request could not be forwarded to the origin server or to any parent caches.
The most likely cause for this error is that:
The cache administrator does not allow this cache to make direct connections to
origin servers, and all configured parent caches are currently unreachable.
```

Chapter 4

Client Site Proxy for Standalone Server - Performance Sizing Guide

This chapter includes the following topics:

About performance sizing and the CSP for Standalone Server

This aim of this guide is to help you to determine the number of Client Site Proxy (CSP) Standalone servers to deploy in your network environment to support your user base and traffic profile.

The CSP for Standalone Server is the component of the Web Security service that you install on-site on a Microsoft Windows server.

The CSP captures information that is specific to the user's computer that is making requests to the Internet. To achieve this, the CSP authenticates the user making the Web request against the domain controller, captures and encrypts details of the domain name, user name, and local IP address and adds them to the HTTP request as custom HTTP headers. This is information is utilized together with information on the user that is held by the service to apply policy specifically to the user as defined in the portal.

About the CSP test environment

We conducted the tests in a controlled environment that simulated high traffic load to test the performance limits of the CSP.

We tested versions 1.0.18 and 1.0.20 of the CSP under two simulated user traffic loads to determine the maximum number of users that could be supported before performance began to degrade.

Note: The performance and capacity of CSP for Standalone Server versions 1.0.18 and 1.0.19 are equivalent.

We used the following system resource configuration to test both versions of the CSP:

Table 4-1 System resource configuration for CSP tests

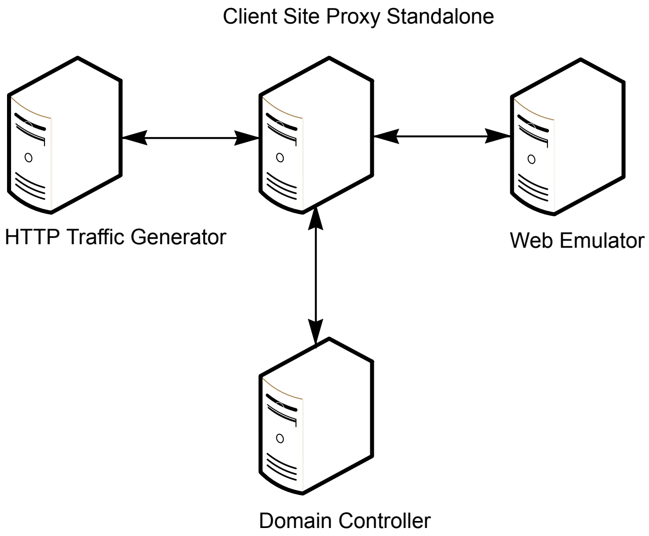
Component	CSP for Standalone Server hardware configuration and version	Domain controller server hardware configuration and version
Processor	1 Dual core 3.0 GHz CPU	2 Quad Core Intel Xeon 2.33 GHz CPUs
Memory	2 GB RAM	4 GB RAM
Disk space	140 GB Ultra fast SCSI	140 GB Ultra fast SCSI
Operating system	Windows 2008 SP2 (32-bit)	Windows 2008 SP2 (32-bit)
NIC	Copper 1 GB/100 MB Ethernet NIC	Copper 1 GB/100 MB Ethernet NIC

Testing the CSP on a virtualized environment was beyond the scope of this guide. You should expect some performance degradation if you choose to deploy the CSP on a virtualized environment when compared to a dedicated system with similar system resources.

All systems were set up on Windows 2008; we do not expect the results to vary significantly for other versions of the Windows operating system.

Figure 4-1 shows the test environment. The HTTP traffic generator acts as a client simulator, and requests Web traffic from the Web emulator. The Web emulator acts as a Web server simulator, and serves Web content that is requested by the traffic generator.

Figure 4-1 CSP for Standalone Server test environment



We did not include any Web Security infrastructure in the tests as the sizing guidelines are specific to the CSP Standalone component. Our tests were developed to determine the incremental latency that is introduced by the CSP Standalone application, its capacity, and any performance bottlenecks, in an ideal network environment.

It is possible that CSP Standalone application, along with local network limitations and the destination (origin) server, may impact the user throughput and latency levels seen in a real-world environment.

The Web traffic load generation testing tool used a member-space of 10,000 domain users.

About the CSP tests

We analyzed data from our global infrastructure to create realistic per-user traffic profiles.

A traffic profile represents the Web usage profile of users, and includes metrics such as connections per user, average size of requests and number of Web requests per second per connection. We used these profiles to test the limits of the CSP for Standalone Server.

Our tests were designed to determine the achievable throughput of the CSP when using the recommended system resource configuration, and to estimate how many servers may be needed for a given user base.

We measured the incremental latency that the CSP Standalone added when performing proxy authentication against the domain controller. The tests were performed under varying load conditions with different request rates and size of Web content until either the incremental latency increased significantly or the CSP Standalone generated errors indicating that it could no longer successfully process the web requests at the current traffic volume, that is, at the CSP Standalone capacity limit.

To simulate Web traffic, we used Web Polygraph (http://www.web-polygraph.org) Web traffic load generator to send HTTP GET requests through a CSP to a Web emulator that served the Web contents for the requested domains.

HTTP requests were generated at increasing rates until the maximum supportable throughput levels were achieved.

To simulate a real-world deployment, the traffic was generated with requests directed to different Web site addresses served by the Web emulator. Each connection through the CSP Standalone was individually authenticated. Authentication was performed again after every 30 requests per connection. This is a setting within the test harness used to exercise the CSP Standalone’s IP authentication credential cache. The related CSP parameter is *authenticate_ip_shortcircuit_ttl.*

For all test scenarios, measurements were taken for throughput levels (in both megabits per second and connections/requests per second) and average latency for Web transactions. We also monitored memory and CPU utilization levels. The measurement of the Web request transaction latency was the primary criteria that we used to determine when the CSP Standalone had reached its supported capacity limit.

We used Windows NTLM authentication protocol. This is used by the CSP to authenticate users making Web requests against the domain controller.

We did not include tests with authenticated HTTPS traffic. The effect to the performance and overall capacity of the CSP due to HTTPS requests versus HTTP requests is expected to be minimal and therefore not material to our recommendations.

All web requests were HTTP GET requests generating a Web page response/download.

Results of the CSP tests

Table 4-2 and Table 4-3 show the results for CSP versions 1.0.18 and 1.0.20. These are the figures for network throughput, web request processing rates, and average transaction processing time that you can expect from a single CSP for Standalone Server.

Table 4-2 Test results for CSP for Standalone Server version 1.0.18

	Typical usage profile	High usage profile
Size of Web content (KB)	10	20
Number of requests per second per connection	0.07	0.13
Maximum number of concurrent Web connections per second	1,540	1,530
Throughput (Mbps)	9	33
Incremental processing delay (microsecond)	7	9
Connections per user ratio	3	3
Maximum number of concurrent users	513	510
Provisioned:concurrent user ratio	2.5	2.5
Maximum number of provisioned users	1,282	1,275

Table 4-3 Test results for CSP for Standalone Server version 1.0.20

	Typical usage profile	High usage profile
Size of Web content (KB)	10	20
Number of requests per second per connection	0.07	0.13
Maximum number of concurrent Web connections per second	7,200	4,800
Throughput (Mbps)	41	102
Incremental Processing delay (microsecond)	100	100
Connections per user ratio	3	3
Maximum number of concurrent users	2,400	1,600

Table 4-3 Test results for CSP for Standalone Server version 1.0.20 *(continued)*

	Typical usage profile	High usage profile
Provisioned:concurrent user ratio	2.5	2.5
Maximum number of provisioned users	6,000	4,000

- *Size of Web content* - The average size of Web content through the CSP in KB.
- *Number of requests per second per connection* - The average number of web requests per second for every connection.
- *Maximum number of concurrent users* - The maximum recommended capacity in terms of concurrent user connections that can be supported. Further testing showed that the CSP failed when traffic exceeds the numbers listed above and is therefore not recommended.
- *Throughput* - The maximum raw throughput reached during the tests. The connection limit was reached well before the throughput limit. Consequently, your sizing of the CSP should not be based on throughput.
- *Incremental processing delay* - The incremental latency added by the CSP when operating at the maximum number of concurrent connections.
- *Connections per user ratio* - The ratio of the average number of Web requests per connnections initiated by each individual user. This is based on a sampling of the connection ratios across a variety of our customer environments. Customers with higher or lower ratios of connections/user can adjust this number to arrive at a sizing estimate matched to their specific circumstances
- *Maximum number of concurrent users* - The number of active or simultaneous users who are using the CSP. The figure is derived by dividing the maximum number of connections by the connections/user ratio.
- *Provisioned: concurrent user ratio* - The ratio of subscribed or provisioned users to the number of active or concurrent users. The figure is based on a sampling of the user ratios across a variety of our customers. Customers with higher or lower ratios of active to provisioned users can adjust this number to arrive at a sizing estimate that is matched to their specific circumstances.
- *Maximum number of provisioned users* - This is derived by multiplying the maximum number of concurrent users by the provisioned: concurrent user ratio.

See “Additional information for CSP for Standalone Server version 1.0.20” on page 41. This section provides information on alternative latency data points and the corresponding number of connections for CSP Standalone version 1.0.20.

Using this guide to plan your CSP deployment

We recommend that you keep in mind the following when planning your CSP deployment:

- You should validate the sizing guidelines and assumptions in terms of how they apply to your own test and production environments before deployment.
- You should test with policies and configurations that are consistent with your specific deployment scenario.
- You should carry out testing with a traffic profile that is consistent with your live production environment and use this profile together with this guide to determine the most suitable sizing estimate.

Understanding your organization’s current web traffic will help you to determine the number of CSP servers that are required to stay within the connection, throughput, and response time limits shown in this guide. The Web traffic and number of user connections that needs to be processed in a CSP deployment can often be obtained from the network switch or firewall.

To help you to size the CSP, we offer a tool that enables you to extract various metrics from your proof of concept CSP environment and use them to estimate the number of CSP servers that are required to support your user base.

Click CSP Sizing Tool to download the tool. See the documentation included with the tool for information on installation and usage.

When the user traffic volume is known, your server requirements can be roughly estimated by extrapolating from the testing numbers that are shown in Table 4-4. The estimates assume that:

- The traffic profile is based on typical user usage as described in this guide.
- Load distribution is equal across all servers
- There is no redundancy

Multiple CSP Standalone servers can be deployed to support user numbers in excess of the figures that are shown in Table 4-4. You can distribute user traffic across multiple CSP servers as necessary. It is common for large user locations to deploy the CSP Standalone in a redundant, load-balanced configuration.

Table 4-4 Estimating the number of CSP Standalone servers

Number of provisioned users	Number of dedicated servers required - CSP for Standalone Server version 1.0.18	Number of dedicated servers required - CSP for Standalone Server version 1.0.20
1,000	1	1
2,000	2	1
5,000	4	1
10,000	8	2
20,000	16	4

Additional information for CSP for Standalone Server version 1.0.20

The following tables provide additional information on alternative latency data points and the corresponding number of connections for CSP for Standalone Server version 1.0.20.

Table 4-5 Typical usage latency versus connections

Latency	Connections
10	2,408
20	3,838
30	4,286
40	5,072
50	5,588
60	5,818
70	6,368
80	6,740
90	7,118
100	7,208

Table 4-6 High usage latency versus connections

Latency	Connections
10	1,718
20	2,640
30	3,338
40	3,832
50	4,042
60	4,208
70	4,374
80	4,540
90	4,688
100	4,816

Chapter 5

Client Site Proxy for ISA server

This chapter includes the following topics:

- Troubleshooting - checking the CSP (ISA server)
- Troubleshooting malformed Web pages with CSP for ISA Server

Installing the Client Site Proxy for ISA server step by step

The following table provides an overview of the tasks involved in installing and using the Client Site Proxy (CSP) for ISA server.

Table 5-1 Overview of tasks

Task	More information
Request flow	See "Request flow for Client Site Proxy for ISA server" on page 44.
Planning to install	See "Planning to install the CSP for ISA server" on page 45.
Requirements for installing	See "Requirements for installing the Client Site Proxy for ISA server" on page 46.
Installing	See "Installing the Client Site Proxy for ISA server" on page 48.
Configuring the CSP plugin	See "Process overview – configuring the CSP plugin for ISA server" on page 51.
Upgrading	See "Upgrading the Client Site Proxy for ISA server" on page 49.
Removing the CSP manually	See "Removing the Client Site Proxy for ISA server (Standard Edition) manually" on page 56.
Removing the CSP automatically	See "Removing the Client Site Proxy for ISA server automatically" on page 56.

See "Troubleshooting - testing the Client Site Proxy with web Security policy rules" on page 29.

Request flow for Client Site Proxy for ISA server

The request flow shows the environment where Web Security is deployed with the CSP for ISA server installed. It is worth noting that NTLM authentication is per connection not per request.

Note: The first request will follow all steps but future requests for this TCP session will be replaced by a simple one step request for the web page.

CSP request flow for ISA server

1. The client sends an unauthenticated request to the ISA server
2. The ISA server responds with "Authentication required" of type NTLM 407, unlike a web server 401 response
3. The client sends the user name to the server (in plain text, base-64 encoded).
4. The ISA server generates a 16-byte random number, called a challenge, and sends it to the client.
5. The client encrypts this challenge with the hash of the user's password and returns the result to the ISA server. This is called the response.
6. The ISA server sends the following three items to the domain controller: User name, Challenge sent to the client and Response received from the client
7. The domain controller uses the user name to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge. The domain controller compares the encrypted challenge it computed to the response computed by the client. If they are identical, authentication is successful.
8. The CSP adds the custom HTTP headers that contain the domain\username and local IP address encrypted. The ISA server requests the page from Web Security.
9. Web Security decrypts the headers and evaluates the request against rules in the portal. Rules can now be applied to groups and client IP. If allowed, the page is now requested from the original web server
10. Web Security receives the web page and evaluates the request against rules in the portal.
11. Web Security returns the page to the ISA server
12. The ISA server returns the web page to the client.

Planning to install the CSP for ISA server

For the sites that currently use ISA servers, it is recommended that the Client Site Proxy for ISA server is installed onto existing ISA servers.

The Client Site Proxy for ISA server requires changes to the ISA server firewall rules. Firewall rules are included with the CSP installation. These firewall rules should be treated as examples only. The rules are very broad and may not suit your security requirements. In some cases may interfere with other applications.

The key factors to remember when you create and test the firewall rules are:

- FTP, HTTP, and HTTPS traffic must be authenticated

  Authenticating this traffic ensures that the Domain and Username are captured. The Domain and Username can then be securely added to the HTTP request by the Client Site Proxy for ISA server.

- All web traffic is web proxy chained to Web Security.

  All HTTP requests to be directed to Web Security for scanning.

- Web caching is disabled

  All proxies in the chain must not have caching enabled. Caching affects rule-processing. A page is held in the local ISA cache and served directly to the client. As no request is made to the upstream proxy, no rules are processed.

Note: If the ISA server acts as an edge device, then even more care should be taken with rule creation. Bad placement or incorrectly configured rules may even create security issues for your organization. If you are unsure of how to properly configure ISA server firewall rules then it is recommended that you consult a specialist in this area.

Requirements for installing the Client Site Proxy for ISA server

The following table describes the requirements for installing the CSP for ISA server.

Table 5-2 Requirements for CSP for ISA server

Type of requirement	Description
Domain Membership	The ISA server needs to be a member of the domain that the users will be authenticated against.

Table 5-2 Requirements for CSP for ISA server *(continued)*

Type of requirement	Description
Firewall Access	The CSP plug-in needs to have the following access to the internet. These ports may need to be allowed on your firewall if the ISA server is not your edge device: ■ 53/TCP,UDP DNS (Domain Name System) Allow to all external addresses ■ [Port]/TCP HTTP used by [Proxy Address] Only allow Web Security IP ranges. See your provisioning documentation for this information In the list, the proxy address is shown as [Proxy Address] and the Port is shown as [Port]. Replace these entries with the proxy details included in your provisioning documentation. The CSP server and ISA server must also be able to resolve names on the internet. Ensure that the DNS setting are correct; these can be obtained from your Internet Service Provider.
Upstream Proxy Configuration	The proxy address and port details are included in your provisioning documentation.
Supported ISA Versions	These are the supported ISA versions: ■ ISA server 2004 ■ ISA server 2006
Minimum Requirements for ISA server 2004	These are the minimum requirements for ISA server 2004 ■ *Processor:* PC with a 550 MHz Pentium III or higher processor ■ *Operating System:* Microsoft Windows server 2003 (Standard or Enterprise Edition), Microsoft Windows 2000 server or advanced server with Service Pack 4 (SP4) or later, or Windows 2000 Datacenter server. For ISA server 2004 Enterprise Edition, Windows server 2003 (Standard or Enterprise Edition) is required. ■ *Memory:* 256 MB of RAM or more is recommended. ■ *Hard Disk:* NTFS-formatted local partition with 150 MB of available hard-disk space; additional space will be required for web cache content.

Table 5-2 Requirements for CSP for ISA server *(continued)*

Type of requirement	Description
Minimum Requirements for ISA server 2006	These are the minimum requirements for ISA server 2006 ■ *Processor:* PC with a 733 MHz Pentium III or higher processor ■ *Operating System:* Microsoft Windows server 2003 32-bit operating system with Service Pack 1 (SP1) or Microsoft Windows server 2003 R2 32-bit. ■ *Memory:* 512 MB of RAM or more is recommended. ■ *Hard Disk:* NTFS-formatted local partition with 150 MB of available hard-disk space; additional space will be required for web cache content.
Other devices	The following other devices are required: ■ Network adapter that is compatible with the computer's operating system for communication with the internal network; one additional network adapter, modem, or ISDN adapter for each additional network connected to the ISA server computer ■ One additional network adapter is required for intra-array communications for ISA server Enterprise Edition integrated NLB ■ CD-ROM or DVD-ROM drive ■ VGA or higher-resolution monitor ■ Keyboard and Microsoft Mouse or compatible pointing device **Note:** Actual system requirements will vary based on your deployment configuration, expected load, and the features you choose to install.

Installing the Client Site Proxy for ISA server

Note: You must install the Client Site Proxy for ISA server on the same drive as the Microsoft ISA server. For example, if you have installed Microsoft ISA server on drive C:, then you must install the Client Site Proxy on drive C: also.

If you are installing the Client Site Proxy for ISA server Enterprise Edition, you must have the ISA administrator permission and you can connect to the Configuration Storage server.

To install the ISA plug-in

1. Double-click on **csp_isa_setup.exe**.

   The initial installation screen is displayed.

2. Click **Next**.

   Read the license agreement, and if you accept it, click **Next**.

3. Select who the software will be installed for, then click **Next**.

   If **only for me** is selected, then only this user will be able to uninstall the software.

4. Select the destination folder. You must install the Client Site Proxy for ISA server on the same drive as the Microsoft ISA server. Then click **Next**.

5. Choose the installation method that matches your ISA server deployment. Then click **Next**.

   if you are using the ISA Standard Edition, you can only select **Register the web filter in ISA Standard Edition**. If you are using the ISA Enterprise Edition, you can select **Register the web filter as an Array Add-in** or **Register the web filter as an Enterprise Add-in**.

   If the web filter is registered as an Enterprise Add-in, the settings of the web filter will be applied to each array member, and the filter cannot be disabled in an array configuration unless the web filters are disabled in the enterprise configuration.

   If the web filter is registered as an Array Add-in, each array member computer can enable/disable/modify the web filters settings.

   If you selected Register the web filter in ISA Standard Edition, go on to step 6. Otherwise, specify the Configuration Storage server or IP address for the ISA Enterprise Edition. Click Check Connection to test the connection.

   After the check, click **Next**.

6. Click **Install**.

7. Click **Finish**.

Upgrading the Client Site Proxy for ISA server

Upgrades can be grouped into two kinds:

A patch or point upgrade	This is a minor release. This is the type of upgrade that is released to resolve outstanding issues and would not typically have additional features.

A version upgrade	This is a major release. This type of release has enhanced functionally and more features. Each release includes instructions on how to install the release.

The procedure below is a guide to approaching an upgrade.

For the major and minor releases of the CSP for ISA server, all upgrades should be treated the same.

Warning: Upgrading the CSP causes the service to be unavailable while the upgrade is in progress.

To upgrade the Client Site Proxy for ISA server

1. Click **Start** > **Control Panel**, select **Add or Remove Programs**.
2. Select **Client Site Proxy For ISA server** and click **Remove**. If you use an early CSP plug-in, you may need to remove the plug-in manually.

   The CSP plug-in will now not work.
3. Open a **cmd** window, type `regsvr32 /u C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll` and press **Enter**.

   After a few moments a confirmation dialog should appear indicating success.
4. Run the upgrade installer.

   The next steps check to see if the web filter is installed:
5. Start the ISA server administration application. Do one of the following:
   - If you use ISA Standard Edition, in the left pane, expand **Configuration**, select **Add-ins**.
   - If you use ISA Enterprise Edition and CSP is registered as an Array Add-in, expand **Configuration** under the Arrays, select **Add-ins**.
   - If you use ISA Enterprise Edition and CSP is registered as an Enterprise Add-in, select **Enterprise Add-ins** under the Enterprise.
6. Open a **cmd** window, type `regsvr32 C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll` and press **Enter**.

   After a few moments a confirmation dialog should appear indicating success.
7. Click on the **Web Filters** tab. **Client Site Proxy Filter** should appear in the list of installed filters. If it does not appear after a few moments, register the filter manually (if you use the Standard Edition).
8. Test the functionality of the CSP.

See "Troubleshooting - testing the Client Site Proxy with web Security policy rules" on page 29.

Process overview – configuring the CSP plugin for ISA server

The following table shows the steps that are involved in configuring the Client Site Proxy (CSP) plugin for ISA server.

The configuration process establishes a firewall rule to force client authentication.

Table 5-3 Steps to configure the CSP plugin

Step	Further information
Create a firewall rule to force client authentication – by import process (recommended) or manually	See "Creating a firewall rule to force client authentication by import for CSP for ISA server" on page 51. See "Creating a firewall rule to force client authentication manually for CSP for ISA server " on page 52.
Configure integrated network authentication	See "Configuring integrated network authentication for CSP for ISA server" on page 53.
Configure network web chaining	See "Configuring network web chaining for CSP for ISA server" on page 54.
Disable web caching	See "Disabling web caching for CSP in ISA server" on page 54.
Check that the web filter is installed	See "Checking that the web filter is installed for CSP in ISA server" on page 55.

Creating a firewall rule to force client authentication by import for CSP for ISA server

Establishing the rule to force client authentication can be performed with a semi-automated import process described here. Or the rule can be established manually.

See "Creating a firewall rule to force client authentication manually for CSP for ISA server " on page 52.

We recommend that you use the import process.

To establish a rule using an import process

1. Start the ISA server admin GUI.
2. On the left pane, right click on **Firewall Policy** and select **Import**.

   If you are using ISA server Enterprise Edition, click **Array** and then array name. Then right click **Firewall Policy**, and select **Import**.
3. Navigate to **C:\Program Files\MessageLabs\Client Site Proxy for ISA Server**.
4. Either:
   - If you are using ISA server standard Edition 2004, select **WWWFirewallRule2004.xml**.
   - If you are using ISA server standard Edition 2006, select **WWWFirewallRule2006.xml**.
   - If you are using ISA server Enterprise Edition 2004, and you want to import the firewall rule for an array, select **WWWFireWallRuleForArray2004.xml**.
   - If you are using ISA server Enterprise Edition 2006, and you want to import the firewall rule for an array, select **WWWFireWallRuleForArray2006.xml**
5. Click **Import**.
6. Ensure that the new rule is at the top of the list. Right click it and select **Move Up** until it is.

Creating a firewall rule to force client authentication manually for CSP for ISA server

We recommend that you establish the rule to force client authentication using the import process. However, if the import process fails, you can establish the rule with the manual process described here.

See “Creating a firewall rule to force client authentication by import for CSP for ISA server” on page 51.

To establish the rule manually

1. Start the ISA server admin GUI.
2. On the left pane, expand the local server and click on **Firewall Policy**.
3. On the right, click on **Firewall Policy Tasks/Create New Access Rule**, a wizard is displayed.
4. In the wizard, give the policy a name, for example *Force WWW authentication*, click **Next**.

5 In the **Rule Action** page, click **Allow**. Then click **Next**.

6 In the **Protocols** page, select **Selected protocols**, click **Add**, expand **All Protocols**, and select **HTTP**, **HTTPS**, and **FTP**. Then click **Next**.

7 In the **Access Rule Sources** page, click **Add**, expand **Networks**, and select **Internal**. Click **Close** and then **Next**.

8 In the **Access Rule Destinations** page, click **Add**, expand **Networks** and select **External**. Click **Close** and then **Next**.

9 In the **User Sets** page, there may be a default **All Users** item listed. This must be removed and **All Authenticated Users** must be added.

To do so, select **All Users** and click **Remove**.

Then click **Add**, select **All Authenticated Users**. Click **Add** and then **Close**.

10 Click **Next**.

11 Click **Finish**.

12 At the top of the center pane, click **Apply**.

The progress of your new configuration is displayed.

13 Ensure that the new rule is at the top of the list. Right click it and select **Move Up** until it is.

Configuring integrated network authentication for CSP for ISA server

The required firewall rule will ensure that all traffic is authenticated against the user domain. Selecting **Integrated** is the most common solution as this utilizes NTLM authentication which is transparent to the user. Also, other authentication methods do not provide all the information required by the Client Site Proxy for ISA server.

You must also select a web proxy port number. Port 8080 is a common port number for internal proxy servers.

To configure integrated network authentication

1 Start the ISA server admin GUI

2 In the left pane, (if you are using ISA Enterprise Edition, expand the array), expand **Configuration** and select **Networks**. In the right pane select **Local Host**.

3 Right-click and select **Properties**.

4 In the **Local Host Properties** page, click the **Web Proxy** tab. Check the **Enable Web Proxy Clients**, **Enable HTTP** boxes, and enter the desired port number (8080).

5 Click **Authentication**. Ensure that **Integrated** is the only option selected, and click **OK**.

6 In the left pane, expand **Configuration** and select **Networks.** In the right pane, select **Internal**.

7 In the **Internal Properties** page, select the **Domains** tab.

8 Click **Add** and browse for your domain. Click **OK**.

9 Click **OK** and then **Apply Settings**.

See “Process overview – configuring the CSP plugin for ISA server” on page 51.

Configuring network web chaining for CSP for ISA server

To configure network web chaining

1 Start the ISA server admin GUI.

2 In the left pane (if you are using ISA Enterprise Edition, expand the array), expand **Configuration**, select **Networks**, and select the **Web Chaining** tab.

3 Right click on the **Last Default Rule** and select **Properties**.

4 Select the **Action** tab

5 Select **Redirect to a specified upstream server**.

6 Select **Settings**.

7 Enter your *[Proxy Address]* for the **Server** and the correct *[Port]*for both the **Port** and **SSLPort**. The correct details are included in your provisioning documentation. Uncheck all other check boxes.

8 Select **OK**.

Disabling web caching for CSP in ISA server

To disable web caching

1 Start the ISA server admin GUI.

2 In the left pane (if you are using ISA Enterprise Edition, expand the array), expand **Configuration**, select **Cache**, and select the **Cache Rules** tab.

3 Right click and select **Properties** on the **Last Default Rule**.

4 Select the **HTTP** tab and uncheck **Enable HTTP caching**.

5 Select the **FTP** tab and uncheck **Enable FTP caching**.

6 Click **OK**.

Checking that the web filter is installed for CSP in ISA server

To check that the web filter is installed

1 Start the ISA server admin GUI.

2 Do one of the following:

- If you are using ISA Standard Edition, in the left pane, expand **Configuration**, select **Add-ins**.
- If you are using ISA enterprise edition and CSP is registered as an Array Add-in, expand **Configuration** under the Arrays, select **Add-ins**.
- If you are using ISA enterprise edition and CSP is registered as an Enterprise Add-in, select **Enterprise Add-ins** under the Enterprise.

3 Click on the **Web Filters** tab. **Client Site Proxy Filter** should appear in the list of installed filters.

If the **Client Site Proxy Filter** does not appear, do one of the following:

- If you are using ISA server Standard Edition, register the filter manually.See the following procedure.
- If you are using ISA Enterprise Edition, check that you have the ISA administration permission and the Configuration Storage server can be connected.

To register the filter manually (ISA server Standard Edition)

1 In Windows Explorer, copy the `ClientSiteProxy.dll` file from `C:\Program Files\MessageLabs\Client Site Proxy for ISA Server\` to `C:\Program Files\Microsoft ISA Server\`.

If you installed the ISA plugin in a folder other than the default folder, amend these paths accordingly.

2 At a command prompt, type **regsvr32 C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll** and click **Enter**.

After a few moments a confirmation message is displayed.

Removing the Client Site Proxy for ISA server (Standard Edition) manually

This procedure describes how to remove the Client Site Proxy manually.

To manually remove the CSP in ISA Standard Edition

1. Open a **cmd** window, type `regsvr32 /u C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll` and press **Enter**.
2. After a few moments a confirmation dialog should appear indicating success.

   The CSP plug-in will now not work.
3. Delete the file **C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll**.
4. Manually remove the Firewall rule added
5. Manually remove the **Integrated Network Authentication** settings

See “Removing the Client Site Proxy for ISA server automatically” on page 56.

Removing the Client Site Proxy for ISA server automatically

This procedure describes how to remove the CSP automatically.

To remove the CSP automatically

1. Go to **Control Panel** > **Add/Remove Programs** and remove the plug-in.
2. Manually remove the Firewall rules that are added.
3. Manually remove the **Integrated Network Authentication** setting.

See “Removing the Client Site Proxy for ISA server (Standard Edition) manually” on page 56.

Troubleshooting - checking the CSP (ISA server)

The three main issues that may occur with the Client Site Proxy for ISA server are:

- The CSP ISA plug-in does not have any custom logs within ISA.
  The best way to check that the CSP works correctly is with two policy rules in the portal.
  See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.
- To see the standard ISA server logs:

1. Start the ISA server administration console.
2. In the left pane, select **Monitoring**.
3. In the right pane, select **Start Query** or **Edit Query** as necessary.

You can now see queries to the ISA firewall.

- ISA server cannot contact upstream proxy

  The cause may be network issues or firewall rules on the local ISA server or (if the ISA server is not the edge device) on the edge firewall.

  Example client error (displayed in web browser):

```
Network Access Message: The page cannot be displayed

Explanation: The request timed out before the page could be retrieved.

Try the following:
Refresh page: Search for the page again by clicking the Refresh button.
The timeout may have occurred due to Internet congestion.
Check spelling: Check that you typed the web page address correctly.
The address may have been mistyped.
Contact website: You may want to contact the website administrator to
make sure the web page still exists. You can do this by using the e-mail
address or phone number listed on the website home page.
If you are still not able to view the requested page, try contacting
your administrator or Helpdesk.

Technical Information (for support personnel)
Error Code 10060: Connection timeout
Background: The gateway could not receive a timely response from the
website you are trying to access. This might indicate that the network
is congested, or that the website is experiencing technical difficulties.
Date: 3/10/2006 1:34:34 a.m.
Server: fw.Company.local
Source: Firewall
```

See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.

Troubleshooting malformed Web pages with CSP for ISA Server

Malformed web pages can be the result of the ISA Server giving out cached parts of pages.

To fix this, turn off CARP (Cache Array Routing Protocol) in the cache rules. However, even if you turn off the last cache rule, cache array routing still functions so you should also set the cache size to zero to stop the ISA Server(s) from giving out cached parts of pages.

See "Installing the Client Site Proxy for ISA server step by step" on page 44.

Chapter 6

Client Site Proxy for Forefront TMG server

This chapter includes the following topics:

- Troubleshooting - checking the CSP (TMG server)

Installing the Client Site Proxy for TMG server step by step

The following table provides an overview of the tasks involved in installing and using the Client Site Proxy (CSP) for TMG server.

Table 6-1 Overview of tasks

Task	More information
Request flow	See "Request flow for Client Site Proxy for TMG server" on page 60.
Planning to install	See "Planning to install the CSP for TMG server" on page 61.
Requirements for installing the CSP	See "Requirements for installing the Client Site Proxy for TMG" on page 62.
Installing the CSP	See "Installing the Client Site Proxy for TMG server" on page 64.
Configuring the CSP plugin	See "Process overview – configuring the CSP plugin for TMG server" on page 65.
Upgrading the CSP	See "Upgrading the Client Site Proxy for TMG server" on page 70.
Removing the CSP manually	See "Removing the Client Site Proxy for TMG Standard Edition manually" on page 72.
Removing the CSP automatically	See "Removing the Client Site Proxy for TMG server automatically" on page 71.

See "Troubleshooting - testing the Client Site Proxy with web Security policy rules" on page 29.

Request flow for Client Site Proxy for TMG server

The request flow shows the environment where Web Security is deployed with the CSP for Forefront TMG installed. It is worth noting that NTLM authentication is per connection not per request.

Note: The first request will follow all steps but future requests for this TCP session will be replaced by a simple one step request for the web page.

Request flow for CSP with TMG server

1 The client sends an unauthenticated request to the Forefront TMG .

2 The Forefront TMG responds with "Authentication required" of type NTLM 407, unlike a web server 401 response

3 The client sends the user name to the server (in plain text, base-64 encoded).

4 The Forefront TMG generates a 16-byte random number, called a challenge, and sends it to the client.

5 The client encrypts this challenge with the hash of the user's password and returns the result to the Forefront TMG. This is called the response.

6 The Forefront TMG sends the following three items to the domain controller: User name, Challenge sent to the client and Response received from the client

7 The domain controller uses the user name to retrieve the hash of the user's password from the Security Account Manager database. It uses this password hash to encrypt the challenge. The domain controller compares the encrypted challenge it computed to the response computed by the client. If they are identical, authentication is successful.

8 The CSP adds the custom HTTP headers that contain the domain\username and local IP address encrypted. The Forefront TMG requests the page from Web Security

9 Web Security decrypts the headers and evaluates the request against rules in the portal. Rules can now be applied to groups and client IP. If allowed, the page is now requested from the original web server

10 Web Security receives the web page and evaluates the request against rules in the portal.

11 Web Security returns the page to the Forefront TMG.

12 The Forefront TMG returns the web page to the client.

Planning to install the CSP for TMG server

For the sites that use Forefront TMG, it is recommended that the CSP is installed onto the existing Forefront TMG.

For the sites where Forefront TMG instances are members of an array, the CSP must be installed on each array member after it has joined the array. For an array that is controlled by an Enterprise Management server (EMS), the CSP is not installed onto the EMS computer itself.

The CSP for Forefront TMG requires changes to the firewall rules.

The CSP installation includes firewall rules as examples only. These firewall rules are very broad and may not suit your security requirements. In some cases they may interfere with other applications.

The key factors to remember when you create and test the firewall rules are:

- FTP, FTP over HTTP, and HTTPS traffic must be authenticated
  Authenticating this traffic ensures that the Domain and Username are captured. The Domain and Username can then be added securely to the HTTP request by the Client Site Proxy for Forefront TMG .
- All web traffic is web proxy chained to Web Security.
  All HTTP requests to be directed to Web Security for scanning.
- Web caching is disabled.
  All proxies in the chain must not have caching enabled. Caching affects rule-processing. The page is held in the local TMG cache and served directly to the client. As no request is made to the upstream proxy, no rule processing is possible.

If TMG acts as an edge device, then even more care should be taken with rule creation. Bad placement or incorrectly configured rules may even create security issues for your organization. If you are unsure of how to properly configure TMG firewall rules then it is recommended that you consult a specialist in this area.

Requirements for installing the Client Site Proxy for TMG

The following table describes the requirements for installing the CSP for TMG .

Table 6-2 Requirements for CSP for TMG server

Type of requirement	Description
Domain Membership	The Forefront TMG needs to be a member of the domain that the users will be authenticated against.

Table 6-2 Requirements for CSP for TMG server *(continued)*

Type of requirement	Description
Firewall Access	The Forefront TMG plug-in needs to have the following access to the Internet. These ports may need to be allowed on your firewall if the TMG server is not your edge device. ■ 53/TCP,UDP DNS (Domain Name System) Allow to all external addresses ■ [Port]/TCP HTTP used by [Proxy Address] Only allow Web Security IP ranges. See your provisioning documentation for this information. In the list, the proxy address is shown as [Proxy Address] and the Port is shown as [Port]. Replace these entries with the proxy details included in your provisioning documentation. The CSP server and Forefront TMG server must also be able to resolve names on the Internet. Ensure that the DNS settings are correct; these can be obtained from your Internet service provider .
Upstream Proxy Configuration	The proxy address and port details are included in your provisioning documentation.
Supported Forefront TMG Editions	Two editions of Forefront TMG are supported: ■ Forefront TMG Standard Edition 2010 ■ Forefront TMG Enterprise Edition 2010 The earliest supported Forefront TMG version is Service Pack 1 (SP1, version 7.0.8108.200). The earlier RTM version is not supported. Forefront TMG Enterprise Edition supports two types of array configuration: ■ Standalone array—a TMG computer acts as the Configuration Storage server. This version is currently supported for CSP. ■ Enterprise array—an Enterprise Management server (EMS) acts as the Configuration Storage server The Configuration Storage server is where the Forefront TMG configuration is stored.

Installing the Client Site Proxy for TMG server

When you install TMG, you must install the CSP on the same drive as the TMG. For example, if you have installed TMG on drive "C:", then you must also install the CSP on drive "C:" .

When installing the CSP for Forefront TMG Enterprise Edition, you must have the administrator permission and be able to connect to the Configuration Storage server.

You must configure all necessary TMG arrays (standalone or enterprise) before you install the CSP.

To install the TMG plug-in

1. Double-click on **csp_tmg_setup.exe**.

   You will then be presented with the initial installation screen.

   On the Welcome to the InstallShield Wizard, click **Next**.

   Read the license agreement, and if you accept it, click **Next**.

2. Select for whom the software will be installed, click **Next**.

3. Select the destination folder. You must install the CSP on the same drive as the TMG. Then click **Next**.

4. Choose the installation method that matches your CSP server deployment, then click **Next**.

   - For TMG Standard Edition or the Enterprise Edition in a standalone configuration i.e. not as an array member, select **Register the web filter in Forefront TMG Standard Edition**. If you selected **Register the web filter as an Array Add-in,** proceed with the installation.
   - For TMG Enterprise Edition as a standalone array member, select **Register the Web Filter as an Array Add-in**. In this case, each array member computer can enable/disable/modify the web filters settings.
   - For TMG Enterprise Edition as a member of an array controlled by an Enterprise Management server (EMS), select **Register the web filter as an Enterprise Add-in**. In this case, settings of the web filter are applied to each array member, and the filter cannot be disabled in an array configuration unless the web filters are disabled in the enterprise configuration.

   When installing the TMG Enterprise Edition, specify the Configuration Storage server or IP address.

   Click **Check Connection** to test the connection.

The Configuration Storage server is the first server of the array for a standalone array, and is the EMS for an enterprise array.

After you have checked the connection, click **Next**.

5 Click **Install**.

6 Click **Finish**

Process overview – configuring the CSP plugin for TMG server

The following table shows the steps that are involved in configuring the Client Site Proxy (CSP) plugin for Forefront TMG server.

The configuration process establishes a firewall rule to force client authentication.

Table 6-3 Steps to configure the CSP plugin

Step	Further information
Create a firewall rule to force client authentication – by import process (recommended) or manually	See "Creating a firewall rule to force client authentication by import for CSP for TMG server" on page 65. See "Creating a firewall rule to force client authentication manually for CSP for TMG server " on page 66.
Configure integrated network authentication	See "Configuring integrated network authentication for TMG server" on page 67.
Configure network web chaining	See "Configuring network web chaining for CSP for Forefront TMG" on page 68.
Disable web caching	See "Disabling web caching for CSP in Forefront TMG" on page 68.
Check that the web filter is installed	See "Checking that the web filter is installed for CSP in TMG server" on page 69.

Creating a firewall rule to force client authentication by import for CSP for TMG server

Establishing the rule to force client authentication can be performed with a semi-automated import process described here. Or the rule can be established manually.

See "Creating a firewall rule to force client authentication manually for CSP for TMG server " on page 66.

We recommend that you use the import process.

To establish a rule using an import process

1. Start the Forefront TMG admin GUI.
2. In the left pane, right click on **Firewall Policy** and select **Import**.
3. If you are using Enterprise edition, click **Array** and then specify the array name.
4. Right click **Firewall Policy** and select **Import**.
5. Navigate to `C:\Program Files\MessageLabs\Client Site Proxy for Forefront TMG`.
6. Do one of the following:
   - If you are using Forefront TMG Standard Edition or Enterprise Edition in a standalone array, select `WWWFirewallRule.xml`.
   - If you are using Forefront TMG Enterprise Edition in an EMS controlled array, select `WWWFireWallRuleForArray.xml`.
7. Click **Import**.
8. Ensure that the new rule is at the top of the list. Right click it and select **Move Up** until it is.

Creating a firewall rule to force client authentication manually for CSP for TMG server

We recommend that you establish the rule to force client authentication using the import process. However, if the import process fails, you can establish the rule with the manual process described here.

See "Creating a firewall rule to force client authentication by import for CSP for TMG server" on page 65.

To establish the rule manually

1. Start the Forefront TMG admin GUI.
2. In the left pane, click **Firewall Policy**.
3. In the right pane, select the **Tasks** tab and click "**Firewall Policy Tasks/Create Access rule**". A wizard is displayed.
4. Specify the policy name, e.g. "Force www Authentication". Then click **Next**.
5. In the **Rule Action** page, click **Allow**. Then click **Next**.

6. In the **Protocols** page, select **Selected protocols**.
7. Click **Add** and expand **All Protocols**.
8. Double-click **HTTP**, **HTTPS**, **FTP**, and **FTP over HTTP**.
9. Click **Close** and then click **Next**.
10. In the **Malware Inspection** page, select **Do not enable malware inspection for this rule**. Click **Next**.
11. In the **Access Rule Sources** page, click **Add**, expand **Networks**, and double-click **Internal**. Click **Close** and then **Next**.
12. In the **Access Rule Destinations** page, click **Add**. Expand **Networks** and double-click **External**. Click **Close** and then **Next**.
13. In the **User Sets** page, if **All Users** is listed, select and click **Remove**. Then click **Add** and double-click **All Authenticated Users**. Click **Close** and then **Next**.
14. Click **Finish**.
15. Right-click the new rule and select **Move Up** until the rule is at the top of the list.
16. At the top of the center pane, click **Apply**.

Configuring integrated network authentication for TMG server

The required firewall rule will ensure that all traffic is authenticated against the user domain. Selecting **Integrated** is the most common solution as this uses NTLM authentication, which is transparent to the user. In addition, other authentication methods do not provide all the information required by the Forefront TMG.

You must also select a web proxy port number. Port 8080 is a common port number for internal proxy servers.

To configure integrated network authentication

1. Start the Forefront TMG admin GUI.
2. In the left pane, click **Networking**.
3. In the center pane, select the **Networks** tab.
4. Right-click **Local Host** and select **Properties**.
5. Select the **Web Proxy** tab.

6 Check **Enable Web Proxy Clients** and **Enable HTTP** boxes, and enter the required port number (8080).

7 Click **Authentication**. Ensure that **Integrated** is the only option selected. Click **OK**.

8 Double-click **Internal**.

9 Select the **Domains** tab.

10 Click **Add** and browse for your domain. Click **OK**.

11 At the top of the center pane, click **Apply**.

Configuring network web chaining for CSP for Forefront TMG

To configure network web chaining

1 Start the Forefront TMG admin GUI.

2 In the left pane, click **Networking**.

3 In the center pane, select the **Web Chaining** tab.

4 Right-click **Default Rule**, select **Properties**.

5 Select **Action** tab.

6 Select **Redirect to a specified upstream server**.

7 Click **Settings**.

8 Enter the proxy address in **Server** and the port in both **Port** and **SSL Port**.

Proxy address and port are specified in your provisioning documentation.

9 Uncheck all other check boxes.

10 Click **OK**, and **OK** again.

11 At the top of the center pane, click **Apply**.

Disabling web caching for CSP in Forefront TMG

To disable web caching

1 Start the Forefront TMG admin GUI.

2 In the left pane, click **Web Access Policy**.

3 In the right pane, select the **Tasks** tab.

4 Click **Related Tasks/Configure Web Caching**.

5 Select the **Cache Drives** tab.

6 For each cache drive, select and click **Configure...**. Specify *0* as the **Maximum cache size**.

7 Click **Set** and click **OK**.

8 Click **Close**.

9 At the top of the center pane, click **Apply**.

10 Select **Save the changes and restart the services**. Then click **OK**.

Checking that the web filter is installed for CSP in TMG server

To check that the web filter is installed

1 Start Forefront TMG admin GUI.

2 Do one of the following:

- If you are using Forefront TMG Standard Edition, expand the local server and click **System** in the left pane.
- If you are using Forefront TMG Enterprise Edition and the CSP is registered as an **Array Add-in**, expand **Arrays** and click **System** in the left pane.
- If you are using Forefront TMG Enterprise Edition and the CSP is registered as an **Enterprise Add-in**, expand **Enterprise** and click **System** in the left pane.

3 In the center pane, select the **Web Filters** tab.

If **Client Site Proxy Filter** does not appear in the list of installed filters, do one of the following:

- If you are using Forefront TMG 2010 Standard Edition, register it manually. See the following procedure.
- If you are using Forefront TMG Enterprise Edition, check that you have the administration permission and that the Configuration Storage server is accessible.

To register the web filter manually (Forefront TMG 2010 Standard Edition only)

1. In Windows Explorer, copy the `ClientSiteProxy.dll` file from `C:\Program Files\MessageLabs\Client Site Proxy for Forefront TMG\` to `C:\Program Files\Microsoft Forefront Threat Management Gateway\`.
2. At a command prompt, type **`regsvr32 C:\Program Files\Microsoft Forefront Threat Management Gateway\ClientSiteProxy.dl`** and click **Enter**.

   After a few moments a confirmation message is displayed.

Upgrading the Client Site Proxy for TMG server

Upgrades can be grouped into two kinds:

A patch or point upgrade	This is a minor release. This is the type of upgrade that is released to resolve outstanding issues and would not typically have additional features.
A version upgrade	This is a major release. This type of release has enhanced functionally and more features. Each release includes instructions on how to install the release.

The procedure below is a guide to approaching an upgrade.

Warning: Upgrading the CSP will cause the service to be unavailable while the upgrade is in progress.

To upgrade the Client Site Proxy for TMG server

1. Click **Start** > **Control Panel**, select **Add or Remove Programs**.
2. Select **Client Site Proxy for Forefront TMG** and click **Remove**.

   Note: If you use an early CSP plug-in, you may need to remove the plug-in manually:

   - Open a **cmd** window, type **`regsvr32 /u C:\Program Files\Microsoft Forefront Threat Management Gateway \ ClientSiteProxy.dll`** and press **Enter**.
     After a few moments a confirmation dialog should appear indicating success.

3 Run the upgrade installer.

The next steps check that the web filter is installed.

4 Start the TMG administration console.

- If you use Forefront TMG Standard Edition, in the left pane, expand **Configuration**, select **Add-ins**.
- If you use Forefront TMG Enterprise Edition and CSP is registered as an Array Add-in, expand **Configuration** under **Arrays**, select **Add-ins**.
- If you use Forefront TMG Enterprise Edition and CSP is registered as an Enterprise Add-in, select **Enterprise Add-ins** under **Enterprise**.

5 Click on the **Web Filters** tab. **Client Site Proxy Filter** should appear in the list of installed filters. If it does not appear after a few moments, register the filter manually (if you use the Standard Edition).

6 Open a **cmd** window, type `regsvr32 C:\Program Files\Microsoft Forefront TMG\ClientSiteProxy.dll` and press **Enter**.

After a few moments a confirmation dialog should appear indicating success

7 Test the functionality of the CSP.

See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.

Removing the Client Site Proxy for TMG server automatically

This procedure describes how to automatically remove the CSP.

Note: The Client Site Proxy must be removed from a Forefront TMG computer before the TMG instance is removed from an array and before TMG is uninstalled from the computer.

To remove the CSP automatically

1 Use **Control Panel** > **Add/Remove Programs** and remove the CSP.

2 Manually remove the Firewall rules that are added.

3 Manually remove the **Integrated Network Authentication** setting.

See “Removing the Client Site Proxy for TMG Standard Edition manually” on page 72.

Removing the Client Site Proxy for TMG Standard Edition manually

This procedure describes how to remove the Client Site Proxy manually.

The Client Site Proxy must be removed from a Forefront TMG computer before the TMG instance is removed from an array and before TMG is uninstalled from the computer.

To manually remove CSP in Forefront TMG Standard edition

1. At the **cmd** prompt, type `regsvr32 /u C:\Program Files\Microsoft Forefront Threat Management Gateway\ClientSiteProxy.dll` and press **Enter**.
2. A confirmation dialog will appear indicating success.

   The CSP plug-in will now not work.
3. Delete the file **C:\Program Files\Microsoft ISA Server\ClientSiteProxy.dll**.
4. Manually remove the Firewall rule added.
5. Manually remove the **Integrated Network Authentication** settings.

See “Removing the Client Site Proxy for TMG server automatically” on page 71.

Troubleshooting - checking the CSP (TMG server)

The three main issues that may occur with the Client Site Proxy for Forefront TMG server are:

- The CSP plug-in does not have any custom logs within Forefront TMG.
  The best way to check that the CSP works correctly is with two policy rules in the portal.
  See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.
- To see the standard TMG server logs:
  1. Start the TMG server administration console.
  2. In the left pane, select **Monitoring**
  3. In the right pane, select **Start Query** or **Edit Query** as necessary
  You can now see queries to the server firewall
- The server cannot contact upstream proxy
  The cause may be network issues or firewall rules on the local ISA server or (if the ISA server is not the edge device) on the edge firewall.
  Example client error (displayed in web browser):

```
Network Access Message: The page cannot be displayed

Explanation: The request timed out before the page could be retrieved.

Try the following:
Refresh page: Search for the page again by clicking the Refresh button.
The timeout may have occurred due to Internet congestion.
Check spelling: Check that you typed the web page address correctly.
The address may have been mistyped.
Contact website: You may want to contact the website administrator to
make sure the web page still exists. You can do this by using the e-mail
address or phone number listed on the website home page.
If you are still not able to view the requested page, try contacting
your administrator or Helpdesk.

Technical Information (for support personnel)
Error Code 10060: Connection timeout
Background: The gateway could not receive a timely response from the
website you are trying to access. This might indicate that the network
is congested, or that the website is experiencing technical difficulties.
Date: 3/10/2006 1:34:34 a.m.
Server: fw.Company.local
Source: Firewall
```

See “Troubleshooting - testing the Client Site Proxy with web Security policy rules” on page 29.

Section 3

Set up the web proxy in users' browsers

Chapter 7

Introduction

This chapter includes the following topics:

- Setting up Web Security with user/group configuration and synchronizing users/groups with the Active Directory
- Setting up Web Security without user/group configuration or only custom users/groups (no Active Directory synchronization)
- About the HTTP X-Forwarded-For header

Setting up Web Security with user/group configuration and synchronizing users/groups with the Active Directory

To set up WSS with user/group configuration

1 Receive the confirmation that the service has been enabled, from the Support team.

2 Install the Client Site Proxy.

3 Install the Group Synchronization Tool (see the *Address Synchronization Tool Administrator Guide*)

4 Set up web proxying on a test PC.

See “Configuring proxy server settings in Internet Explorer” on page 79.

See “Configuring proxy server settings in Firefox” on page 80.

5 Configure Web Security to protect your network (Web AntiSpyware and AntiVirus) in the portal.

6 Configure the firewall to permit the required access on the test PC.

See "Overview to deploying Web Security" on page 9.

7 Test web browsing on the test PC.

8 Configure the firewall to permit access on all PCs, if not already set up.

See "Overview to deploying Web Security" on page 9.

9 Set up web proxying on client PCs, and test web browsing on each.

See "Setting up web proxying" on page 79.

10 Configure the Web URL Filtering Service in the portal.

11 Test web browsing on client PCs, including successful blocking of web sites as appropriate.

12 Configure firewall - remove any test-only configuration, and remove the old port 80 access.

See "Overview to deploying Web Security" on page 9.

13 Test the web browsing, and adjust the configuration as necessary.

Setting up Web Security without user/group configuration or only custom users/groups (no Active Directory synchronization)

To set up WSS without user/group configuration

1 Receive the confirmation that the service has been enabled, from the Support team.

2 Set up web proxying on a test PC.

See "Configuring proxy server settings in Internet Explorer" on page 79.

See "Configuring proxy server settings in Firefox" on page 80.

3 Configure Web Security to protect your network (Web AntiSpyware and AntiVirus) in the portal.

4 Configure the firewall to permit the required access on the test PC.

See "Overview to deploying Web Security" on page 9.

5 Test web browsing on the test PC.

6 Configure the firewall to permit access on all PCs, if not already set up.

See “Overview to deploying Web Security” on page 9.

7 Set up web proxying on client PCs, and test web browsing on each.

See “Setting up web proxying” on page 79.

8 Configure the Web URL Filtering Service in the portal.

9 Test web browsing on client PCs, including successful blocking of web sites as appropriate.

10 Configure firewall - remove any test-only configuration, and remove the old port 80 access.

See “Overview to deploying Web Security” on page 9.

11 Test the web browsing, and adjust the configuration as necessary.

12 Configure custom users and groups (if required) in the portal and create appropriate rules for those users and groups.

About the HTTP X-Forwarded-For header

The X-Forwarded-For header is a de facto standard for identifying the originating IP address of a client connecting to a web server through one or more HTTP proxy servers or load balancers. The header comprises a list of IP addresses, with the left-most being the farthest downstream client, and each successive proxy that received the request appended in turn.

To relay internal IP information for policy enforcement, the web gateway in the client should be configured to insert the X-Forwarded-For header. If there is any network address translation between the user and the web gateway, the internal IP addresses relayed to the service are the translated address.

Most proxy servers and web gateways support X-Forwarded-For headers. Such proxy servers and gateways are Squid, Apache, NetCache, Blue Coat ProxySG and Microsoft ISA Server 2004/2006 with Winfrasoft X-Forwarded-For for ISA Server.

Chapter 8

Web Proxying

This chapter includes the following topics:

- About web proxies
- Setting up web proxying
- Configuring proxy server settings in Internet Explorer
- Configuring proxy server settings in Firefox
- Configuring proxy server settings using a logon script
- Configuring proxy server settings using Group Policy Management
- Configuring proxy server settings using PAC files

About web proxies

A web proxy is a system by which the proxy server retrieves web pages on behalf of a user and then forwards the information back to the user.

In the context of Web Security, the services act as proxies, providing protection and control. In other contexts, web proxies may also be used as a cache to speed up web browsing.

Control

The control means that, under the conditions that you specify in your rule set up in the portal, items from the web that are not a threat, and so would normally be delivered, can be blocked. You can set this up for the following: certain times or days, categories of web sites, specific users or groups, and specific file types or MIME types. The user receives a notification page in their web browser to indicate what happened and why they did not receive the requested web page

Protection

If any requested web pages (or other files requested for download on the web) are perceived as a potential threat, they can be blocked from being delivered to the user. The user receives a Web Security notification web page in their web browser to alert them about what has happened, and why they have not received the requested web page .

Setting up web proxying

To use Web Security, users' web requests need to be sent to the Web Security servers, rather than going directly to the web sites . This is achieved by setting up the web browsers to use a proxy server.

Several methods can be used to set the required proxy settings:

- Manually entered on each PC
- Set by a Windows NT4 login script;
- Automatically set up with a ‘PAC’ file
- Settings that are pushed out by Group Policies (in Active Directory)

Which of these methods you use depends on the number of PCs needing to be configured, and what existing arrangements you may have for rolling out other settings to your users.

Configuring proxy server settings in Internet Explorer

To configure proxy server settings in Internet Explorer

1. In Internet Explorer, on the **Tools** menu, click **Internet Options**.
2. On the **Connections** tab, click **LAN Settings**.
3. Check **Proxy Server**.

   Verify that **Bypass proxy server for local addresses** is checked so that your intranet can be accessed.

4 Click on **Advanced**.

Verify that **Use the same proxy server for all protocols** is unchecked.

Enter the proxy details included in your provisioning documentation for **HTTP**, **Secure** and **FTP**:

Clear any entries from the **Gopher** and **Socks** boxes.

If any nonlocal IP addresses (such as an Extranet site) need to be excluded from using Web Security, enter the addresses in the **Exceptions** box.

5 Click **OK** to save the settings.

Note: The proxy address is shown as [Proxy Address] and the Port is shown as [Port]. Replace these entries with the proxy details included in your provisioning documentation.

Configuring proxy server settings in Firefox

To configure proxy server settings in Firefox

1. In Firefox, click **Tools** > **Options** > **General** > **Connection Settings**.
2. Select **Manual Proxy Configuration**.
3. Verify that the **Use this proxy server for all protocols box** is not checked.
4. Enter the proxy details included in your provisioning documentation for **HTTP**, **Secure**, and **FTP**:
5. Verify that the boxes for **Gopher Proxy**, and **SOCKS Host**, are empty.
6. Enter the details of your network and intranet server, and any other addresses to be excluded from using the proxy settings, in the **No Proxy For** box.
7. Click **OK** twice to save the settings.

Note: The proxy address is shown as [Proxy Address] and the Port is shown as [Port]. Replace these entries with the proxy details included in your provisioning documentation.

Configuring proxy server settings using a logon script

The proxy settings for users' web browsing can be set up using a Microsoft Windows NT4 login script, as in the following example.

Note: The **ProxyOverride** setting is used for any sites, which are handled locally; for example, intranet or Extranet sites.

login.bat

```
@echo off
regedit /s %0\..\SetProxy.reg
```

SetProxy.reg

```
REGEDIT4
 [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]
 "ProxyServer"="[Proxy Address]:[Port]"
 "ProxyEnable"=dword:00000001
 "ProxyOverride"="192.168.0.*;www.yourextranet.com;<local>"
 "AutoConfigURL"=""
```

Note: Replace [Proxy Address] and [Port] with the proxy details provided in your provisioning documentation. Also insert your own local network IP range and any specific URLs in place of the highlighted examples used here.

Configuring proxy server settings using Group Policy Management

Note: In earlier versions of Microsoft Windows, Internet Explorer Maintenance (IEM) could be used to configure a subset of Internet Explorer settings in an environment using Group Policy. In Windows 8, the IEM settings have been deprecated in favor of Group Policy Preferences, Administrative Templates (.admx), and the Internet Explorer Administration Kit 10 (IEAK 10). (reference: Microsoft TechNet article https://technet.microsoft.com/en-us/library/jj890998.aspx)

The Microsoft Internet Explorer 10 procedure below is from the Microsoft Tech Net article at this location: https://technet.microsoft.com/en-us/library/jj149118.aspx.

For Microsoft Internet Explorer 10 and above, using Microsoft Windows 8 or Windows Server 2012 and above.

Note that the procedure refers specifically to Internet Explorer 10. However, if you want to configure Group Policy Preferences for Internet Explorer 11 or future releases of Internet Explorer, use of the Internet Explorer 10 Internet Settings option is required.

Internet Explorer 10 preference items let you update Internet options for Internet Explorer 10 and above. Internet Explorer preference items do no provide a selection of actions because the only possible action is **Update**.

Creating an Internet Explorer item

1. Open the Group Policy Management Console. Right-click the Group Policy object (GPO) that should contain the new preference item, and then click **Edit**.
2. In the console tree under **User Configuration**, expand the **Preferences** folder, and then expand the **Control Panel Settings** folder.
3. Right-click the **Internet Settings** node, point to **New**, and select Internet Explorer 10.
4. In the **New Internet Explorer 10 Properties** dialog box, enter the Internet options for Group Policy to configure.
5. Click the Common tab, configure any options, and then type your comments in the **Description** box.
6. Click **OK**.

   The new preference item appears in the details pane.

For Microsoft Internet Explorer 8 and previous versions, use the following procedure to manage your Group Policy Objects.

If you use the Group Policy method to roll out the web proxy settings, follow these procedures in the order in which they occur.

Note: Because each group of settings in each of the Group Policy Objects (GPOs) has to be processed, it is best practice to have as few GPOs as possible. Also, you should have them at key points in the Active Directory (AD) infrastructure (such as site or domain). Adapt the instructions in the following procedures to fit in with your own AD setup.

To create a new Group Policy Object (GPO)

1. In the Group Policy Management tool, on the **Start** menu, click **Programs > Administrative Tools > Group Policy Management**.
2. In the **Group Policy Management** window, under **Domains**, right-click the domain name, and click **Create and Link a GPO Here…**

   This will open the **New GPO** window.

To name the GPO

1. In the **New GPO** window, enter a relevant name for the GPO in the **Name** field; in this example, `Web Proxy Policy.`
2. Click **OK**.

To change the GPO status

1. Once the `Proxy Policy` GPO has been created, it appears in the left pane under the specified domain.

   Select the **Proxy Policy** GPO
2. In the right pane, click the **Details** tab
3. Click on the drop-down list to change the **GPO Status** to **User configuration settings disabled**.

   This option lets users log on more quickly, as it limits the parts of the GPO that are applied.

To edit the GPO

1. In the left pane, right-click the **Proxy Policy** GPO
2. Select **Edit**.

To configure and enable the proxy settings

1. In the **Group Policy** window, in the left pane:
   - Select **Windows Settings**
   - Select **Internet Explorer Maintenance**
   - Select **Connection**.
2. In the right pane:
   - Double-click **Proxy Settings**.
   - Check the **enable proxy settings** box to enable the proxy.
   - Uncheck the **Use the same proxy server for all protocols** box.
3. In rows **1. HTTP, 2. Secure**, and **3. FTP**:

- In the **Address of proxy** and **Port** fields, enter the details included in your provisioning documentation.
- Ensure that the **Gopher**, and **Socks** boxes are empty.
- Under **Exceptions,** ensure that **Do not use proxy server for local (intranet) addresses** is checked.
- If any other IP addresses need to bypass the proxy server for some reason (such as an Extranet site), detail them in the box.

4 Click **OK**.

To secure the proxy settings

1 When the proxy settings have been enabled, disable the option for users to change the proxy settings

In the **Group Policy** window, in the left pane:

- Select **User Configuration**
- Select **Administrative Templates**
- Select **Internet Explorer**

2 In the right pane, right-click **Disable changing proxy settings**.

3 Select **Properties**.

4 Click **Enabled**.

5 Click **Apply**, then **OK**.

Any users to whom the Group Policy is applied are prevented from changing their proxy settings.

Configuring proxy server settings using PAC files

A Proxy Client Auto-Configuration (PAC) file is a file that an Internet browser uses to define its proxy settings. PAC files can be pushed out across a network using Group Policy (in Microsoft Internet Explorer), or can be set up locally using the browser settings (Internet Explorer or Firefox).

See “Creating a PAC file” on page 85.

See “Configuring Internet Explorer to use a PAC file” on page 86.

See “Configuring Firefox to use a PAC file” on page 87.

Creating a PAC file

In the following example of a PAC file, the web browser runs the PAC file and looks to see if the computer is on a local network address. If it is, the specified proxy server is used on the specified port. If the computer is not on the local area network, the PAC file tells the browser to connect to the Internet directly. An example is when a laptop user connects from a remote location.

The following is a sample proxy.pac file:

```
function FindProxyForURL(url, host)
{
if (isInNet(myIpAddress(), "10.10.10.0", "255.255.255.0"))
return "PROXY [Proxy Address]:[Port]";
else
return "DIRECT";
}
```

Replace [Proxy Address] and [Port] with the proxy details provided in your provisioning documentation. Also insert your own local network IP range and subnet mask in place of the highlighted examples used here.

To create a PAC file

1. Open a text file, for example in Notepad
2. Paste the text from the example file above into the Notepad file.
3. Replace the IP address and subnet mask indicated below to those for your network:
4. Save the file in an appropriate location as *proxy.pac*.

   To ensure that the file is saved as a PAC file, in the **Save as type** field, select **All Files**.

Deploying the use of PAC / WPAD files

A PAC file is a file that your browser can use to define proxy settings. The file can be pushed out across a network using Group Policy (Internet Explorer) or set up locally.

Example:

```
function FindProxyForURL(url, host)
{
if (isInNet(myIpAddress(), "10.10.10.0", 255.255.255.0"))return "PROXY 10.10.10.1:8080";
else
return "DIRECT";
}
```

Note: Replace 10.10.10.0, 255.255.255.0 with your internal IP address range and 10.10.10.1 with the IP of your proxy server

The browser runs the PAC file. The PAC file then looks to see if the computer is on a 10.10.10.0 address. If it is, it tells Internet Explorer to use a proxy server. If the computer is not on a 10.10.10.0 address, the PAC file tells Internet Explorer to connect to the Internet directly.

To use a WPAD file, first build a .pac configuration file and rename it to wpad.dat in lowercase. This file must then be placed in the root directory of the Web server on your network. The .pac file sets the proxy server settings given to the browser.

Your Internet browser must be set to **Automatically Detect settings** in the **Connections > LAN Settings** dialog box.

When you open the Internet browser, the automatically configured setting forces the browser to locate the http://wpad/wpad.dat configuration file. So it is important that the client can resolve the name wpad to the name of the Web server .

This can be achieved in the following ways:

- Defining in the local hosts file the IP of the Web server that wpad should resolve to.
- Using DHCP (Dynamic Host Configuration Protocol)
  Configure a new option type called wpad for code 252 and a string value of `http://xxx.yyy.zzz.qqq/wpad.dat` (where `xxx.yyy.zzz.qqq` is the address of a Web server hosting the `wpad.dat` file). This allows this option to be delivered to DHCP clients during the usual DHCP Discover process.
- DNS
  A host entry must exist for wpad on the DNS server, which resolves to the name of the Web server hosting the wpad.dat file.

Configuring Internet Explorer to use a PAC file

To set up Internet Explorer to look at the PAC file

1. In Internet Explorer, click **Tools** > **Internet Options** > **Connections** > **LAN Settings**.
2. Select **Use automatic configuration script**.

3 Enter the location of your PAC file (for example, **file://C:\proxy.pac**).

Change the directory according to the location of your PAC file.

4 Click **OK**.

Configuring Firefox to use a PAC file

To set up Firefox to look at the PAC file

1 In Firefox, click **Tools** > **Options** > **General** > **Connection Settings**.

2 Select **Automatic Proxy Configuration URL**.

3 Type the location of your PAC file in the related field: **C:\proxy.pac**

Change the directory according to the location of your PAC file.

4 Click **Reload** > **OK** > **OK** to save the settings.

Chapter 9

Web Proxy AutoDiscovery (WPAD)

This chapter includes the following topics:

Non-ISA environments

Traditionally, browser proxy setting can be configured using policy or manual configuration. The aim of using WPAD and of PAC files for automatic configuration is to reduce the burden of administration for business Internet connectivity by publishing these values for your browsers to discover automatically.

Using WPAD is by no means the only solution to achieve automatic browser configuration.

While some browser configuration may still be required, this is a useful solution if you use different browsers and if you are interested in minimal ongoing configuration. It is also useful for users who roam between different offices.

Using a PAC configuration file for WPAD

You first need to build a PAC configuration file and rename it to wpad.dat in lowercase. This file then needs to be placed in the root directory of the Web server on your network. The PAC file is responsible for setting the proxy server settings given to the browser.

Below is an example of the content of a PAC file. Note the port number 8080, which in this case is used to connect to an ISA Server. However, this can be another proxy solution such as SQUID.

```
function FindProxyForURL (url, host)
{
//varable strings to return
var proxy_yes = "PROXY 192.168.3.11:8080;
var proxy_no = "DIRECT";
//Web sites you wish to go to directly and not through ML
//This list would include internally hosted websites, intranets etc
if (shExpMatch(url, "*.localhost.*")) {return proxy_no; }
//For all other requests send to PROXY.
return proxy_yes;
}
```

Ensuring that MIME types are recognized

It is also important that the correct mime types are recognized by the browser accessing the Web server. In IIS this is achieved within the HTTP Header options of the Web site hosting the wpad.dat file by adding PAC and DAT as application/x-ns-proxy-autoconfig MIME types:

```
.dat   application/x-ns-proxy-autoconfig
.pac   application/x-ns-proxy-autoconfig
```

Setting browsers to automatically detect proxy settings

Your browsers must be set to **Auto-detect settings for this network** in the **Connection Settings** window. This is not the default behavior but it can be achieved by one of the following methods:

- Manually select the connection setting to automatically detect settings in Internet Explorer or Mozilla Firefox
- Configure the setting automatically using Local policy or Group Policy. (A firefox.adm file is freely available for Mozilla Firefox browsers.)

Resolving WPAD name to Web server name

When the user opens a browser, the automatically configured setting forces the browser to locate the http://wpad/wpad.dat configuration file. Therefore, it is important that the client can resolve the name `wpad` to the name of the Web server. This can be achieved in one of the following ways:

- Using the local hosts file
- DHCP
  See "Configuring DHCP options" on page 90.
- DNS
  See "Resolving Web server name using DNS" on page 90.

Once the `wpad` file is installed on the necessary server, a configured browser (using manual configuration or policy) will resolve the name `wpad` (using DHCP or DNS) to the correct published server. It will use the contents of that file for proxy configuration. The client is now configured to use `wpad` proxy configuration.

Configuring DHCP options

For DHCP configuration a new **Option Type** called `wpad` must be configured for code 252. Also, a string value of http://xxx.yyy.zzz.qqq/wpad.dat (where xxx.yyy.zzz.qqq is the address of a Web server hosting the wpad.dat file) should be included. This allows this option to be delivered to DHCP clients during the usual DHCP Discover process.

For the new Option Type, you must complete these fields: **Name**, **Data type**, **Code** and **Description**.

Resolving Web server name using DNS

To use DNS to resolve the name, a host entry must exist for `wpad`, which resolves to the name of the Web server hosting the wpad.dat file. In the **New Host** dialog, you must enter: **Name**, **Fully qualified domain name**, **IP address** and tick the **Create associated pointer (PTR) record** box.

ISA environments

An ISA 2004/06 Server can be used to reduce the administration for automatic configuration of the proxy. The following methods are available:

- Automatically publishing WPAD
  See "Automatically publishing WPAD" on page 91.
- Using the Firewall client
  See "Using the firewall client" on page 91.

If you use ISA server and the firewall client, using the firewall client is the most efficient way to achieve auto-configuration.

Where no ISA server is available or no firewall client software can be installed, use of a published PAC or DAT script file is necessary.

See “Non-ISA environments” on page 88.

Automatically publishing WPAD

In the Internal Properties dialog box of the Network Tab for the Internal Network interface, you can publish auto-discovery information to proxy clients.

To automatically publish WPAD

1. Click The Auto Discovery tab and tick the **Publish automatic discovery information for this network box.**
2. Enter a port in the **Use this port for automatic discovery requests:** box
3. Click **OK**.

Note: Always specify port 80 when a DNS server is used for automatic discovery.

For the auto-discovery to work successfully, the client computers need to be DHCP-enabled and the DHCP 252 option must be delivered as part of their address assignment. No PAC file or `wpad.dat` file is required.

See “Configuring DHCP options” on page 90.

Using the firewall client

Install the Firewall Client on the user computers and select the option to publish auto-discovery information as described here:

See “Automatically publishing WPAD” on page 91.

To set up the firewall client for use

1. On the Firewall Client tab, tick **Enable Firewall client support for this network**.
2. Enter the relevant **ISA Server name or IP address**
3. Tick **Automatically detect settings**.
4. Tick **Use automatic configuration script** and select the **Use default URL** option button.
5. Tick **Use a web proxy server** and enter its name or IP address.
6. Click **OK**.

The firewall client software can then be installed using group policy or manually and set to update the browser client settings automatically.

Interestingly, this works for both Internet Explorer and Firefox during testing. However, the Firefox settings do not update within the interface.

With ISA server you can achieve proxy auto-configuration by using the DCHP 252 option and the wpad.dat published script as before. However, where it is possible to install the firewall client software on the client computers, proxy auto-configuration is straightforward through the ISA firewall client software.

Delivery of all the proxy information comes from the ISA server itself. No DNS or DHCP `wpad` entries or published Web server PAC or DAT scripts are required.

Section 4

Set up web roaming

Remote Connect

This chapter includes the following topics:

About web roaming

Web Security protects users when they are away from the workplace, for example when they work from home or use an Internet hotspot.

The roaming facility may be set up for all users on an individual basis.

Two versions of the web roaming service are available:

Remote Connect

Provides the facility for roaming users, without the need for agent software to be installed.

This service is available to all clients. Users must use a PAC file to ensure that browsers are directed to our Roaming Proxy server when they are off-site. No dependency exists between this functionality and the way that policies are applied to users. In other words, the policies that apply to users when they are in the office also apply when they roam.

Smart Connect

Provides an enhanced service for web roaming, using agent software to monitor the connection to the Internet.

Smart Connect has an additional charge for this service.

See “Configuring settings for Web Roaming in the portal” on page 96.

Deploying Remote Connect step by step

Table 10-1 Steps to set up Remote Connect

Step	Action	Description
Step 1	Understand Remote Connect	See “About web roaming” on page 94.
Step 2	Set up web roaming in the portal	See “Configuring settings for Web Roaming in the portal” on page 96.
Step 3	Activate users for web roaming	See “About users and groups for roaming” on page 97. See “Activating users for roaming” on page 97. See “About the user name and password for web roaming” on page 97.

Table 10-1 Steps to set up Remote Connect *(continued)*

Step	Action	Description
Step 4	Configure browsers to use a roaming PAC file	See "About PAC files for roaming" on page 98. See "Configuring Firefox to use the roaming PAC file" on page 101. See "Configuring Internet Explorer to use the roaming PAC file" on page 102. See "Configuring Safari to use the roaming PAC file" on page 103. See "Example roaming PAC file" on page 98.
Step 5 (optional)	Disable PAC file	See "Disabling the PAC file in Internet Explorer" on page 103. See "Disabling the PAC file in Safari" on page 104.

Configuring settings for Web Roaming in the portal

To locate the Roaming section in the portal

- Select **Services** > **Web Security Services** > **Roaming**.

To enable the Roaming service

- In the **Settings** tab, click **Enable Roaming**.

To set the password expiry period

- In the **Settings** tab, select the **Password Expiry** period from the list, as appropriate for your security policy.

  When a user's password expires, they are sent an email with a link enabling them to reset their password.

About users and groups for roaming

The Roaming feature uses the same custom and synchronized groups that are set up for use with Web Security policies. So the same policies apply to users when they are in the office or are roaming.

To learn more about users and groups and how to manage them, see Help on Web Security.

Activating users for roaming

Only users with an email address can be set up as roaming users - their email address is used as their logon name.

To activate a user for roaming

1. Select **Services** > **Web Security Services** > **Roaming**.
2. Click the **Users** tab.

   When you first open this tab, the first page of users is shown. If the user of interest is not visible, type their name or type their email address in the **Enter Keyword box** and click **Search**.

   The users are listed showing their **Active** status (as Yes or No) and whether they have a password set.

   Users set their own password. The **Password** column shows whether they have set their password yet, to use the service. Users who are active but have no password were configured in the portal for Web Security but have not browsed the web when they roam.
3. Select the check box next to the required user and click **Activate Selected**. The **Active** status of the user changes to **Yes**. As long as their computer has been configured with an appropriate PAC file, the user can then log on to use roaming,

About the user name and password for web roaming

When Remote Connect users browse the web for the first time, Web Security prompts for their user name and password. The user name is their normal business email address.

When you set up the user in the portal, the system sends them an email prompting them to set up a web roaming password. If they subsequently forget this password, the **Forgotten password** link on the logon page enables them to reset their password.

See “About PAC files for roaming” on page 98.

About PAC files for roaming

After you set up the users in the portal, you must configure their web traffic to redirect through the Web Security network.

We recommend that you install a PAC file on the laptop, to ensure that they can browse the web with the minimum of user intervention.

See “Example roaming PAC file” on page 98.

Example roaming PAC file

This topic gives an example of a PAC file for the Web Roaming service. You can customize this example PAC file for your specific networks and users.

Note: The Support team update this example file from time to time. This example PAC file works only if you enter your configuration details as explained in the comment lines.

Example Roaming PAC file

```
function FindProxyForURL(url, host)
{
   var debug = false;
   var direct = "DIRECT";

   // Proxy addresses by region.
   var proxy1_eu = "PROXY proxy1.eu.webscanningservice.com:3128";
   var proxy1_us = "PROXY proxy1.us.webscanningservice.com:3128";
   var proxy2_us = "PROXY proxy2.us.webscanningservice.com:3128";
   var proxy1_ap = "PROXY proxy1.ap.webscanningservice.com:3128";
   var proxy1_hk = "PROXY proxy1.hk.webscanningservice.com:3128";
   var proxy1_jp = "PROXY proxy1.jp.webscanningservice.com:3128";


   // *****************************************************************
   // Proxy address for roaming users, specify the appropriate region
   // *****************************************************************
   var roaming1_eu = "PROXY roaming1.eu.webscanningservice.com:80";
   var roaming1_us = "PROXY roaming1.us.webscanningservice.com:80";
   var roaming2_us = "PROXY roaming2.us.webscanningservice.com:80";
   var roaming1_ap = "PROXY roaming1.ap.webscanningservice.com:80";
   var roaming1_hk = "PROXY roaming1.hk.webscanningservice.com:80";
   var roaming1_jp = "PROXY roaming1.jp.webscanningservice.com:80";
   var roaming = roaming1_eu;


   // *****************************************************************
   // Specify your CSP address if applicable, one line for each
   // distinct company subnet.
   // *****************************************************************
   // var proxy_csp_1 = "PROXY <CSP address>:3128";
   // var proxy_csp_2 = "PROXY <CSP address>:3128";

   // *****************************************************************
   // Failover open to Roaming
   // *****************************************************************
   // var proxy_csp_1_failing_open = proxy_csp_1 + ";" + roaming;
   // var proxy_csp_2_failing_open = proxy_csp_2 + ";" + roaming;


   // Source IP address.
   var myIp = myIpAddress();

   // If the host is this computer, connect directly
   if ((host == "localhost") ||
       (host == "localhost.localdomain") ||
       (host == "127.0.0.1"))
   {
      if (debug) alert("PAC: DIRECT: localhost: " + host);
      return direct;
   }

   // If host name is local (i.e. contains no dots), connect directly.
   if (isPlainHostName(host))
   {
      if (debug) alert("PAC: DIRECT: plain host: " + host);
      return direct;
   }


   // If host name is part of the IANA private IP address ranges, connect
   // directly.
   if (/^\d+\.\d+\.\d+\.\d+$/.test(host) &&
         (isInNet(host, "10.0.0.0", "255.0.0.0") ||
          isInNet(host, "172.16.0.0", "255.240.0.0") ||
          isInNet(host, "192.168.0.0", "255.255.0.0")))
   {
      if (debug) alert("PAC: DIRECT: IANA private network: " + host);
      return direct;
   }


   // *****************************************************************
   // Specify remote URLs that are trusted and don't require proxying
   // and should be bypassed when roaming.
   // *****************************************************************
   if (shExpMatch(host, "*.download.microsoft.com") ||
       shExpMatch(host, "*.windowsupdate.com") ||
       shExpMatch(host, "*.windowsupdate.microsoft.com") ||
       shExpMatch(host, "windowsupdate.microsoft.com") ||
       shExpMatch(host, "*.update.microsoft.com") ||
       shExpMatch(host, "update.microsoft.com"))
   {
      if (debug) alert("PAC: BYPASS: Windows Update: " + host);
      roaming = direct;
   }


   // *****************************************************************
   // Specify VPN ranges, one line for each VPN range.
   // When using a VPN, proxying is done through roaming proxy.
   // *****************************************************************
   // if (isInNet(myIp, "<VPN IP 1>", "<VPN Mask>" )) { if(debug) alert("PAC: ROAMING: VPN1: " +
   // if (isInNet(myIp, "<VPN IP 2>", "<VPN Mask>" )) { if(debug) alert("PAC: ROAMING: VPN1: " +


   // *****************************************************************
   // Specify local FQDNs which do not require proxying, one line per
   // expression. Shell expression patterns can be used.
   // *****************************************************************
   // if (shExpMatch(host, "<Local FQDN 1>")) { if(debug) alert("PAC: ROAMING: Local FQDN 1: " +
   // if (shExpMatch(host, "<Local FQDN 2>")) { if(debug) alert("PAC: ROAMING: Local FQDN 1: " +


   // *****************************************************************
   // Specify company subnet source IP address ranges which require
```

```
   // proxying, one line per expression. Specify adequate proxy region
   // or CSP address for each range.
   // ***************************************************************
   // if (isInNet(myIp, "<Subnet IP 1>", "<Subnet Mask>")) { if(debug) alert("PAC: ROAMING: Subr
   // if (isInNet(myIp, "<Subnet IP 2>", "<Subnet Mask>")) { if(debug) alert("PAC: ROAMING: Subr


   // When outside company subnet, connect to roaming proxy.
   if (debug && roaming != direct) alert("PAC: ROAMING: Default: " + host);
   return roaming;
}
```

Configuring Firefox to use the roaming PAC file

To enable the PAC file in Firefox

1. Save the roaming user PAC file to a location on your PC, for example `C:\roaming_PAC.txt`.
2. To set up Firefox to look at the PAC file:

   1. In Firefox, select **Tools > Options**.

   2. Select the **Advanced** category.

   3. Select the **Network** tab.

   4. In the **Connection** section, select **Settings**.

   5. Click **Automatic Proxy Configuration URL**.

   6. Type the address of your PAC file, for example **file://C:\roaming_PAC.txt**.

   7. Select **Reload**.

   8. Select **OK**.

   9. Select **OK**.
3. To verify that the PAC file is applied and that requests are proxied, navigate to a website that you normally block.

   For example, if you normally block web-based email sites, try to browse to http://mail.yahoo.com. You should see a message telling you that the page is blocked.

To disable the PAC file in Firefox

1. In Firefox, select **Tools > Options**.
2. Select the **Advanced** category.

3 Select the **Network** tab.

4 Click **Connection Settings**.

5 Select the **Direct Connection to the Internet** option.

6 Select **OK**.

7 Select **OK**.

Configuring Internet Explorer to use the roaming PAC file

The following procedures describe how to:

- Enable the roaming PAC file within Internet Explorer.
- Set up Internet Explorer to use the PAC file over dial-up and VPN connections
- Disable the PAC file if required.

To enable the PAC file in Internet Explorer

1 Save the roaming user PAC file to a location on your PC, for example `C:\roaming_PAC.txt`.

2 To set up Internet Explorer to use the PAC file for all LAN connections:

1. In Internet Explorer, select **Tools** > **Internet Options**.

2. Select the **Connections** tab.

3. Click **LAN Settings**.

4. Check the box to enable **Use automatic configuration script**.

5. Enter the **Address** of your PAC file, for example `file://C:\roaming_PAC.txt`.

6. Select **OK**.

To set up Internet Explorer to use the PAC file for dial-up and VPN connections

If you use a dial-up or VPN connection, you must also configure the laptop to use the PAC file for those connections.

To set up Internet Explorer to use the PAC file over dial-up and VPN

1 In Internet Explorer, select **Tools** > **Internet Options**.

2 Select the **Connections** tab.

3 Select the **Dial-up and Virtual Private Network settings** from the list and click **Settings** on the right of the list.

4 Check the box to enable **Use automatic configuration script**.

5 Enter the **Address** of your PAC file, for example `file://C:\roaming_PAC.txt`.

6 Select **OK**.

7 Select **OK**.

Disabling the PAC file in Internet Explorer

This procedure describes how to stop Internet Explorer using the PAC file.

To disable the PAC file in Internet Explorer

1 In Internet Explorer, select **Tools** > **Internet Options**.

2 Select the **Connections** tab.

3 Click **LAN Settings**.

4 Deselect the checkboxes to disable **Use automatic configuration script** and **Use a proxy server for your LAN**.

5 Select **OK**.

Configuring Safari to use the roaming PAC file

To set up Safari to use the PAC file:

1 Save the roaming user PAC file to a location on your PC, for example on the desktop as `roaming_PAC.txt`.

2 In Safari, click the **Safari** menu and click **Preferences**.

3 Click **Advanced**.

4 Click **Proxies: Change Settings**.

5 Click **Configure Proxies drop-down menu > Using a PAC File**.

6 In the **PAC file URL** box enter the address of your PAC file, for example:

file://localhost/Users/username/Desktop/roaming_PAC.txt

7 Click **OK**.

8 Click **Apply**.

Disabling the PAC file in Safari

To disable the PAC file in Safari

1. In Safari, on the **Safari** menu, click **Preferences**.
2. Select the **Advanced** category.
3. Click **Proxies: Change Settings**.
4. In the drop-down menu, click **Manually** and ensure that all options are unchecked.
5. Click **OK**.
6. Click **Apply**.

Web roaming FAQs and troubleshooting

Table 10-2 Web roaming FAQs and troubleshooting

Question	Answer
What are the options available to enable roaming users? Can group policy be used?	Two versions of the web roaming service are available: ▪ **Remote Connect** provides the facility for roaming users, without the need for agent software to be installed. Users need to use a PAC file to ensure that browsers are directed to our Roaming Proxy server when they are off-site. No dependency exists between this functionality and the way that policies are applied to users. The policies that apply to users when they are in the office also apply when they roam. ▪ **Smart Connect** provides an enhanced service for web roaming, using agent software to monitor the connection to the Internet.
Is the agent an extra charge?	Only the Smart Connect service uses the agent software, for which there is an additional charge. The Remote Connect service does not require agent software. No additional charges apply to use this functionality.
Once a roaming user leaves the company, do I have to explicitly disable them in the roaming service?	Users are deleted from the roaming service when they are removed from the Active Directory. However, if the user belongs to a Custom group, then they must be manually disabled in the roaming service.

Table 10-2 Web roaming FAQs and troubleshooting *(continued)*

Question	Answer
What can users do if they encounter problems with web browsing while they roam?	If users have connectivity issues when they roam, they may be able to address the problem themselves by referring to the troubleshooting and FAQs information: See "Roaming user FAQs and troubleshooting" on page 105. This information is also available online at: WSS Roaming FAQ **Note:** Ensure that your users are aware of this URL.

Roaming user FAQs and troubleshooting

You may encounter the following issues or questions when using the Web Security Remote Connect service.

Table 10-3 Roaming user FAQs and troubleshooting

Question	Answer
I am prompted to log on to browse the web. What is my roaming user name?	Your user name is your business email address. You should have received a system email with a link to be able to set your password. If you do not have that email, click the Forgotten Password link on the logon page. The system then emails you a reset password link. To ensure that your new password meets appropriate security requirements, a password policy is enforced.
How do I reset my roaming password?	On the web roaming logon page, click the Forgotten Password link. The system then emails you a reset password link. To ensure that your new password meets appropriate security requirements, a password policy is enforced.

Table 10-3 Roaming user FAQs and troubleshooting *(continued)*

Question	Answer
Why am I not prompted for my user name and password while I roam?	You should be prompted for your user name and password the first time you try to browse the web when connected on a new network. Subsequently, the browser may cache your user name and password and submit them automatically without prompting you. If you are not prompted for your user name and password, it may be because your PAC file is not properly installed and configured. You must reload your PAC file if you modify it, or restart your web browser to reload the modified PAC file. If you can browse the web by specifying the proxy server in your web browser, there may be a problem with the PAC file. Running the following tests may help you determine the cause of the problem: ■ Navigate to http://www.google.com. You should be prompted for your roaming credentials when roaming. ■ Navigate to http://mail.yahoo.com. If web-based email sites are normally blocked, you should see a policy block page. ■ Navigate to http://www.eicar.org/download/eicar.com. If you have the Web AntiVirus scanning enabled, you should see a virus block page.
Why do I see an "Access Denied" page instead of the webpage that I wanted to visit?	When you roam and try to access the sites that your corporate policy allows, you may be directed to an "Access Denied" page from www.webscanningservice.com. This page may state that "Your IP address has not been identified as a customer of the Web Security Service and has been denied." The problem may occur because your web browser has cached results of the PAC lookup. The problem can occur when you have used the web browser on one network then moved to another network without restarting the browser. To correct this problem, restart the web browser to clear the cache and reread the PAC file.

Table 10-3 Roaming user FAQs and troubleshooting *(continued)*

Question	Answer
Why am I prompted for my roaming user name and password when I am not roaming?	When you are connected to the Internet using your corporate network, you may be prompted for your roaming credentials. The two causes are: ▪ Your web browser may have cached results of the PAC lookup. The problem can occur when you have used the browser on one network then moved to another network without restarting the browser. To correct this problem, restart the web browser to clear the cache and reread the PAC file. ▪ Your PAC file may be wrongly configured for your organization's IP address range. Provide your network administrator with your IP address and ask them to verify that the IP range in the PAC file covers your address.
Can I use my roaming connection when I use a ‘captive portal’ network which directs me to a payment page?	Some Internet service providers, such as those used in hotels and Internet hotspots, require payment for the service. These service providers use a ‘captive portal’ to redirect the user to a sign-up page to enter credit card details. Most of these captive portals are intelligent. Once they have made the appropriate charge for your browsing, your normal web proxy settings for the roaming service are used In some cases, the sign-up redirection interacts poorly with the web browser 's proxy settings and may not allow the user to see the sign-up page. We recommend that you disable the web browser 's proxy settings to allow access to the sign-up page. Once the sign-up process is complete, you should be able to turn on your proxy settings. In our tests, almost all portals were intelligent, so web roaming was accomplished seamlessly. If you experience this problem, make a note of the ISP and email the details to the Support team.
Will a network using a transparent proxy prevent me from using my roaming connection?	Some networks use a transparent proxy, also referred to as an intercepting proxy. The transparent proxy is applied to all web traffic on port 80, the default port for roaming users. All users browsing the web from that network are directed through a proxy server, regardless of the proxy settings on their computer. Transparent proxy enforcement overrides the Web Security roaming user proxy settings. It disables your roaming user settings when you browse from that network. If you experience this problem, please make a note of the ISP and email the details to the Support team.

Table 10-3 Roaming user FAQs and troubleshooting *(continued)*

Question	Answer
How do I enter the location of the PAC file in Internet Explorer?	1 In Internet Explorer, on the **Tools** menu, click **Internet Options**. 2 On the **Connections** tab, click **LAN Settings**. 3 Ensure that **Automatically detect settings** and **Proxy server** are unchecked. 4 Ensure that **Use automatic configuration script** is checked. 5 Enter the location of the PAC file. Ensure that the path is prefixed with **file://**, as in **file://c:\roaming.pac**. 6 Click **OK** twice to return to the browser. 7 Restart Internet Explorer to ensure that the PAC file has been loaded.
How do I prevent the PAC file being loaded in Internet Explorer?	1 In Internet Explorer, on the **Tools** menu, click **Internet Options**. 2 On the **Connections** tab, click **LAN Settings**. 3 Ensure that **Automatically detect settings**, **Use automatic configuration script**, and **Proxy server** are unchecked. 4 Click **OK** twice to return to the browser. 5 Restart Internet Explorer to ensure that the PAC file is not loaded.
How do I enter the location of the PAC file in Mozilla Firefox?	1 In Firefox, on the **Tools** menu, click **Options**. 2 On the **Advanced > Network** tab, click **Settings**. 3 In the **Connection Settings** window, select the **Automatic proxy configuration URL** option. 4 Enter the location of the PAC file. Ensure that the path is prefixed with **file:///**, as in **file:///c:/roaming.pac**. 5 Click **Reload** to ensure that the specified PAC file has been loaded, then click **OK** twice to return to the browser.
How do I prevent the PAC file from being loaded in Mozilla Firefox?	1 In Firefox, on the **Tools** menu, click **Options**. 2 On the **Advanced > Network** tab, click **Settings**. 3 In the **Connection Settings** window, select the **Direct connection to the Internet** option 4 Select **OK** twice to return to the browser.
Why does Internet Explorer crash when I use HTTPS?	A known issue exists with Internet Explorer 6.0 and using digest authentication to access https. Download and install the following fix: Internet Explorer 7.0

Table 10-3 Roaming user FAQs and troubleshooting *(continued)*

Question	Answer
Does Internet Explorer's automatic proxy caching affect the way roaming works?	By default, Internet Explorer caches the web proxy you selected for each host to which the user browses. In testing automatic proxy caching has not resulted in any problems. We recommend that you restart your web browser to reload the PAC file when any proxy settings have been changed.
Why do Mozilla Firefox's live bookmarks (also known as RSS feeds) fail to load while I roam?	You may not have entered your roaming user name and password. Browse to a website and enter your roaming user name and password. Firefox now loads your live bookmarks.
Are there any restrictions on the PAC file entries I can use with Mozilla Firefox?	When you edit the PAC file, be wary of the Firefox defect number 235853. In summary, this means that it is best to avoid using the functions `isResolvable()` or `dnsResolve()` which may stop DNS resolution from happening asynchronously. Firefox may appear to hang while name resolution occurs.
Does the user have to create the password before they leave the organization?	The user can create the password from their roaming location if they have access to their email. From this page they create their new password. An off-site user who retained the email with the link, would be able to use the link to set their password when required. If a user is off-site and has lost or deleted the emailed link, it is still possible for them to set their password. The user who cancels authentication while browsing through the roaming service seize an ‘authentication required’ page. From this page, the user can choose to set their password and is emailed a password reset link.
Why do some software updates not work when I use the Roaming Service?	When you use the roaming service, you may encounter errors with software updates. Some 'update agents', such as for Microsoft updates, do not support authenticating proxies. The standard PAC template we provide gives direct access to Microsoft update sites. Customers can add their own bypasses to trusted sites. You should ensure that the rules are not too generous, allowing too much traffic to bypass the Web Security proxy.