ERICOM
BE CONNECTED, BE SECURE

Ericom® Secure Gateway

Administrator's Manual

Version 10.0

Legal Notice

This manual is subject to the following conditions and restrictions:

This Administrator's Manual provides documentation for Ericom® Secure Gateway. Your specific product might include only a portion of the features documented in this manual.

The proprietary information belonging to Ericom® Software is supplied solely for the purpose of assisting explicitly and property authorized users of Ericom Secure Gateway.

No part of its contents may be used for any purpose, disclosed to any person or firm, or reproduced by any means, electronic and mechanical, without the prior expressed written permission of Ericom® Software.

The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

The software described in this document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of that agreement.

Information in this document is subject to change without notice. Corporate and individual names, and data used in examples herein are fictitious unless otherwise noted.

ESGAdminMan20220519JL

Table of Contents

ABOUT THIS DOCUMENT

This guide provides instructions on how to install, configure and use Ericom Secure Gateway. The Ericom Secure Gateway enables remote, secure connections from Ericom clients running at unsecured locations (i.e., Internet) to internal network resources. Ericom Secure Gateway provides authentication and authorization services, as well as data encryption. Follow the instructions in this manual and start enjoying the benefits of Ericom Secure Gateway within minutes!

This guide includes the following information:

- Overview of Ericom Secure Gateway
- Preparation and installation procedures
- Usage instructions
- Known issues and limitations

This guide assumes that the reader has knowledge of the following:

- Enabling RDP on Windows operating systems
- Firewall configuration

Important terminology used in this document:

- DMZ (demilitarized zone) – a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet.
- SSL – Secure Sockets Layer is a cryptographic protocol that provides communications security over the Internet.
- RDP – Remote Desktop Protocol. A remote display protocol developed by Microsoft. RDP is a standard component of Microsoft Windows.
- RDP Host – a Windows system that can be remotely accessed using Microsoft RDP, such as a Terminal Server (RDS Session Host) or Windows workstation with remote access enabled.
- WebSocket – a bi-directional, full-duplex communication mechanism introduced in the HTML5 specification.

For more information about this product and other Ericom products, please visit the Ericom website (www.ericom.com).

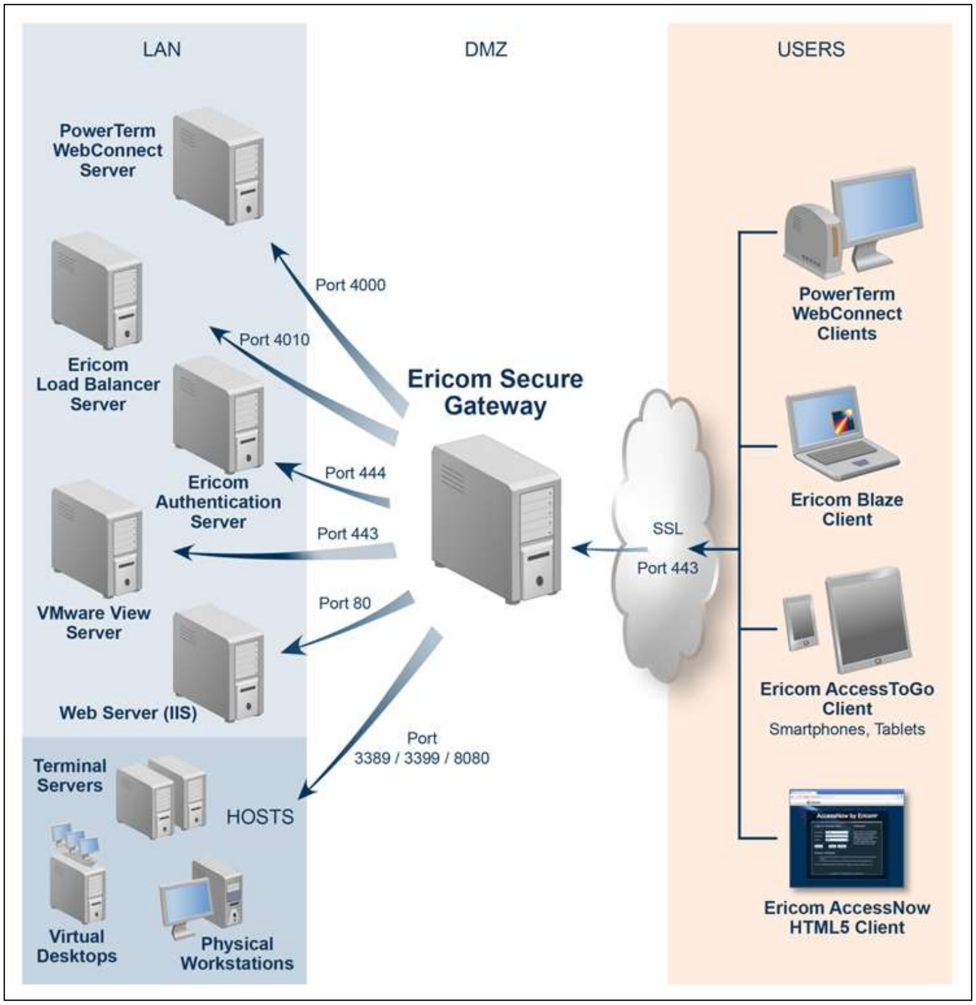
1. OVERVIEW

Ericom Secure Gateway provides end-users with secured remote access to internal network resources, such as RDP hosts (virtual desktops, Terminal Servers, etc.) The Secure Gateway provides the following benefits:

- Secure, single port access to internal resources
- Eliminates the need to purchase, install, configure and manage VPN for Ericom clients
- Install Ericom Secure Gateway in the DMZ while all other resources reside securely behind the internal firewall
- Install certificate once on Ericom Secure Gateway instead of on all hosts that need to be accessed
- TLS 1.2 compliant
- Compatible with Ericom Blaze 7.x and higher
- Compatible with Ericom PowerTerm WebConnect 6.0 and higher
- Compatible with Ericom AccessNow™ 7.x HTML5 and higher
- Compatible with Ericom AccessToGo™ 7.x and higher

Architecture

Ericom Secure Gateway acts as a gateway between end users in remote locations and applications and desktops in the datacenter. It may be installed in a DMZ to route traffic between the Internet and the LAN. The following diagram illustrates how the Secure Gateway requires just one port to be made available for secured remote access. All communication related web traffic, connection broker communication, and session protocols are tunneled through the SSL based Secure Gateway connection.



NOTE The Load Balancer functionality is not enabled. Contact Ericom Sales for information on load balancing Terminal Servers through the ESG.

2. INSTALLATION

Pre-requisites

Ericom Secure Gateway must run on Windows 2012 or higher.

- TLS 1.1 and 1.2 are supported on 2016 and 2019.

.NET Framework 4.6.2 Full Installation is required – this can be downloaded from Microsoft's website.

The Ericom Secure Gateway uses port 443 by default. This is a common port that is also used by IIS so watch out for port conflicts.

Recommended: system with at least 2 cores 4GB RAM

The following ports need to be configured on the network.

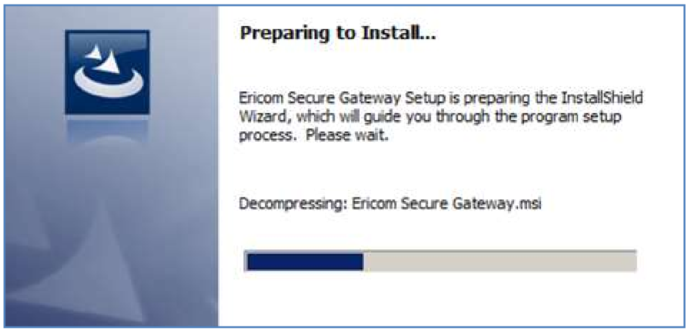
- Port 443 is required between the **Internet** and the **Secure Gateway** server; this value is adjustable.
- For **RDP** Access: Port 3389 is required between the **Secure Gateway** server and the **RDP** host; this value is adjustable.
- For **Ericom Blaze**: Port 3399 is required between the **Secure Gateway** server and the RDP host running Ericom **Blaze Server**; this value is adjustable.
- For **Ericom AccessNow**: Port 8080 is required between the **Secure Gateway** server and the **AccessNow** Server; this value is adjustable.
- For **PowerTerm WebConnect**: Port 4000 is required between the **Secure Gateway** and the **PowerTerm WebConnect** server; this value is adjustable. Depending on the protocol used (RDP, Blaze, and AccessNow), one or more of the above ports is also needed between the Secure Gateway and the RDP host.

The session communication between the end-user and the RDP host requires that *RDP access be enabled on the host*. Also ensure that the RDP port (3389) is opened on the local firewall of the RDP host.

The Secure Gateway includes an HTTP proxy and will listen on port 80 by default. This can be disabled post-installation.

Secure Gateway Install

To install the Secure Gateway, launch the installer (*Ericom Secure Gateway Server.msi)* on a x64 server running Windows 7 SP1, 8.1, 10, 2012R2, 2016, 2019, 2022. Authorization may be required to perform the installation on some systems. Click *Next* and accept the *License Agreement*, then click *Install* to perform the installation.

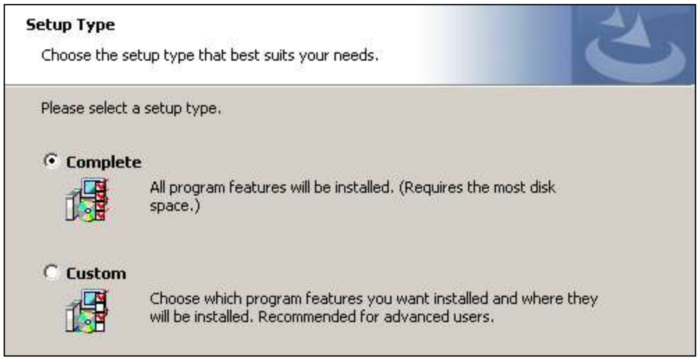


Preparing to Install...

Ericom Secure Gateway Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Decompressing: Ericom Secure Gateway.msi

When prompted for the *Setup Type* choose one of the following:



Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

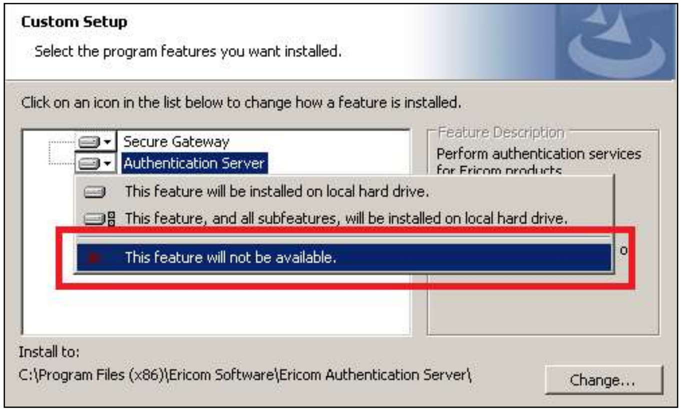
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

- Complete – Select this when using the Secure Gateway with Ericom AccessNow and/or Blaze standalone. Use this setting if PowerTerm WebConnect will be used along with any of the standalone product lines listed above.
- Custom – Select this option to install just the Ericom Secure Gateway or the Authentication Server. If *only* PowerTerm WebConnect is used, the Authentication Server does not have to be installed as the broker will be handling the authentication.



Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Secure Gateway

Authentication Server

This feature will be installed on local hard drive.

This feature, and all subfeatures, will be installed on local hard drive.

This feature will not be available.

Feature Description

Perform authentication services for Ericom products

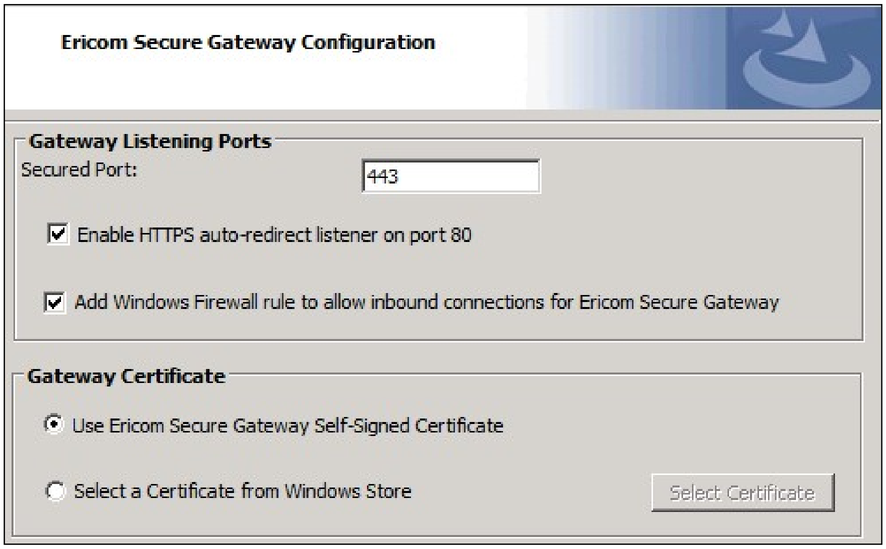
Install to:

C:\Program Files (x86)\Ericom Software\Ericom Authentication Server\

Secure Gateway Configuration

When prompted, enter the desired port that the Secure Gateway should listen on. By default, the port will be 443.

The Secure Gateway includes a built-in web server that will also operate over the specified port using HTTPS. The Secure Gateway can automatically redirect HTTP web requests to HTTPS by checking the setting *Enable HTTPS auto-redirect on port* ***80***.



Ericom Secure Gateway Configuration

Gateway Listening Ports

Secured Port: 443

☑ Enable HTTPS auto-redirect listener on port 80

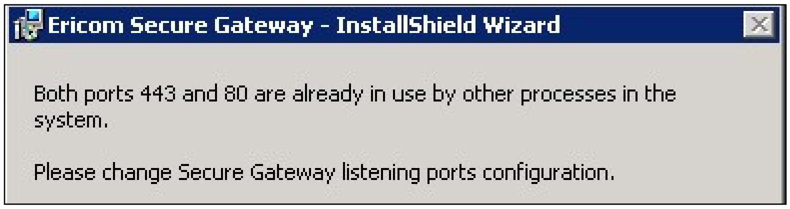
☑ Add Windows Firewall rule to allow inbound connections for Ericom Secure Gateway

Gateway Certificate

● Use Ericom Secure Gateway Self-Signed Certificate

○ Select a Certificate from Windows Store

NOTE If IIS is running on the same server, make sure there are no port conflicts. Either change the IIS ports to values other than 80 and 443, or change the Secure Gateway port to a value other than 443 and disable the HTTP auto redirect feature after the installation. If there is a port conflict on either the HTTP or HTTPS port, a warning will be displayed:



Both ports 443 and 80 are already in use by other processes in the system.

Please change Secure Gateway listening ports configuration.

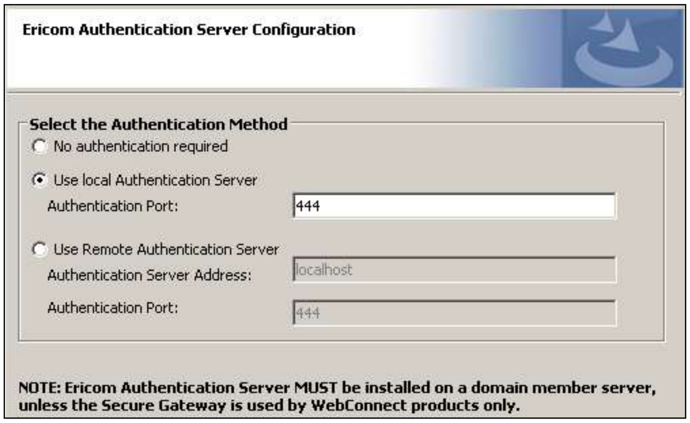
To use a trusted certificate that is already installed on the machine where the Secure Gateway is being installed on, click on *Select Certificate* and select the desired certificate to be use by the Secure Gateway. The trusted certificate may also be configured post-installation.

Authentication Server Configuration

At the next dialog, *Authentication Server Configuration*, specify the Authentication Server that will be used.

NOTE The Authentication Server requires that the server be a member of the Domain that it is authenticating from. On some networks, the Authentication Server should be installed on the LAN rather than the DMZ for best security practice.

- If this the server will act as a new Authentication Server, select *local.*
- If there is an Authentication Server already in use, select *Remote Authentication Server* and specify the address and port.
- If PowerTerm WebConnect will be used and there is no need for standalone client access, select *No authentication required*.



Ericom Authentication Server Configuration

Select the Authentication Method

○ No authentication required

● Use local Authentication Server

Authentication Port: 444

○ Use Remote Authentication Server

Authentication Server Address: localhost

Authentication Port: 444

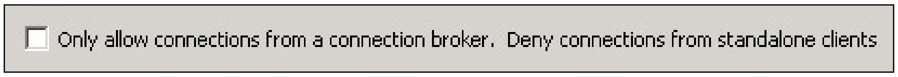
NOTE: Ericom Authentication Server MUST be installed on a domain member server, unless the Secure Gateway is used by WebConnect products only.

NOTE	The Authentication Server listens on port 444 by default, verify that this port is enabled on the network and Windows firewalls.

Connection Broker Configuration

The Connection Broker dialog allows the administrator to configure the ESG to work with a supported Connection Broker: *PowerTerm WebConnect*. Select the desired broker to configure. If no broker will be used, select *No connection broker in use*.

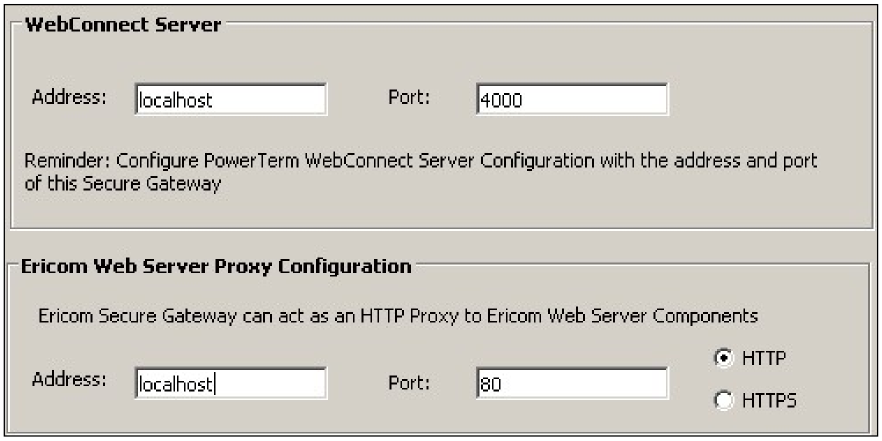
When a connection broker is in use, it is strongly recommended to enable *Only allow connections from a connection broker*. All connection attempts from standalone clients will be denied with attempting to connect using the Secure Gateway.



□ Only allow connections from a connection broker. Deny connections from standalone clients

PowerTerm WebConnect Configuration

When prompted for the PowerTerm WebConnect Server information, enter the address of the PowerTerm WebConnect and the web server that is hosting its web pages. The address must be accessible from the Ericom Secure Gateway server (use ping.exe or telnet.exe to verify connectivity).



WebConnect Server

Address: localhost Port: 4000

Reminder: Configure PowerTerm WebConnect Server Configuration with the address and port of this Secure Gateway

Ericom Web Server Proxy Configuration

Ericom Secure Gateway can act as an HTTP Proxy to Ericom Web Server Components

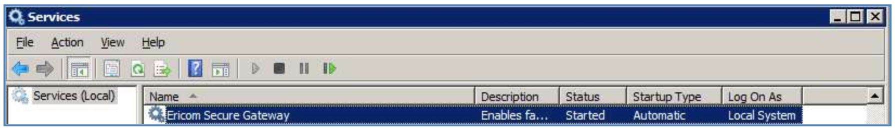
Address: localhost Port: 80

● HTTP
○ HTTPS

Completing the Installation

After entering the configuration data, click *Next* to continue the installation. At the end of the installation click *Finish*.

Ericom Secure Gateway runs as a service, and can be stopped and restarted from the Windows services manager:

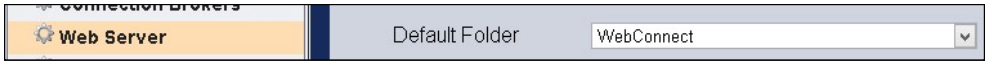


Name	Description	Status	Startup Type	Log On As
Ericom Secure Gateway	Enables fa...	Started	Automatic	Local System

The service is configured to run automatically on system startup. If the service is stopped or is unable to listen on its configured port, clients will be unable to connect to hosts through the gateway. If the service is unable to listen on its configured port, it will write an error message into the Windows application event log.

All configuration settings may be modified using the web-based Administration console or by editing the EricomSecureGateway.exe.Config file.

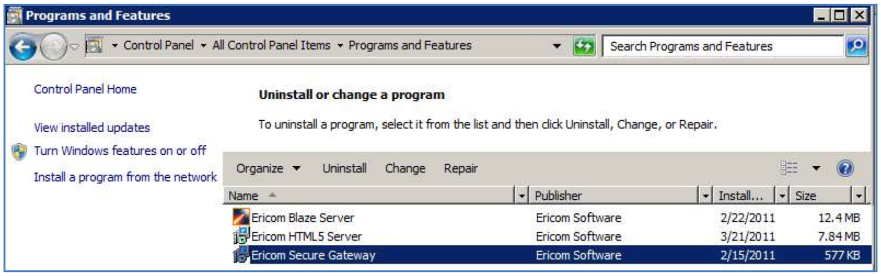
NOTE If the ESG is primarily used for PowerTerm WebConnect access, go to the web based console and set the *Default Folder* under the *Web Server* tab to the desired product.



Default Folder: WebConnect

Uninstalling Ericom Secure Gateway

Uninstall Ericom Secure Gateway by using the Control Panel | Add/Remove Programs or Programs and Features. Select *Ericom Secure Gateway* and click *Uninstall*.


Programs and Features
Control Panel ▸ All Control Panel Items ▸ Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Install a program from the network
Organize
Uninstall
Change
Repair

Uninstall or change a program

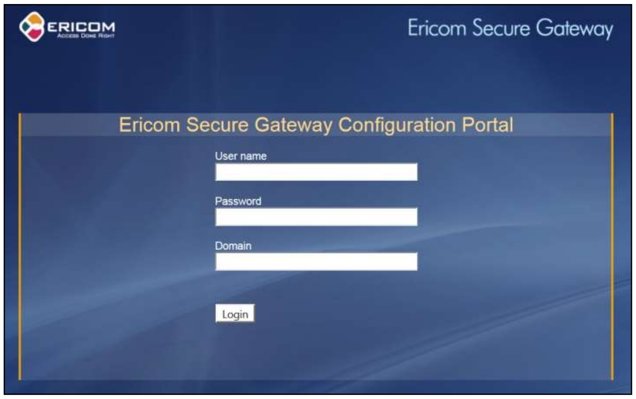
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher	Install...	Size
Ericom Blaze Server	Ericom Software	2/22/2011	12.4 MB
Ericom HTML5 Server	Ericom Software	3/21/2011	7.84 MB
Ericom Secure Gateway	Ericom Software	2/15/2011	577 KB

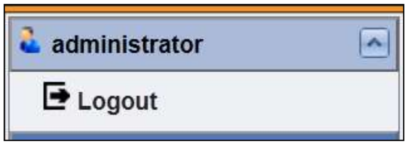
3. CONFIGURATION PORTAL

The Ericom Secure Gateway (ESG) includes a Configuration Portal to allow the administrator to adjust any related settings. Most of these settings were set during the installation process. To access the Configuration Portal page, use a web browser and navigate to the Secure Gateway's configuration URL: https://<ESG-server-address>:<port-number>/admin

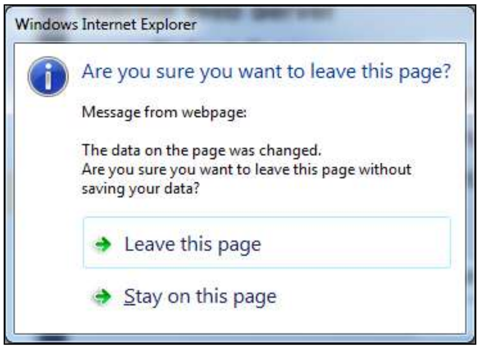
Login with any user that is a member of the local *Administrators* group on the ESG server. All logins are audited in the Ericom Secure Gateway log file. Remind administrators to use strong passwords to ensure secure access.



To log out of the Configuration Portal, press the *Logout* button.



After making changes to any settings, press the *Save* button. If the *Save* button is not pressed, and a different page is selected, a warning dialog will appear. Press *Leave this Page* to continue and cancel any changes. Click on *Stay on this page*, to return to the current page to save changes.



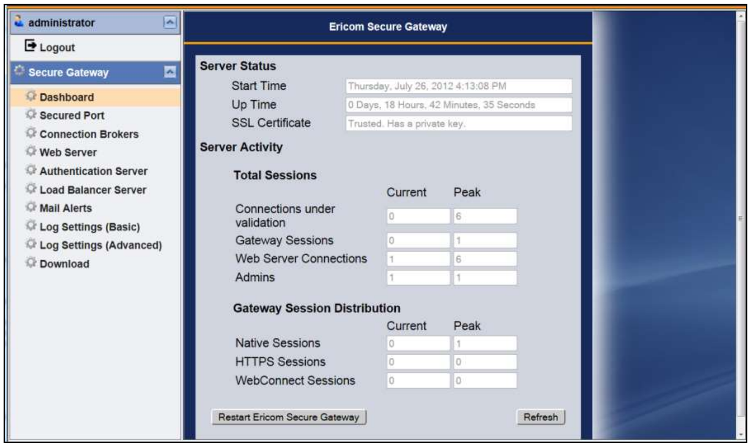
Are you sure you want to leave this page?

Message from webpage:

The data on the page was changed.
Are you sure you want to leave this page without saving your data?

Dashboard

The ESG Configuration Dashboard displays useful statistics related to the Ericom Secure Gateway operation. Open this page to view server uptime, SSL certificate status, Session activity, and to restart the Ericom Secure Gateway Server service.



Server Status

Start Time	Thursday, July 26, 2012 4:13:08 PM
Up Time	0 Days, 18 Hours, 42 Minutes, 35 Seconds
SSL Certificate	Trusted. Has a private key.

Server Activity

Total Sessions

	Current	Peak
Connections under validation	0	6
Gateway Sessions	0	1
Web Server Connections	1	6
Admins	1	1

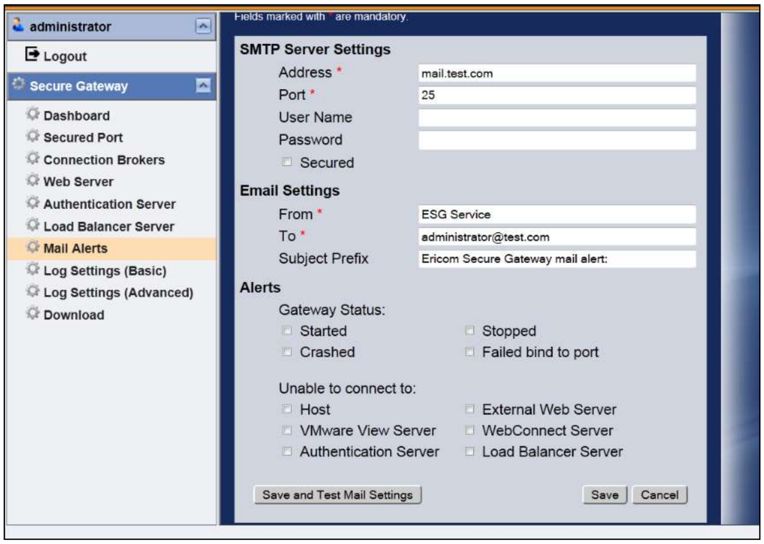
Gateway Session Distribution

	Current	Peak
Native Sessions	0	1
HTTPS Sessions	0	0
WebConnect Sessions	0	0

Mail Alerts

The Ericom Secure Gateway can be configured to send e-mail alerts upon specified system events. To configure mail alerts, enter the SMTP information of the email server. Then check the desired parameters that will trigger the sending of a mail alert.

Click *Save* or Save and Test Mail Settings to apply the configuration.



Fields marked with * are mandatory.

SMTP Server Settings

Address *	mail.test.com
Port *	25
User Name	
Password	

□ Secured

Email Settings

From *	ESG Service
To *	administrator@test.com
Subject Prefix	Ericom Secure Gateway mail alert:

Alerts

Gateway Status:

□ Started □ Stopped
□ Crashed □ Failed bind to port

Unable to connect to:

□ Host □ External Web Server
□ VMware View Server □ WebConnect Server
□ Authentication Server □ Load Balancer Server

Other configuration pages will be covered in the following chapters.

4. Port and SSL Certificate

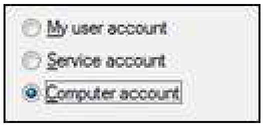
The Ericom Secure Gateway includes a self-signed certificate. Certain web browsers may display a security warning when a self-signed certificate is detected. To remove the warning, install a trusted certificate.

A trusted certificate must be purchased from a trusted certificate authority (i.e. GoDaddy). A .CER file that is returned by the authority usually does not include the private key. The .CER file needs to be converted into a PFX that includes the private key. This is usually performed on the system (e.g. IIS) where the original CSR was created. When creating the PFX, take note of the newly entered password and configure the certificate to be exportable.

The Ericom Secure Gateway uses the certificate in the Windows Certificate Store (*Computer Account)*.

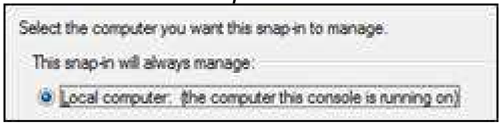
To add, view, or modify certificates perform the following:

1) Run mmc.exe
2) Go to *File* | *Add/Remove Snap-in*
3) Add Certificates and select *Computer account*



○ My user account
○ Service account
● Computer account

4) Select *Local Computer*

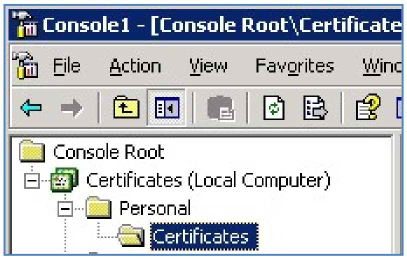


Select the computer you want this snap-in to manage:

This snap-in will always manage:

● Local computer: (the computer this console is running on)

5) Click *Finish* and then *OK*.
6) Browse to the *Certificates* | *Personal* | *Certificates* folder to view all the available certificates that can be used by the Secure Gateway.


Console1 - [Console Root\Certificate
File
Action
View
Favorites
Winc
Console Root
Certificates (Local Computer)
Personal
Certificates

7) If a trusted certificate will be used with the Secure Gateway, place it in the same location as the Secure Gateway certificate (*Personal* | *Certificates*).

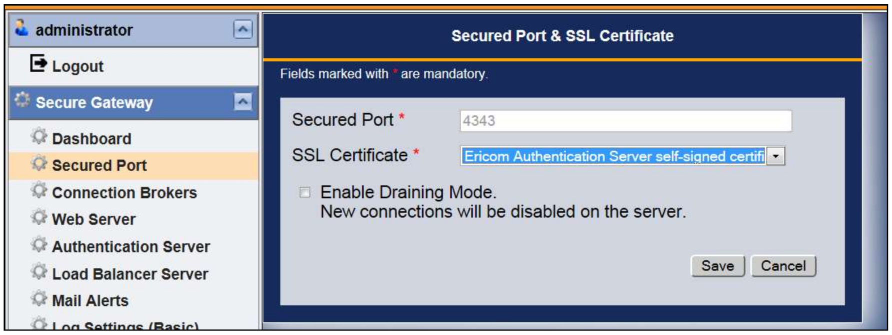
Ericom Secure Gateway identifies a certificate using a unique thumbprint that is configured in the Gateway's configuration file *EricomSecureGateway.exe.config*).

<add key="CertificateThumbprint" value="<enter trusted cert val here>" />

Configure the Secured Port and SSL Certificate

Use the Secured Port and SSL Certificate page to modify the port that will be used be the Secure Gateway. Make sure that the desired port is not currently in use by the server before configuring it. Verify port status by using the netstat utility.

Select the desired SSL certificate to be used by the ESG. It is strongly recommended to use a trusted certificate when the ESG is used in production. Verify whether the selected certificate is trusted by viewing the *Dashboard* page.



Secured Port & SSL Certificate

Fields marked with * are mandatory.

Secured Port * 4343

SSL Certificate * Ericom Authentication Server self-signed certifi

□ Enable Draining Mode.
New connections will be disabled on the server.

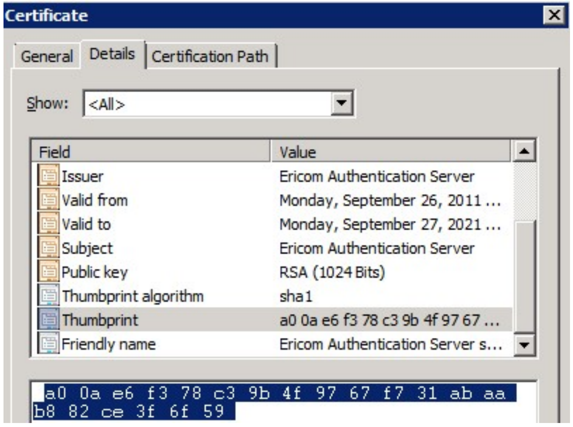
Manually Configuring a Trusted Certificate

There are two methods to manually configure the Secure Gateway to use a trusted certificate.

Method 1: Run "EricomSecureGateway.exe /import_cert" to select a certificate from Windows Store and import its thumbprint to the configuration file.

Method 2: Add the thumbprint value to the configuration file by performing the following:

1) Go to the Certificate Details tab and highlight the Thumbprint.



Show: <All>

Field	Value
Issuer	Ericom Authentication Server
Valid from	Monday, September 26, 2011 ...
Valid to	Monday, September 27, 2021 ...
Subject	Ericom Authentication Server
Public key	RSA (1024 Bits)
Thumbprint algorithm	sha1
Thumbprint	a0 0a e6 f3 78 c3 9b 4f 97 67 ...
Friendly name	Ericom Authentication Server s...

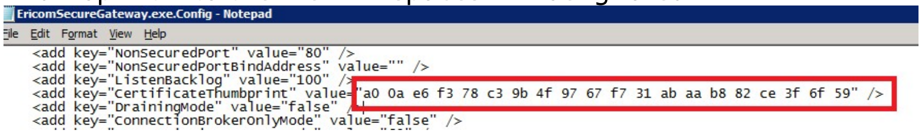
```
a0 0a e6 f3 78 c3 9b 4f 97 67 f7 31 ab aa
b8 82 ce 3f 6f 59
```

2) Press CTRL-C to copy it.

3) Click *OK* to close the dialog.

4) Open the *EricomSecureGateway.exe.Config* file

5) Delete the existing Thumbprint and press CTRL-V to copy the new Thumbprint into the file. All spaces will be ignored.



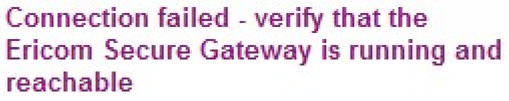
EricomSecureGateway.exe.Config - Notepad
File Edit Format View Help

```
    <add key="NonSecuredPort" value="80" />
    <add key="NonSecuredPortBindAddress" value="" />
    <add key="ListenBacklog" value="100" />
    <add key="CertificateThumbprint" value="a0 0a e6 f3 78 c3 9b 4f 97 67 f7 31 ab aa b8 82 ce 3f 6f 59" />
    <add key="DrainingMode" value="false" />
    <add key="ConnectionBrokerOnlyMode" value="false" />
```

6) Save the file and the new Thumbprint will be used. Restarting the Secure Gateway service will apply the new certificate immediately.

The Thumbprint can also be manually typed in.

NOTE The DNS address of the Secure Gateway server must match the certificate name. If it does not, this error message will appear upon connection:



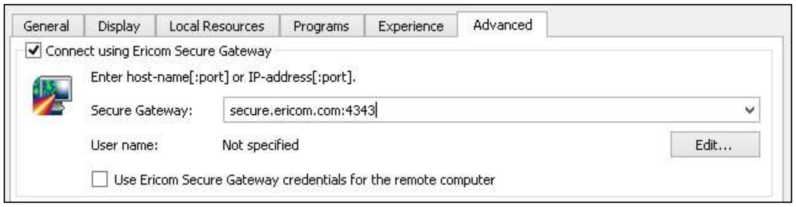
Connection failed - verify that the Ericom Secure Gateway is running and reachable

5. Blaze Client Configuration

Ericom Blaze Client supports connections to Access Servers using the Secure Gateway. To configure the Blaze Client for use with the Secure Gateway perform the following:

1) Make sure that Access Server 7.x is installed and running on the RDP host.

2) Launch Blaze Client and go to the *Advanced* tab. Check "Connect using Ericom Secure Gateway" and enter the address and port (address:port) of the Secure Gateway Sever. This address should be one that is reachable from the Blaze Client.



☑ Connect using Ericom Secure Gateway

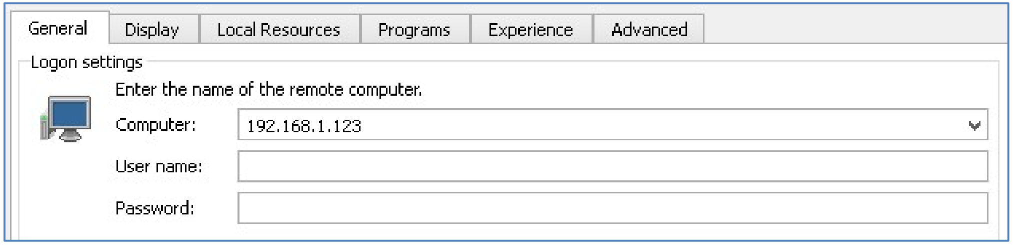
Enter host-name[:port] or IP-address[:port].

Secure Gateway: secure.ericom.com:4343

User name: Not specified

☐ Use Ericom Secure Gateway credentials for the remote computer

3) Go to the *General* tab and enter the address of the Blaze Server from the point of view of the Secure Gateway (this will usually be an internal address).



Logon settings

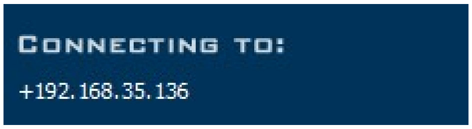
Enter the name of the remote computer.

Computer: 192.168.1.123

User name:

Password:

4) Click Connect. When Blaze client connects to the remote desktop using the Secure Gateway, a '+' will appear as a prefix to the destination address in the Blaze Connection Banner (see example below).



CONNECTING TO:

+192.168.35.136

Configuring Failover Gateways

Multiple Ericom Secure Gateways can be configured as a failover chain in the **AccessNow** web client and **Blaze** client. This will provide redundancy for the Secure Gateway function as alternate Gateways will be automatically used when the primary one is unavailable. If the connection to the first Secure Gateway in the list fails, the request will be redirected to the server listed next. There is no limit for this list.

To specify a failover list of Secure Gateways, enter each gateway address separated by a semicolon (';').

Here is a sample list of servers:

Us-bl2012r2;securegateway.ericom.com;192.168.0.3:4343

The primary gateway is Us-bl2012r2 over port 443

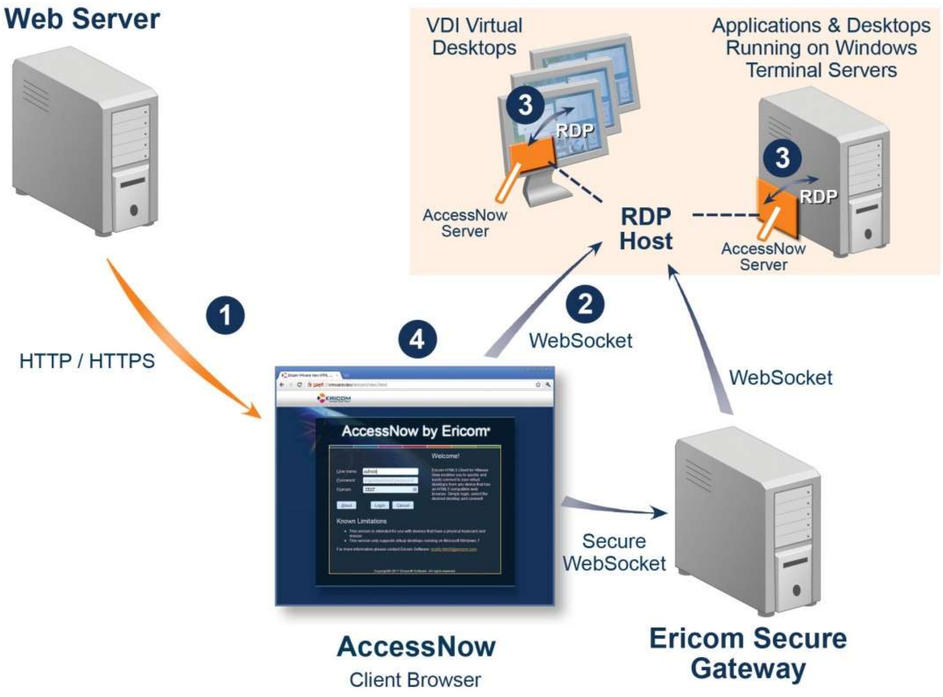
The second Secure Gateway is securegateway.ericom.com over port 443

The third Secure Gateway is 192.168.0.3 over port 4343 (any port value other than 443 needs to be explicitly specified).

NOTE Maintain uptime for the servers at the front of the list to ensure the fastest login times. If the primary server is unavailable, the end-users will experience longer login times as the login process must wait for the primary server to timeout before attempting to connect to a failover server.

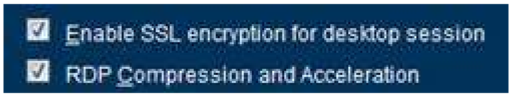
6. ERICOM ACCESSNOW™ HTML5 CLIENT CONFIGURATION

AccessNow can use the Ericom Secure Gateway to provide secured connections between AccessNow clients and AccessNow servers. This diagram describes how these components work together:



In this configuration, the AccessNow Server *always establishes a secure* WebSocket connection to the Ericom Secure Gateway. The Gateway then establishes a WebSocket connection to the AccessNow server.

The WebSocket connection between the *Gateway and the AccessNow server* can be secured or not, based on a configuration setting in the AccessNow client (check *Enable SSL* for the AccessNow web configuration).

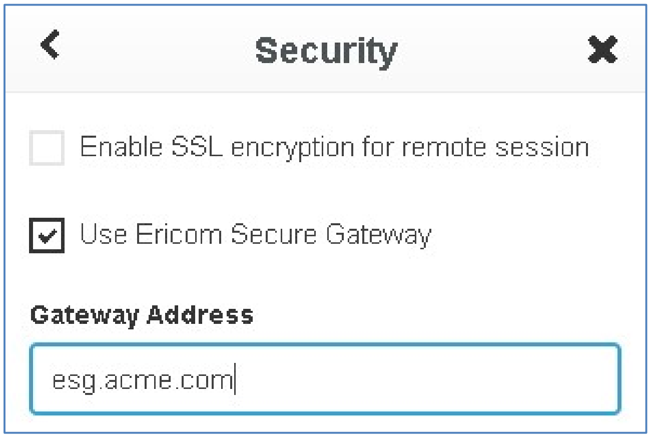


☑ Enable SSL encryption for desktop session

☑ RDP Compression and Acceleration

Configuration

To enable the use of Ericom Secure Gateway with AccessNow: click on the *Settings* button. Go to *Security* and check *Use Ericom Secure Gateway* and provide the Gateway address:



☐ Enable SSL encryption for remote session

☑ Use Ericom Secure Gateway

Gateway Address

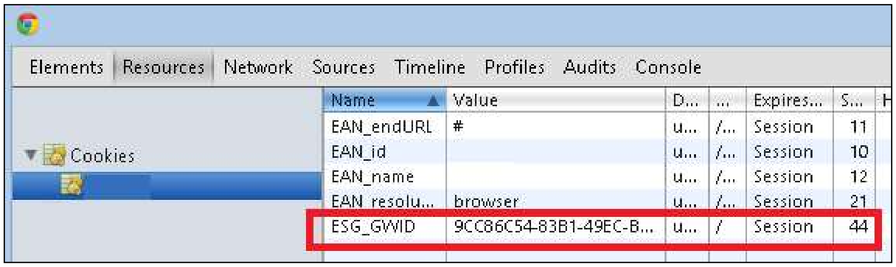
esg.acme.com

When using AccessNow Standalone with the EGS, the *AccessNow Server* address value should be that which is recognized from the ESG server (usually the internal address of the AccessNow server), not from the end user's device. The same holds for the *RDP Host* value.

It is strongly recommended to always enter a value for AccessNow Server when using the ESG. (Note that when a value is not entered, it takes the value of the address used in the URL).

ESG Session Cookie

The ESG generates a session cookie when it delivers AccessNow pages to the client browser. This session cookie is generated both for pages ESG delivers itself (when functioning as a webserver) and for pages that it tunnels through (when functioning as a proxy). The session cookie name is *ESG_GWID*, and it can be used by a page to determine that it was delivered by or through ESG.



Name	Value	D...	...	Expires...	S...	H
EAN_endURL	#	u...	/...	Session	11	
EAN_id		u...	/...	Session	10	
EAN_name		u...	/...	Session	12	
EAN_resolu...	browser	u...	/...	Session	21	
ESG_GWID	9CC86C54-83B1-49EC-B...	u...	/	Session	44	

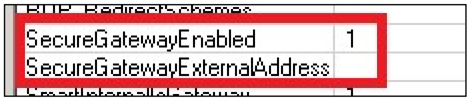
NOTE Since this is a session cookie, it persists until the browser is closed. As a result, if the same address is used both for ESG and for a different webserver, e.g. Access Server or IIS, and the user switches between the two without closing the browser, the ESG_GWID cookie will continue to exist. This can confuse the client into thinking it was delivered by ESG even if it was not.

The AccessNow client uses the presence of the ESG_GWID cookie to determine if it has been delivered using ESG, and adjusts its behavior accordingly:

- If a *Gateway address* is not specified in *config.js*, the client will display and use the URL address as the ESG address in the *Advanced* dialog, and "*Use ESG*" will be checked by default.
- If a *Gateway address* is not specified in the UI, config.js, or via the API, but the cookie exists; the client will use the URL address as the ESG address
- If a *Gateway address* is specified, and that gateway address is the same as the URL address, but the cookie does not exist, the client will perform a *direct* connection instead, *ignoring* the *Gateway address* setting.

Session Cookie and PowerTerm WebConnect with AccessNow

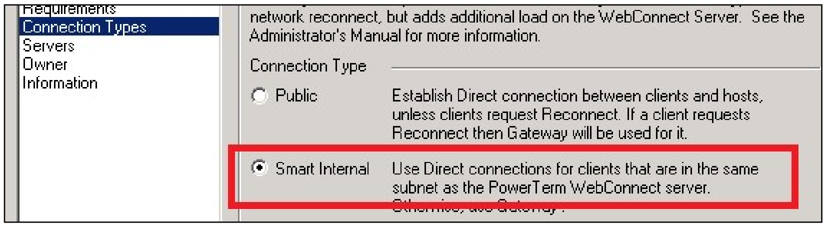
When used with **PowerTerm WebConnect** (PTWC), if the environment variable *SecureGatewayExternalAddress* is empty, but *SecureGatewayEnabled* address is 1 (enabled), the client will use the URL address as the ESG address. When *SecureGatewayExternalAddress* is defined, it has the higher precedence.



RDP_RedirectSchemes	
SecureGatewayEnabled	1
SecureGatewayExternalAddress	
SmartInternalIsGateway	1

This mechanism may be used to simulate the PTWC SmartInternal Feature for AccessNow connections (AccessNow does not currently support PowerTerm WebConnect's SmartInternal function). To enable this feature, set:

- *SecureGatewayEnabled* to *1*
- *SecureGatewayExternalAddress* to the desired ESG address, or leave empty to use the address specified in the URL by the user.
- *SmartInternalIsGateway* to *0*, or leave empty (default is 0). All AccessNow connections not passing through the ESG will operate in *Direct* mode. And all AccessNow connections passing through the ESG will use *Gateway* mode because the session cookie will be present.
- Set published connections to *SmartInternal*



network reconnect, but adds additional load on the WebConnect Server. See the Administrator's Manual for more information.

Connection Type

○ Public — Establish Direct connection between clients and hosts, unless clients request Reconnect. If a client requests Reconnect then Gateway will be used for it.

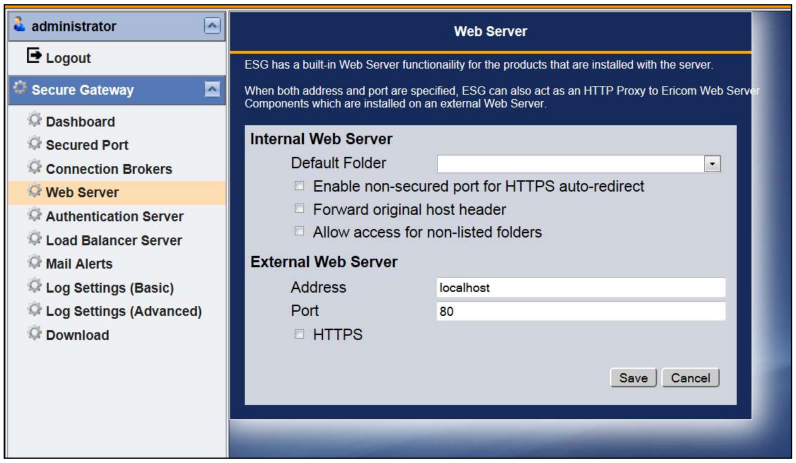
● Smart Internal — Use Direct connections for clients that are in the same subnet as the PowerTerm WebConnect server. Otherwise, use Gateway.

7. BUILT-IN WEB SERVER

Internal Web Server

The Ericom Secure Gateway has a built in Web server. The Web server supports the ability to host the web pages for certain Ericom products: Ericom AccessNow and Ericom Blaze. The built in Web server cannot be disabled and always listens on the Ericom Secure Gateway port.

To configure the Web server, open the Configuration tool and go to *Web Server*.



ESG has a built-in Web Server functionaility for the products that are installed with the server.

When both address and port are specified, ESG can also act as an HTTP Proxy to Ericom Web Server Components which are installed on an external Web Server.

Internal Web Server

Default Folder:

□ Enable non-secured port for HTTPS auto-redirect

□ Forward original host header

□ Allow access for non-listed folders

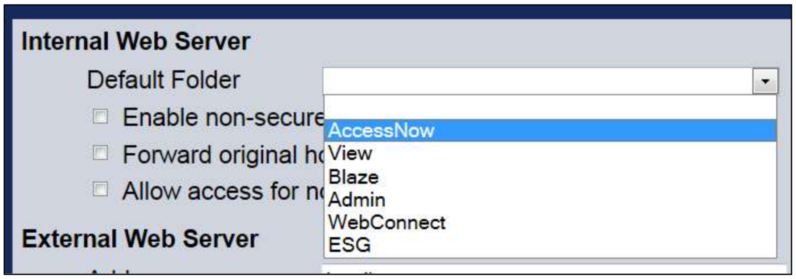
External Web Server

Address: localhost

Port: 80

□ HTTPS

Click on the drop down box to select the Ericom component that should be the default URL for the built in Web Server. Click *Save*. When the user goes to the root path of the URL, the selected component will be used.



For example, if AccessNow is selected, when the user navigates to https://<esg-server-address>:<port-number>/ the URL will automatically redirect to: https://<esg-server-address>:<port-number>/accessnow/start.html

NOTE	The ESG may be used to host non-Ericom related pages, but this is not officially supported. Hosted web pages should be of basic static content.

External Web Server

The Ericom Secure Gateway has a built in Web server proxy. The web server supports the ability to proxy the web pages of Ericom PowerTerm WebConnect. Enter the *Address* and *Port* of the PowerTerm WebConnect's Web server in order to use the ESG as proxy.

NOTE   The ESG may be used to proxy non-Ericom related pages, but this is not officially supported. The web pages that are proxied through the ESG should be of basic static content.

Connecting to the Web Server

To connect to an Ericom resource available through the Secure Gateway Web server, the end user opens a browser and navigates to the desired URL. If a port other than 443 is being used by the Secure Gateway, it must be explicitly stated in the URL. For example: https://myserver:4343/accessnow/start.html

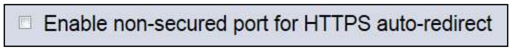
The following URL's are available by default.

Ericom Secure Gateway Welcome Page	https://server:port/ or https://server:port/welcome.html
Ericom AccessNow	https://server/accessnow/start.html
Ericom PowerTerm WebConnect (proxy mode)	https://server/webconnect/start.html
Ericom Blaze (downloads the Ericom Blaze client)	https://server/blaze/blaze.exe

HTTP Redirect

The Ericom Secure Gateway Web server listens on port 80 by default. This is so that HTTP references to the server will automatically redirect to the HTTPS URL. For example, if a user enters HTTP://server.test.local/view/view.html the Web server will accept this request and redirect the user automatically to HTTPS://server.test.local/view/view.html

This feature only works if the Secure Gateway is listening on port 443. If it is configured to use any other port, the HTTP automatic redirect will not be supported. To enable this feature, check the setting: *Enabled non-secured port for HTTPS auto-redirect*:



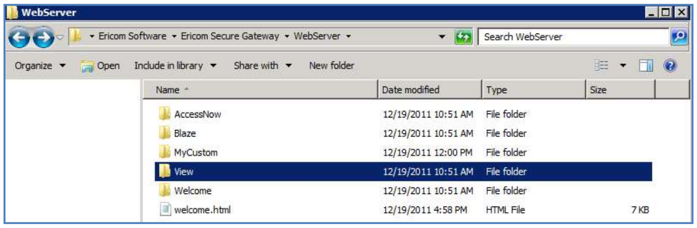
□ Enable non-secured port for HTTPS auto-redirect

Configure this feature in the *EricomSecureGateway.exe.Config* file using:
<add key="EnableNonSecuredPortForHttpsAutoRedirect" value="**false**" />

Advanced Configuration

Back up the current *EricomSecureGateway.exe.config* file before making any changes.

To configure the settings of the built-in Web server: open the *EricomSecureGateway.exe.config* using a text editor. Each folder in the *WebServer* directory may have a default document assigned for it, and may also be restricted so that end users cannot access it.



Name	Date modified	Type	Size
AccessNow	12/19/2011 10:51 AM	File folder	
Blaze	12/19/2011 10:51 AM	File folder	
MyCustom	12/19/2011 12:00 PM	File folder	
View	12/19/2011 10:51 AM	File folder	
Welcome	12/19/2011 10:51 AM	File folder	
welcome.html	12/19/2011 4:58 PM	HTML File	7 KB

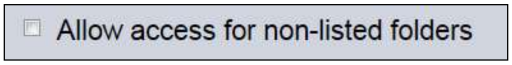
For example, the settings below will configure the following:

- Set the *View* folder as the default folder
- Set the view.html as the default document for the View folder
- Restrict access to any unlisted folders in the directory
- Deny access to the *AccessNow*, *Blaze*, and *MyCustom* folders.

```
<internalWebServerSettings>
  <Folders default_folder="View" allow_access_for_non_listed_folders="false">
    <add folder_name="AccessNow" default_page="start.html" allow_access="false"/>
    <add folder_name="View" default_page="view.html" allow_access="true"/>
    <add folder_name="Blaze" default_page="blaze.exe" allow_access="false"/>
   <add folder_name="MyCustom" default_page="hello.html" allow_access="false"/>
  </Folders>  </internalWebServerSettings>
```

Preventing Access to Non-listed Folders

Additional subfolders folders may be added to the ESG *WebServer* folder. These can be accessible, even if they are not listed in the *internalWebServerSettings* list. To prevent access to folders that are not explicitly defined in the *internalWebServerSettings* list, uncheck *Allow access for non-listed folders* (or set allow_access_for_non_listed_folders="false”).


□ Allow access for non-listed folders

8. BUILT-IN AUTHENTICATION SERVER

The Ericom Secure Gateway includes an Authentication Server. The Authentication Server provides a layer of security by authenticating end-users before they can contact any internal resource (i.e. Terminal Server, AccessNow Server, etc.) The Authentication Server is used primarily with standalone clients and not with PowerTerm WebConnect.

The Authentication Server is installed on a server that is a member of the domain that it will use to authenticate users (except when the PowerTerm WebConnect connection broker is used). The Authentication Server can only be configured for one domain at a time.

Use the Configuration page to modify settings for the Authentication Server. The configuration settings are stored in the file *EricomAuthenticationServer.exe.config*. The user configurable settings are located under the <appsettings> section and defined in the following table.

Setting	**Description**
Port	This is the numerical value of the port that the Authentication Server listens over. Make sure that no other services on the system are using the same port. A port conflict will interfere with the operation of the Authentication Server
BindAddress	The address that the Authentication Server will bind to
CertificateThumbprint	The SSL certificate thumbprint that is used by the Authentication Server. A self-sign certificate is installed and used by default.
LogStatisticsFreqSeconds	The frequency interval to log service operations

NOTE When the Authentication Server is enabled, only Domain Users will be able to authenticate. Local system users (such as Administrator) will not be able to login through the Authentication Server.

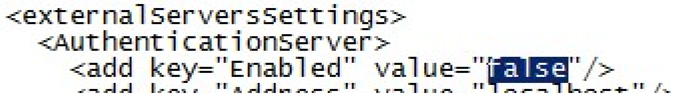
Disabling Authentication Server with Brokers

When all access is through a connection broker, and not from any standalone clients (i.e. Blaze client), the Authentication Server should be disabled.

At the Configuration page uncheck *Enabled* to disable the Authentication Server.

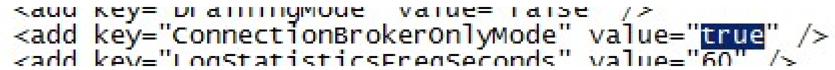
To configure the Authentication Server for connection broker-only use, apply the following changes to *EricomSecureGateway.exe.config*:

1) Set AuthenticationServer | Enabled | set to ***false***



```
<externalServersSettings>
  <AuthenticationServer>
    <add key="Enabled" value="false"/>
    <add key="Address" value="localhost"/>
```

2) Set Appsettings | ConnectionBrokerOnlyMode | set to ***true***



```
 <add key="DrainingMode" value="false" />
 <add key="ConnectionBrokerOnlyMode" value="true" />
 <add key="LogStatisticsFreqSeconds" value="60" />
```

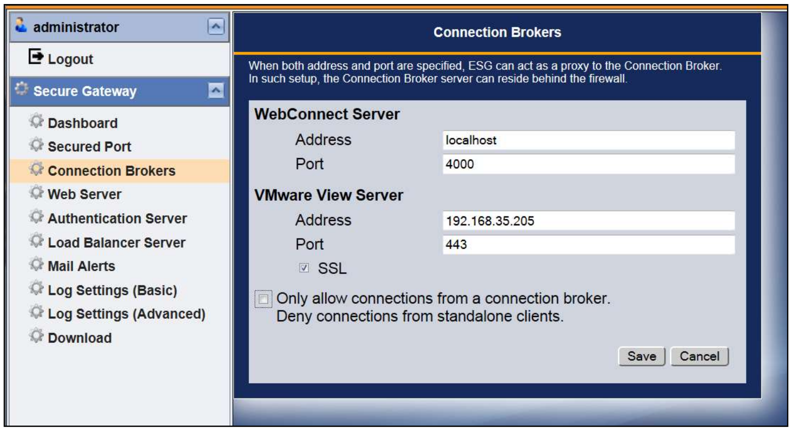
This will prevent any connections from standalone clients through the Secure Gateway and force all users to login only through a connection broker.

PowerTerm WebConnect Recommended

The built-in Authentication Server provides basic security. Any user that is a member of the domain where the Authentication Server is authenticating from will be able to login. To provide enhanced control on who is allowed to login, please use Ericom PowerTerm WebConnect.

9. Connection Brokers

Use this page to enter the address and port settings of a Powerterm WebConnect server.



Connection Brokers

When both address and port are specified, ESG can act as a proxy to the Connection Broker. In such setup, the Connection Broker server can reside behind the firewall.

WebConnect Server

Address: localhost

Port: 4000

VMware View Server

Address: 192.168.35.205

Port: 443

☑ SSL

☐ Only allow connections from a connection broker. Deny connections from standalone clients.

Select the *Deny connections from Standalone clients* setting to only allow connections through a connection broker. Connection attempts via the standalone Blaze and AccessNow clients will be denied, requiring all users to authenticate through a managed broker.

The PowerTerm WebConnect server address must be configured with an address that is reachable from the ESG server. Use the *ping* and *telnet* utility to verify connectivity between the ESG and connection broker server.

PowerTerm WebConnect 6.0 Configuration

PowerTerm WebConnect 6.0 client components support the Ericom Secure Gateway. The Secure Gateway is typically installed in the DMZ and acts as a single port relay proxy for all PowerTerm WebConnect related communication. This means that only one port needs to be opened on the external firewall. The Secure Gateway will securely tunnel all related communication through its port: PowerTerm WebConnect (4000), RDP (3389), Blaze (3399), AccessNow (8080), HTTP (80), HTTPS (443), emulation (80), SSH (22), and more.

In order to configure PowerTerm WebConnect for use with the Secure Gateway, there are two steps to complete:

1) Configure three environment variables in the PowerTerm WebConnect Administration console to enable the Secure Gateway.

2) (Optional) Configure Secure Gateway "**sg**" specific Application Zone, Application Portal and AccessToGo clients that will be used externally to point to the Secure Gateway for the PowerTerm WebConnect address. The Secure Gateway is acting as a proxy to the broker server.

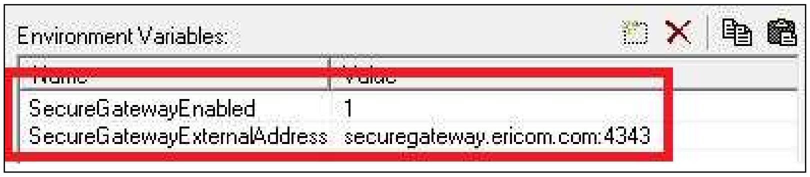
3) (Optional) If the Secure Gateway will be used for both brokered and non-brokered access (i.e. Blaze Client) then the Authentication Server will be required in order to provide security for standalone clients.

Configure the Three Broker ESG Variables

Open the *PowerTerm WebConnect Administration Tool* and go to *Server | Configuration*. Scroll down the list of Environment Variables and go to the Secure Gateway related settings:

SecureGatewayEnabled	1 – Enabled 0 – Disabled (will use an alternate service gateway built into the broker when Gateway mode is specified)
SecureGatewayExternalAddress	The address and port of the Secure Gateway server that will be reachable by the Ericom clients. This address and port must be reachable by end-users who will be connecting over the ESG.
SmartInternalIsGateway	AccessNow and AccessToGo do not support SmartInternal automatic detection. All settings that are set to SmartInternal will automatically use *Direct* by default with these clients. To force all SmartInternal connections to use Gateway, set this value to ***1***

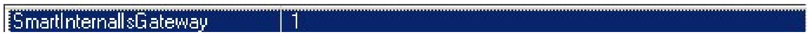
In this example, all Ericom clients will connect to the Secure Gateway at the address: securegateway.ericom.com over port 4343.


Environment Variables:

Name	Value
SecureGatewayEnabled	1
SecureGatewayExternalAddress	securegateway.ericom.com:4343

> NOTE If the Secure Gateway is using a trusted certificate, enter the DNS address of the Secure Gateway rather than the IP address here. A trusted certificate will need to recognize the domain name of the address.

If *SmartInternalIsGateway* is set to 1, all "Access" components (AccessNow, AccessPad, and AccessToGo) will use Gateway mode when the connection's Gateway setting is set to *SmartInternal*.

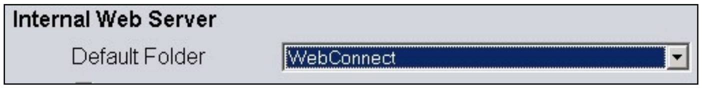


SmartInternalIsGateway	1

NOTE “Access” components currently do not support the *SmartInternal* feature (this will be available in a future release).

Configure the Client files

When WebConnect is set as the Default ESG Web Server folder, the default page will be pointed to *sgstart.html*.



Internal Web Server

Default Folder: WebConnect

This may be changed in the EricomSecureGateway.exe.config file under folder_name=”WebConnect”:

*<add folder_name="WebConnect" default_page="**sgstart.html**" allow_access="true" />*

The “sg” versions of the *Application Zone* and *Web Portal page* files on the PowerTerm WebConnect broker may need to be configured to point to the Secure Gateway for the PowerTerm WebConnect Service.

STOP When using the same address (e.g. sg.acme.com) for internal and external users make sure that the external DNS for sg.acme.com will reference the external IP/address of the Secure Gateway (such as the address of the firewall that is forwarding port 443), and that the internal DNS will reference the internal IP/address of the Secure Gateway.

Optional “/websocket” parameter

When the Secure Gateway is using port 443, certain traffic may be filtered by the firewall. To prevent connectivity issues, configure the external facing firewall to allow **all** TCP traffic over the Secure Gateway port.

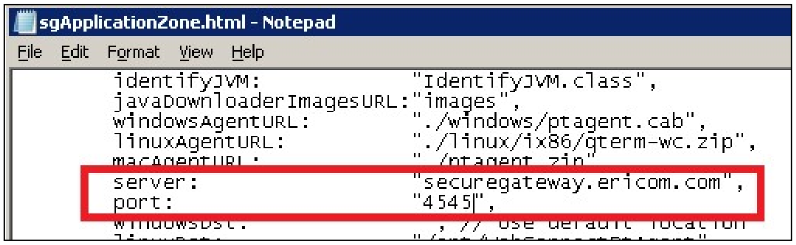
On firewalls where HTTP/HTTPS filtering cannot be disabled, configure PowerTerm WebConnect traffic to use WebSockets by adding the parameter */websocket*.

Application Zone Configuration

By default, the *sgapplicationzone.html* will use the address and port in the URL. In most cases, no customization is required in this page.

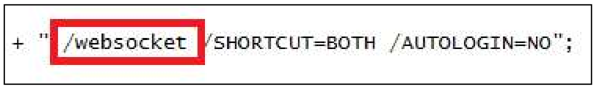
However, hardcoded values can be set for the “server:” and “port” variable.

In this example, the sgapplicationzone.html is pointed to the external Secure Gateway address on port 4545 (securegateway.ericom.com:4545) in order to access the PowerTerm WebConnect Service.



```
sgApplicationZone.html - Notepad
        identifyJVM:              "IdentifyJVM.class",
        javaDownloaderImagesURL:"images",
        windowsAgentURL:          "./windows/ptagent.cab",
        linuxAgentURL:            "./linux/ix86/qterm-wc.zip",
        macAgentURL:              "./ptagent.zip",
        server:                   "securegateway.ericom.com",
        port:                     "4545",
        windowsDst:               "", // Use default location
```

To enable WebSockets mode, add the parameter /websocket:

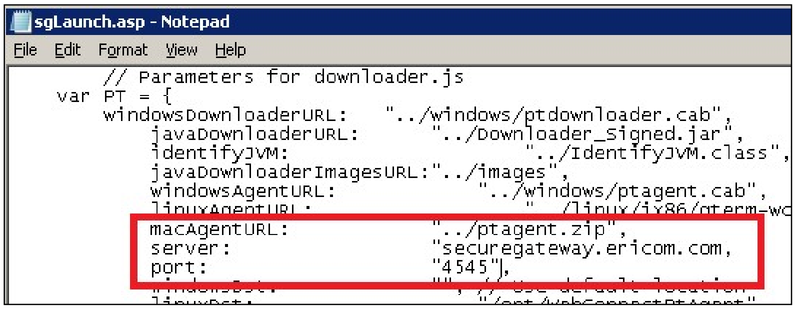


```
+ "/websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

Web Portal - sgLaunch.asp Configuration

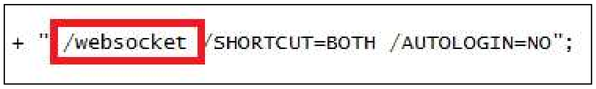
By default, the *sgLaunch.asp* will use the address and port in the URL. In most cases, no customization is required in this page.

Similar to sgapplicationzone.html, hardcoded values can be set for the “server:” and “port” variable.



```
sgLaunch.asp - Notepad
        // Parameters for downloader.js
    var PT = {
        windowsDownloaderURL:   "../windows/ptdownloader.cab",
            javaDownloaderURL:      "../Downloader_Signed.jar",
            identifyJVM:                    "../IdentifyJVM.class",
            javaDownloaderImagesURL:"../images",
            windowsAgentURL:            "../windows/ptagent.cab",
            linuxAgentURL:                  "../linux/ix86/qterm-wc
            macAgentURL:                "../ptagent.zip",
            server:                     "securegateway.ericom.com,
            port:                       "4545"],
```

To enable WebSockets mode, add the parameter /websocket:

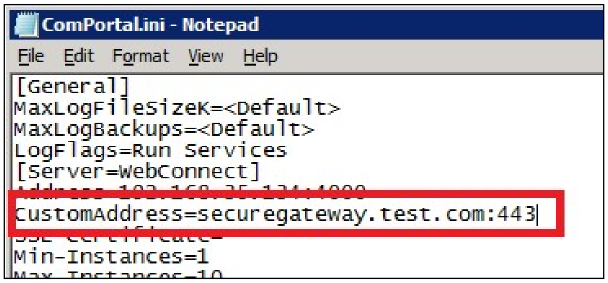


```
+ "/websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

Web Portal - Comportal.INI Configuration

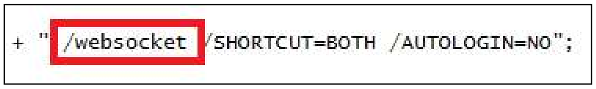
If the PowerTerm WebConnect Server and the IIS are running on separate machines, then configure *ComPortal.INI* to point to the Secure Gateway address and port. In this configuration there is no need to modify the *Launch.asp* or sgLaunch.asp file.

In the following example, the Comportal.INI is configured to point to the Secure Gateway in order to reach the PowerTerm WebConnect service.



```
[General]
MaxLogFileSizeK=<Default>
MaxLogBackups=<Default>
LogFlags=Run Services
[Server=WebConnect]
Address=192.168.35.134:4000
CustomAddress=securegateway.test.com:443
SSL-Certificate=
Min-Instances=1
Max-Instances=10
```

To enable WebSockets mode, add the parameter /websocket to the *Launch.asp* or sgLaunch.asp file:



```
+ " /websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

AccessToGo Client Configuration

Once PowerTerm WebConnect is configured for remote access with the Secure Gateway, it will support AccessToGo connections. Perform the following to connect to PowerTerm WebConnect using AccessToGo:

1) Download the AccessToGo app

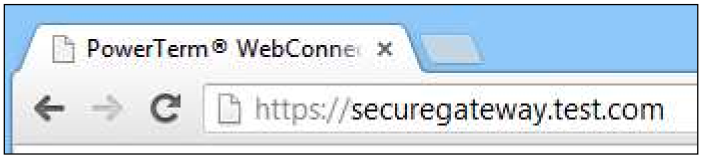
2) Create a new PowerTerm WebConnect connection

3) For the Server field, enter the server address and port (e.g. *securegateway.test.com:443*)

4) Click OK and tap on the connection to launch it.

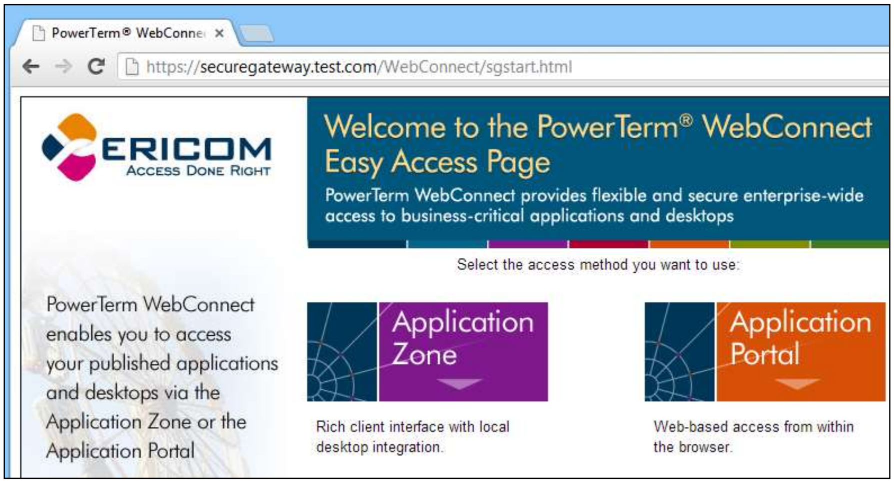
Connecting using the Secure Gateway

Once the Secure Gateway is properly configured for PowerTerm WebConnect access, direct users to the URL of the Secure Gateway. The user simply has to enter https://securegateway.test.com (or http):



https://securegateway.test.com

And the page will automatically redirect to https://securegateway.test.com/WebConnect/sgstart.html



PowerTerm® WebConne

https://securegateway.test.com/WebConnect/sgstart.html

ERICOM ACCESS DONE RIGHT

Welcome to the PowerTerm® WebConnect Easy Access Page

PowerTerm WebConnect provides flexible and secure enterprise-wide access to business-critical applications and desktops

Select the access method you want to use:

PowerTerm WebConnect enables you to access your published applications and desktops via the Application Zone or the Application Portal

Application Zone

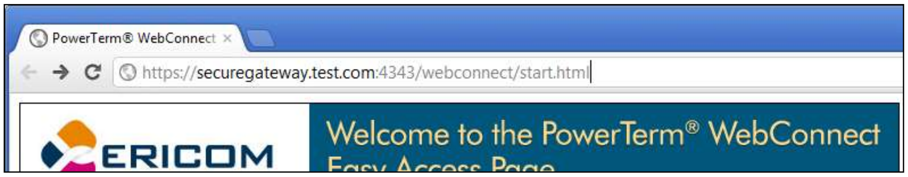
Rich client interface with local desktop integration.

Application Portal

Web-based access from within the browser.

Since the Secure Gateway is acting as a proxy to the Web server, all subfolders and filenames will be intact (i.e. /webconnect/sgstart.html).

If a port other than 443 is used as the Secure Gateway port, it must be explicitly specified in the URL (i.e. ":4343"):



PowerTerm® WebConnect

https://securegateway.test.com:4343/webconnect/start.html

ERICOM

Welcome to the PowerTerm® WebConnect Easy Access Page

NOTE All *SmartInternal* connections will automatically use *Gateway* mode when the user connects to PowerTerm WebConnect using the Secure Gateway. Direct connections will not be affected.

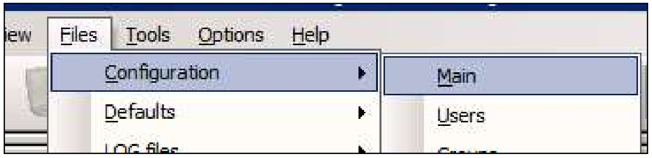
Configure the Authentication Server

The Authentication Server is not required when PowerTerm WebConnect is used by itself. To configure this, see the section on *Disabling Authentication Server with Brokers.*

However, if standalone clients will be used in the environment as well, PowerTerm WebConnect and the Secure Gateway must work with the same Authentication Server. To configure PowerTerm WebConnect to use a specific Authentication Server, perform the following:

1) Go to the PowerTerm WebConnect Administration Tool

2) Files | Configuration | *Main*



3) Go to the end of the file and search for the “Authentication Server” section. If you imported an earlier *ptserver.ini* file, the section may not be available and will have to be created

4) Set the Address to be that where the Authentication Server is running at. In the example below, the Authentication Server is running on 192.168.0.2

```
[Authentication Server]

Address=192.168.0.2

Port=444

CertificateDnsIdentity=

MaxClockSkewMinutes=180
```

5) In the Secure Gateway configuration file (EricomSecureGateway.exe.config) go to <externalServersSettings> | *AuthenticationServer* and set the value of *Address* to be the same value that is set in step 4.

```
<externalServersSettings>
   <AuthenticationServer>
      <add key="Address" value="192.168.0.2"/>
      <add key="Port" value="444"/>
```

Manual Configuration of the ESG

In addition to using the Configuration GUI, settings that were previously configured during the installation process may be changed by manually editing the EricomSecureGateway.exe.*config* file. This is a sample configuration where the Secure Gateway is configured to work with a PowerTerm WebConnect Server (PTWC) at address 192.168.35.134:

```
<WebConnectServer>

  <add key="Address" value="192.168.1.134"/>

  <add key="Port" value="4000"/>

</WebConnectServer>

<WebServer>

  <add key="Address" value="192.168.1.134"/>

 <add key="Port" value="80"/>

  <add key="SecuredConnection" value="false"/>

</WebServer>
```

10. ADVANCED CONFIGURATION

All configurable settings related to the Secure Gateway may be found in the *EricomSecureGateway.exe.config* file. This is a text file that can be opened with a text editor.

Changing parameter values marked as "Reloadable" do not require a service restart. "Not Reloadable" parameters will only take effect after the next service restart.

Whitelist Security

Whitelist functionality was added in Ericom Secure Gateway 7.6.1.

There are three types of whitelists that are configurable: End-user Address and Range, Relay Server Address and Range, and Target Host Address and Range. A Relay Server is the Ericom component that is relaying communication between the end user and the target host (e.g. Ericom AccessServer. IPv4 and IPv6 addresses are supported.

All whitelists are disabled by default. To enable a type of whitelist change the enabled setting from 'false' to 'true'.

For example:

```
<add key="ClientWhitelistByIPAddressesEnabled" value="false" />
<add key="ClientWhitelistByIPAddressesEnabled" value="true" />
```

Addresses are entered in the standard format, for example 192.168.1.1, and are separated by semicolons (;).

Address ranges are defined using a lower IP, the character '-', and the upper IP. For example: 192.168.1.1-192.168.255.255

The list of all the configuration options is:

```
<Visitor>
  <add key="HandshakeTimeoutSeconds" value="60" />
  <add key="ClientWhitelistByIPAddressesEnabled" value="false" />
  <add key="ClientWhitelistAllowedIPv4Addresses" value="" />
  <add key="ClientWhitelistAllowedIPv6Addresses" value="" />
  <add key="RelayServerWhitelistByIPAddressesEnabled" value="false" />
  <add key="RelayServerWhitelistAllowedIPv4Addresses" value="" />
  <add key="RelayServerWhitelistAllowedIPv6Addresses" value="" />
  <add key="TargetHostRestrictedToRelayServerIPEnabled" value="false" />
  <add key="TargetHostWhitelistByIPAddressesEnabled" value="false" />
```

```
      <add key="TargetHostWhitelistAllowedIPv4Addresses" value="" />
      <add key="TargetHostWhitelistAllowedIPv6Addresses" value="" />
    </Visitor>
  <Admin>
      <add key="InactivityTimeoutMinutes" value="5" />
      <add key="WhitelistByIPAddressesEnabled" value="true" />
      <add key="WhitelistAllowedIPv4Addresses" value="" />
      <add key="WhitelistAllowedIPv6Addresses" value="" />
    </Admin>
```

Note: ClientWhitelistByIPAddressesEnabled and the Admin whitelist settings existed in previous versions as 'LockdownAllowed****Addresses, if these settings are currently configured, simply copy the parameters to the new values.

Blocking HTTP/HTTPS Communication

To force Ericom Secure Gateway to exclusively use Websockets for AccessNow communication, HTTP/HTTPS may be disabled. In the configuration file, go to the 'Http' setting and set the first key from 'Enabled' to 'Disabled'.

```
<Http>
  <add key="Enabled" value="true" />
  <add key="ClientPullDataTimeoutSeconds" value="30" />
  <add key="ServerPushDataTimeoutSeconds" value="10" />
</Http>
```

Configure Session Cookie Timeout

In version 7.6.1 a client session cookie was added to protect the initial upgrade call once the Websocket is established. A token is also sent with the upgrade request (this approach is designed to protect against XSRF attacks). This cookie is identified as ESG_CSID and is valid for a configurable duration.

The cookie timeout is configured in the file as:

```
<add key="ClientSessionCookieTimeoutMinutes" value="0" />
```

If the user tries to connect (via either both Websocket or HTTPS – if enabled) and the cookie has expired, the connection will be rejected and the users must reload the page to re-attempt the login.

The cookie timeout duration is recognized by all active browsers that have opened the page on the same device. For example, if the user opens the page using Firefox and then closes it, and opens the page on Chrome, the timeout countdown will resume in Chrome from where it was left off in Firefox.

Detailed flow of the session cookie lease:

- A cookie is cached in the ESG the first time an end-user's browser requests a page
- The cookie lease duration is defined based on ClientSessionCookieTimeoutMinutes
- The lease is maintained on the ESG (server) side, not in the browsers, so all browsers are treated as a single browser from the end-user's device.
- The cookie value and lease are per client (IP address), so multiple browsers on the same user device will use the same cookie value and the same lease.
- The cookie lease duration is not extended each time a page is retrieved. It will expire only after the configured duration
- This requires the user to contact the ESG by reloading the page after each expiration.

Same-Origin Verification (AccessNow Only)

NOTE: This feature is used with AccessNow only. Do not enable this feature if other Ericom clients (e.g. Blaze client) are being used concurrently.

In version 7.6.1, two whitelist parameters were added to configure trusted origin and host addresses.

To configure the whitelists, open the configuration file and go to sessions Settings | Visitor:

- OriginHttpHeaderWhitelistAddresses
- HostHttpHeaderWhitelistAddresses

On the Websocket upgrade message, the ESG will check if 'OriginHttpHeaderWhitelistAddresses' is configured.

If the 'Origin' HTTP header exists in the message, it will verify that it is in the list of trusted addresses.

Otherwise, it checks if the 'Referer' HTTP header exist in the message, and if so it will verify that it in the list of trusted addresses.

If there is no match, ESG will deny the Websocket upgrade request.

Next, the ESG will check if 'HostHttpHeaderWhitelistAddresses' is configured.

If the 'Host' HTTP header exists in the message, it will verify that it is in the list of trusted addresses.

If there is no match, ESG will deny the WebSocket upgrade request.

If both tests are passed, ESG will accept the connection.

Configuring HTTP Security Headers

HTTP security headers are configured in the EricomSecureGateway.Config file:

To configure the value of X-Frame-Options, edit:

```
<Property name="XFrameOptions" type="string" value="" />
```

To configure the value of Content Security Policy (i.e., X-Content-Type-Options: nosniff), edit:

```
 <Property name="ContentSecurityPolicy" type="string" value="" />
```

To configure the value of the Access Control Allow origin, edit:

```
    <Property name="AccessControlAllowOrigin" type="string" value="*" />
```

High Availability

To provide high availability to the Secure Gateway layer, install two or more Secure Gateways and use a third-party redundant load balancer to manage access to them.

The load balancer will provide one address for end users to connect to. As requests arrive at the load balancer, they will be redirected to an available Secure Gateway based on built-in weighting criteria. A basic round-robin load balancer may also be used, but it may not detect whether a Secure Gateway is active.

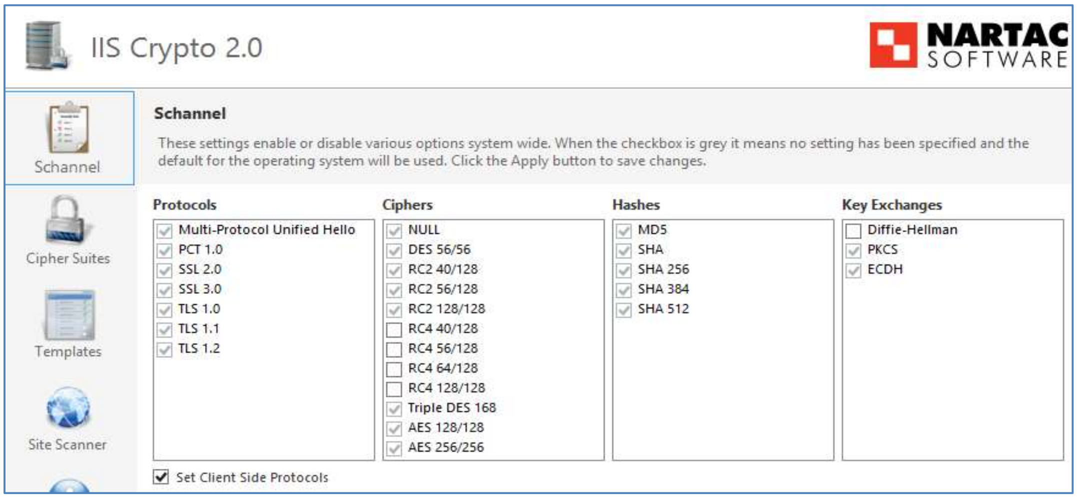
Configure for Qualys A Grade

Starting in version 7.5, the Ericom Secure Gateway (standalone) installed on a Windows 2012R2 server achieve a Qualys® (https://www.ssllabs.com/ssltest/) A grade (accurate as of August 8, 2017).

A trusted certificate and Nartac's free IIS Crypto tool (https://www.nartac.com/Products/IISCrypto) are also required.

Upon installing the ESG, configure it to use the trusted certificate over the self-signed certificate. Note that wildcard certificates may return a lower Qualys grade.

Next, use IIS Crypto and disable the RC4 ciphers and Diffie-Helman key exchange as follows:



Schannel

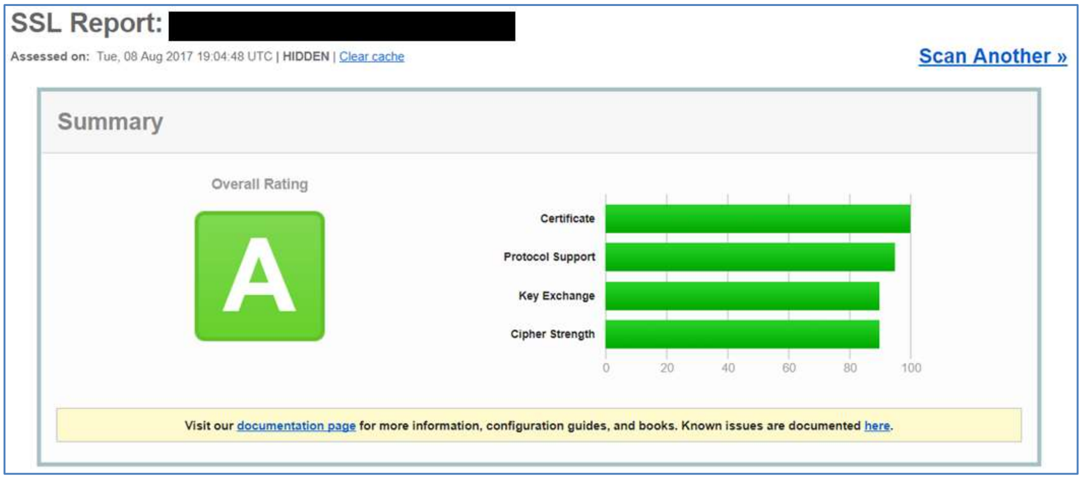
These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

Protocols	Ciphers	Hashes	Key Exchanges
☑ Multi-Protocol Unified Hello	☑ NULL	☑ MD5	□ Diffie-Hellman
☑ PCT 1.0	☑ DES 56/56	☑ SHA	☑ PKCS
☑ SSL 2.0	☑ RC2 40/128	☑ SHA 256	☑ ECDH
☑ SSL 3.0	☑ RC2 56/128	☑ SHA 384	
☑ TLS 1.0	☑ RC2 128/128	☑ SHA 512	
☑ TLS 1.1	□ RC4 40/128		
☑ TLS 1.2	□ RC4 56/128		
	□ RC4 64/128		
	□ RC4 128/128		
	☑ Triple DES 168		
	☑ AES 128/128		
	☑ AES 256/256		

☑ Set Client Side Protocols

Note that other applications that require RC4 and Diffie-Hellman support on the server will be affected. As best practice, Ericom Secure Gateway should be the primary application on the server for best performance and stability.

Reboot the server after the IIS Crypto changes and test the ESG URL in the Qualys website. An ‘A’ grade should be returned:



SSL Report: [redacted]

Assessed on: Tue, 08 Aug 2017 19:04:48 UTC | HIDDEN | Clear cache

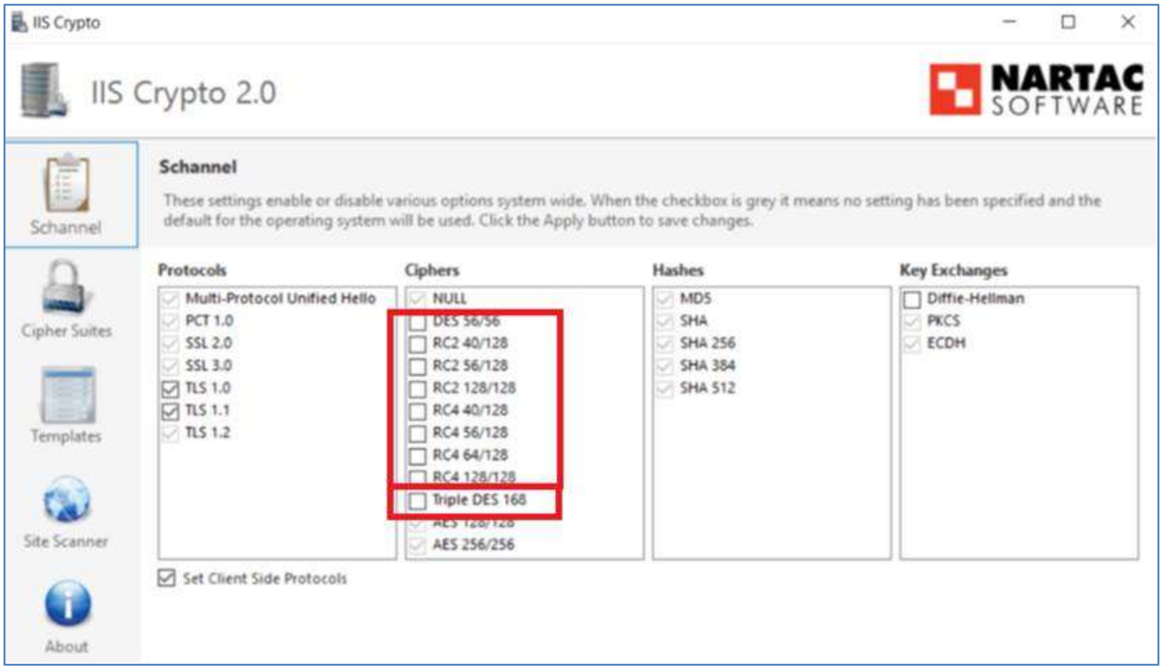
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

Protect against SWEET32

The Ericom Secure Gateway is compatible with an operating system secured to protect against SWEET32. The basic step to protecting against SWEET32 is to disable Triple DES, and this can be performed using Nartac’s IISCrypto. Please remember to back up or snapshot the system before applying the change so it can be rolled back easily.

Protect against SSL Medium Strength Cipher Suites Supported

The Ericom Secure Gateway is compatible with operating system secured to protect against "SSL Medium Strength Cipher Suites Supported". The basic step to protecting against this vulnerability is to disable all lower bit ciphers (RC2 and RC4), and this can be performed using Nartac's IISCrypto. For example, use Nartac IISCrypt to configure the following and then reboot the operating system.



Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

Protocols
- ✓ Multi-Protocol Unified Hello
- ✓ PCT 1.0
- ✓ SSL 2.0
- ✓ SSL 3.0
- ☑ TLS 1.0
- ☑ TLS 1.1
- ✓ TLS 1.2

Ciphers
- ✓ NULL
- □ DES 56/56
- □ RC2 40/128
- □ RC2 56/128
- □ RC2 128/128
- □ RC4 40/128
- □ RC4 56/128
- □ RC4 64/128
- □ RC4 128/128
- □ Triple DES 168
- ✓ AES 128/128
- ✓ AES 256/256

Hashes
- ✓ MD5
- ✓ SHA
- ✓ SHA 256
- ✓ SHA 384
- ✓ SHA 512

Key Exchanges
- □ Diffie-Hellman
- ✓ PKCS
- ✓ ECDH

☑ Set Client Side Protocols

The image above also accounts for SWEET32 by disabling Triple DES.

Please remember to back up or snapshot the system before applying the change so it can be rolled back easily.

DMZ Configuration with PTWC

By default, any user connecting through the ESG over the Internet will be identified by the PowerTerm WebConnect server as using the ESG address. This may interfere with SmartInternal operation if the DMZ IP range is configured in the SmartInternalIpRanges variable.

For example:

- ESG: 10.75.4.1

- PTWC: 10.75.1.1
- End User: 10.10.50.50

If 10.10 is added into SmartInternalIpRanges for PTWC, the user will still connect in Gateway and not Direct because PTWC recognizes the user as 10.75.4.1 (the ESG address) instead of 10.10.50.50.

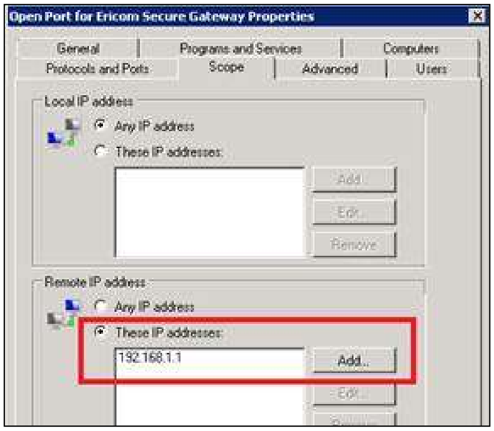
To have PTWC properly recognize the end-user’s IP address, add the parameter “/websocket” to the PARAM list for index.asp and applicationzone.html.

NOTE AccessToGo, AccessPad, and AccessNow do not fully support the SmartInternal feature yet. The Gateway behavior needs to be managed by using *SmartInternalIsGateway* variable with these clients.

Restricting Access to and from ESG

Use the Windows Firewall *Scope* rules to restrict incoming connections to the ESG and Terminal Servers.

To restrict incoming connections to the ESG, go to port rule for the Ericom Secure Gateway. Click on the *Scope* tab and enter the addresses of the systems and/or appliances that will have access to the ESG server. In the example below, only connections originating from 192.168.1.1 can connect through the ESG port.



Local IP address
● Any IP address
○ These IP addresses:

Remote IP address
○ Any IP address
● These IP addresses:
192.168.1.1

To restrict incoming connections on the Terminal Server to only the ESG, set a similar scope rule for the desired port:

- 3389: standard RDP port
- 8080: AccessNow/Blaze port

Changing the Log File Size

The default size of Log files is 32MB. When this limit is reached, a new file will be generated. To change this value, edit the *.config* file and modify the setting *LogSizeMB* setting under the logSettings section. Change the value to the desired size in MB and restart the service for the new value to go into effect. New log files are also generated each time the service is restarted.

SSO Form Post

When using a third-party authentication entity (such as an SSL VPN) that supports form Post, the user can single-sign-on into an AccessNow session using the authenticated credentials. The ESG is required for this feature.

In the authentication entity, there will be a field requesting the Post URL. Enter the SSO URL for the desired product:

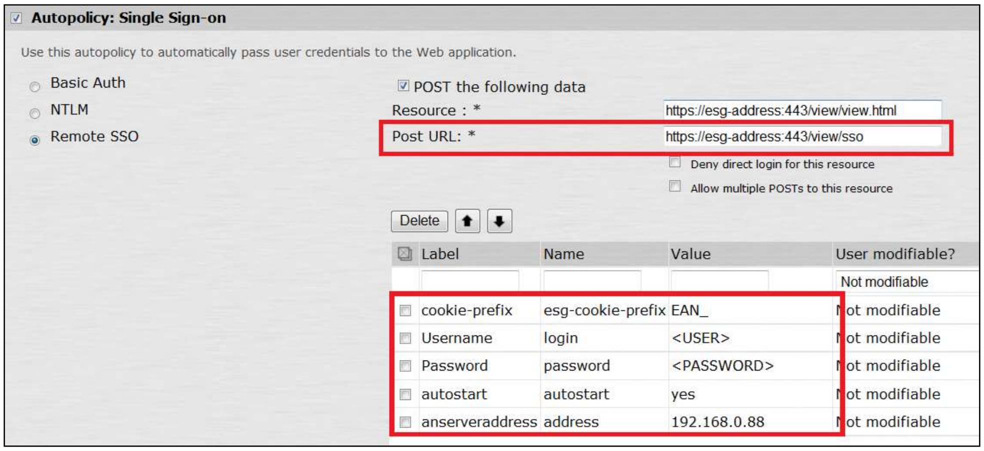
AccessNow: https://esg-address/accessnow/sso

NOTE In both cases, the ESG will auto-redirect the request to the respective default pages (start.html and view.html).

Include the following fields in the form:

- name="autostart" value="yes"
- name="esg-cookie-prefix" value="EAN_"
- name="username"
- name="password"
- name="domain"

Here is an example from a Juniper SSL VPN:



☑ **Autopolicy: Single Sign-on**

Use this autopolicy to automatically pass user credentials to the Web application.

○ Basic Auth
○ NTLM
● Remote SSO

☑ POST the following data

Resource : * https://esg-address:443/view/view.html

Post URL: * https://esg-address:443/view/sso

□ Deny direct login for this resource

□ Allow multiple POSTs to this resource

□	Label	Name	Value	User modifiable?
				Not modifiable
□	cookie-prefix	esg-cookie-prefix	EAN_	Not modifiable
□	Username	login	<USER>	Not modifiable
□	Password	password	<PASSWORD>	Not modifiable
□	autostart	autostart	yes	Not modifiable
□	anserveraddress	address	192.168.0.88	Not modifiable

The value "esg-cookie-prefix" defines the AccessNow cookie prefix in the form. For AccessNow connections, this is a mandatory entry.

If the target is a relative URL, it will replace the "/sso" portion in the path

If the target is a full URL, than it will completely replace the current path.

Sample page to POST values

```
<form name="cookieform" method="post" action="/AccessNow/sso"><p>

<!-- <form name="cookieform" method="post" action="/view/sso"><p> -->

address: <input type="text" name="address"/><br/>

<!-- RDP Host: <input type="text" name="fulladdress"/><br/> -->

Username: <input type="text" name="username"/><br/>

Password: <input type="password" name="password"/><br/>

Domain: <input type="text" name="domain"/><br/>
```

```
Use Ericom Secure Gatway: <input type="checkbox" name="use_gateway"
value="true"/><br/>

Gateway Address: <input type="text" name="gateway_address"/><br/>

Start Program on connection: <input type="checkbox"
name="remoteapplicationmode" value="true"/><br/>

Program Path: <input type="text" name="alternate_shell"
size="256"/><br/>

<input type="hidden" name="autostart" value="true"/>

<input type="hidden" name="esg-cookie-prefix" value="EAN_"/>

<input type="submit"/>

</p></form>
```

Sample page to receive POST values

```
<body>

<%

Response.Write( "address: " & Request.Form("address") & "<br/>")

Response.Write( "fulladdress: " & Request.Form("fulladdress") & "<br/>")

Response.Write( "username: " & Request.Form("username") & "<br/>")

'Response.Write( "password: " & Request.Form("password") & "<br/>")

Response.Write( "domain: " & Request.Form("domain") & "<br/>")

Response.Write( "autostart: " & Request.Form("autostart") & "<br/>")

Response.Write( "esgcookieprefix: " & Request.Form("esg-cookie-prefix") &
"<br/>")

Response.Write( "Use Ericom Secure Gatway: " &
Request.Form("use_gateway") & "<br/>")

Response.Write( "Gateway Address:" & Request.Form("gateway_address") &
"<br/>")

Response.Write( "Start Program on connection: " &
Request.Form("remoteapplicationmode") & "<br/>")

Response.Write( "Program Path: " & Request.Form("alternate_shell") &
"<br/>")

%>

</body>
```

Click jacking Protection for AccessNow

The ESG is required to protect the AccessNow client web pages from click jacking attacks. To protect against click jacking enable the following settings in the ESG configuration file and set the desired values for each:

```
<Section name="InternalWebServer">
            <Property name="XFrameOptions" type="string" value="" />
            <Property name="ContentSecurityPolicy" type="string" 
value="" />
            <Property name="AccessControlAllowOrigin" type="string" 
value="*" />
</Section>
```

Note: XFrameOptions is deprecated but may be used by older MSIE browsers. Consider setting ContentSecurityPolicy to “frame-ancestors 'none'” along with XFrameOptions.

HTTP Host Header Value Reflection Protection

When auto-redirect from HTTP to HTTPS is enabled in ESG a malicious client can cause a redirection to an arbitrary website via a HTTP Host Header Value Reflection attack. This is done when a client passes an incorrect value in the HTTP Host header. Two **EricomSecureGateway.config** settings have been added in v9.2 to prevent this. These settings are only used during HTTP to HTTPS redirection. Note that these two settings operate independently from each other.

AutoRedirectAllowedHost (Regex)

When configured, the incoming Host is matched against this Regular Expression. If the match fails, the redirection will fail with a BadRequest error.

Examples:

To match a specific host: ^esg.mycompany.com$

To match a specific domain: [.]mycompany.com$

To match two specific hosts: ^(h1|h2)[.]mycompany.com$

If the match failed (either an invalid host or a incorrect regular expressions), a messages is added to the ESG log file.

AutoRedirectHttpToHost

When specified, instead of redirecting to HTTPS on the incoming Host name, always redirect to this host (with optional port value) regardless of the value of incoming Host.

11. TECHNICAL SUPPORT

Release Notes

V10.0 (2022)

- Validated on Windows 11, Windows 10 LTSC 2021, Windows 10 21H2, and Server 2022
- Windows 2008R2 no longer supported

V9.5 (2021)

- Compatible with FIPS compliant systems
- JQuery components updated to latest version

V9.4 (2020)

- Maintenance release

V9.2 (2020)

- Two new settings to protect against to HTTP Host Header Value Reflection attacks: AutoRedirectAllowedHost and AutoRedirectHttpToHost (31242)

V9.1 (2019)

- Maintenance version

V9.0 (November 2018)

- Windows 2019 support
- Windows 10 SAC 1809 support
- Version alignment – includes AccessNow and Blaze components matching the same version
- TLS 1.0 disabled by default, can be re-enabled in the configuration file if needed.

V8.5 (September 2018)

- Version alignment – includes AccessNow components matching the same version
- Web Administration Consoles (ESG and EAG) – updated jQuery components to the latest version

V8.4 (March 2018)

- Version alignment – includes AccessNow components matching the same version
- System Requirement update: .Net 4.6.2

V8.3 (December 2017)

- Version alignment – includes AccessNow components matching the same version

V8.2 (October 2017)

- Version alignment – includes AccessNow and Blaze components matching the same version
- Added documentation for SWEET32 and Medium Strength Cipher mitigation
- System Requirement update: .Net 4.5.2

V8.1 (June 2017)

- Version alignment – includes AccessNow and Blaze components matching the same version
- Added clarification content to the trusted certificate section

v8.0 (April 2017)

- Version alignment – includes AccessNow and Blaze components matching the same version

v7.6.1 (February 2017)

- Windows 2016 compatible
- End-user client IP address and address range security whitelist
- Target server IP address and address range security whitelist
- Relay (AccessServer) server IP address and address range security whitelist
- Disable HTTP/HTTPS usage to force Websocket mode
- Enhanced protection against CSRF
- Same-origin verification

Starting from version 7.6.1, release notes will be listed in this section. Release notes for prior versions are provided upon request via technical support.

Common AccessNow Error Messages

Most modern browsers will require that a trusted certificate be used when establishing an encrypted session.

If the user receives the error “Failed to connect using both WebSockets and HTTPS” - there could be a problem with the certificate on the ESG server.

Verify the address that is being used for the ESG. If it is an IP address, it may pose a problem as it will not match the certificate.

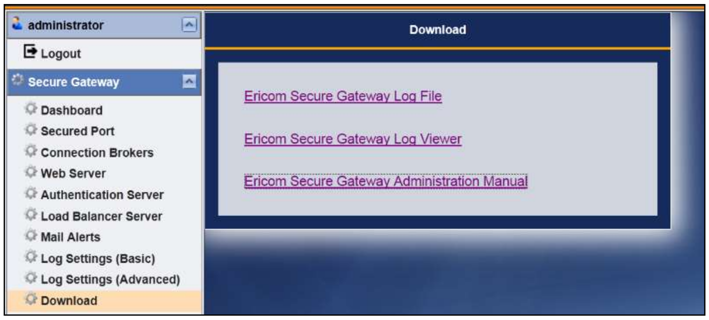
Rather than using the IP address, use a domain name that matches a trusted certificate that has been configured in the ESG.

For example, instead of using 192.168.1.111, use its domain name: *esg.test.com*.

Moreover, install a trusted certificate on the ESG that matches esg.test.com or *.test.com

Obtaining Log Files

When requesting technical support, the ESG logs may be requested. The current log file is accessible using the Configuration page, go to *Download*. The actual log levels may be set under the two Log pages. Consult with an Ericom support engineer on which settings to enable.



The logs require a special viewer that is also downloadable using the *Download* page. The full logs folder is located in a path similar to:

C:\Program Files (x86)\Ericom Software\Ericom Secure Gateway\Logs

Disabling HTTP/HTTPS filtering

Occasionally, certain types of network traffic will be blocked by firewalls. Port 80 and 443 on most firewalls are initially reserved for HTTP and HTTPS respectively. Most firewalls will have a rule in place to filter out any non-HTTP traffic. Depending on what the Secure Gateway will be routing, HTTP filtering may need to be disabled on the firewall.

The Ericom Secure Gateway can proxy various types of traffic. Some are HTTP based and some are not. The only configuration where HTTP filtering does not need to be disabled is if the Web Application Portal and AccessNow are used together.

This table denotes the protocol used by a connection method:

Communication type	**Protocol used**

Web Application Portal login	HTTP/HTTPS
AccessToGo login	HTTPS
Application Zone login	TCP
AccessNow RDP session	HTTPS (Secure Gateway required)
AccessToGo RDP or Blaze session	TCP
RemoteView RDP or Blaze session	TCP

Admin Configuration Portal Idle Timeout

The default idle timeout for the Admin Configuration Portal is five minutes. To change this, edit the EricomSecureGateway.exe.config file and set the *sessionsSettings/Admin/InactivityTimeoutMinutes* setting.

ABOUT ERICOM

Ericom® Software is a leading global provider of Application Access, Virtualization and Cybersecurity Solutions. Since 1993, Ericom has been helping users access enterprise mission-critical applications running on a broad range of Microsoft Windows Terminal Servers, Virtual Desktops, legacy hosts and other systems. Ericom has offices in the United States, United Kingdom and EMEA. Ericom also has an extensive network of distributors and partners throughout North America, Europe, Asia and the Far East. Our expanding customer base is more than 30 thousand strong, with over ten million installations. For more information about Ericom and its products, please visit http://www.ericom.com

For more information about Ericom and its products, please visit http://www.ericom.com

North America
Ericom Software Inc.
231 Herbert Avenue, Bldg. #4
Closter, NJ 07624 USA
Tel +1 (201) 767 2210
Fax +1 (201) 767 2205
Toll-free 1 (888) 769 7876
Email info@ericom.com

UK & Western Europe
Ericom Software (UK) Ltd.
11a Victoria Square
Droitwich, Worcestershire
WR9 8DE United Kingdom
Tel +44 (0)1905 777970

Email ukinfo@ericom.com

International
Ericom Software Ltd.
8 Hamarpeh Street
Har Hotzvim Technology Park
Jerusalem 9777408 Israel
Tel +972 (2) 591 1700
Fax +972 (2) 571 4737
Email info@ericom.com