



Wonderware
InTouch® Access
Anywhere Secure
Gateway
Administrator Manual

All rights reserved. No part of this documentation shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Invensys Systems, Inc. No copyright or patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this documentation, the publisher and the author assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

The information in this documentation is subject to change without notice and does not represent a commitment on the part of Invensys Systems, Inc. The software described in this documentation is furnished under a license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of these agreements.

© 2014 by Invensys Systems, Inc. All rights reserved.

Invensys is a Schneider Electric company.

Invensys Systems, Inc.
26561 Rancho Parkway South
Lake Forest, CA 92630 U.S.A.
(949) 727-3200

<http://www.wonderware.com>

For comments or suggestions about the product documentation, send an e-mail message to ProductDocumentationComments@invensys.com.

All terms mentioned in this documentation that are known to be trademarks or service marks have been appropriately capitalized. Invensys Systems, Inc. cannot attest to the accuracy of this information. Use of a term in this documentation should not be regarded as affecting the validity of any trademark or service mark.

Alarm Logger, ActiveFactory, ArchestrA, Avantis, DBDump, DBLoad, DT Analyst, Factelligence, FactoryFocus, FactoryOffice, FactorySuite, FactorySuite A², InBatch, InControl, IndustrialRAD, IndustrialSQL Server, InTouch, MaintenanceSuite, MuniSuite, QI Analyst, SCADAAlarm, SCADASuite, SuiteLink, SuiteVoyager, WindowMaker, WindowViewer, Wonderware, Wonderware Factelligence, and Wonderware Logger are trademarks of Invensys plc, its subsidiaries and affiliates. All other brands may be trademarks of their respective owners.

Contents

	Welcome	5
	Documentation Conventions	6
	Technical Support	6
Chapter 1	Introduction	7
	Architecture	8
Chapter 2	Installation.....	9
	Prerequisites	9
	Secure Gateway Installation	10
	Secure Gateway Configuration	11
	Uninstalling the Secure Gateway	12
Chapter 3	Secure Gateway Post Installation	13
	Connecting to an InTouch Access Anywhere Server through the Secure Gateway	13
	Configuring the Secure Gateway Node to Expose InTouch Applications	15
Chapter 4	Configuration Portal.....	17
	Dashboard	18

	Mail Alerts	19
	InTouch Access Anywhere HTML5 Client Configuration	19
	Configuration	20
	Advanced Configuration	20
	High Availability	21
	SSO Form Post	21
	Sample Page to POST Values	22
	Sample Page to Receive POST Values	23
	Built-InAuthentication Server	24
Chapter 5	Port and SSL Certificate	25
	Configure the Secured Port and SSL Certificate	27
	Manually Configure a Trusted Certificate	27
	Configure Failover Gateways	28
Chapter 6	Built-In Web Server	29
	External Web Server	30
	Connecting to the Web Server	30
	HTTP Redirect	31
	Disabling HTTP/HTTPS Filtering	32
	Advanced Configuration	32
	Preventing Access to non-listed Folders	33
Chapter 7	Known Limitations.....	35
	Common Error Messages	35
	Obtaining Log Files	36

Welcome

Use InTouch[®] Access Anywhere[™] Secure Gateway to access Wonderware InTouch applications hosted on Terminal Servers by using HTML5 compatible web browsers. Follow the instructions to begin using InTouch Access Anywhere.

This manual assumes knowledge of the following:

- Wonderware[®] InTouch[®]
- Enabling and configuring RDP on Windows operating systems
- Firewall configuration
- Web server administration

Important terminology includes the following:

- DMZ (demilitarized zone) - a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network.
- HTML5 - a new update to the HTML specification. Extends HTML with new features and functionality for communication, display and more.
- 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 (RDP Session Host) or Windows workstation with remote access enabled.
- SSL - Secure Sockets Layer is a cryptographic protocol that provides communications security over the Internet.

- VPN - Virtual Private Network. It enables a computer to securely send and receive data across shared or public networks as if it were directly connected to the private network.
- WebSocket - a bi-directional, full-duplex communication mechanism introduced in the HTML5 specification.

Please visit www.wonderware.com for more information on this and other Wonderware products.

Documentation Conventions

This documentation uses the following conventions:

Convention	Used for
Initial Capitals	Paths and file names.
Bold	Menus, commands, dialog box names, and dialog box options.
Monospace	Code samples and display text.

Technical Support

Wonderware Technical Support offers a variety of support options to answer any questions on Wonderware products and their implementation.

Before you contact Technical Support, refer to the relevant section(s) in this documentation for a possible solution to the problem. If you need to contact technical support for help, have the following information ready:

- The type and version of the operating system you are using.
- Details of how to recreate the problem.
- The exact wording of the error messages you saw.
- Any relevant output listing from the Log Viewer or any other diagnostic applications.
- Details of what you did to try to solve the problem(s) and your results.
- If known, the Wonderware Technical Support case number assigned to your problem, if this is an ongoing problem.

Chapter 1

Introduction

InTouch Access Anywhere Secure Gateway is a complementary component of the InTouch Access Anywhere server which provides secure remote access to InTouch applications past a firewall through a DMZ.

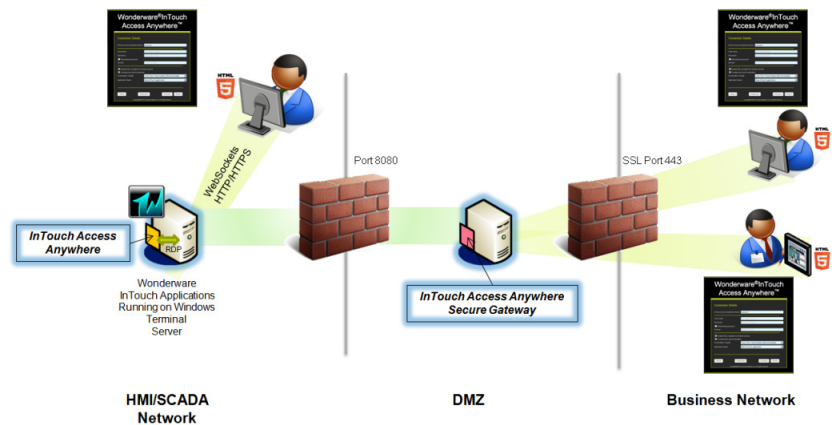
Secure Gateway provides the following benefits:

- Accesses internal resources using a single secure port
- Eliminates the need to purchase, install, configure and manage VPN
- Secure Gateway is installed in a perimeter network, also known as a DMZ, while all other resources reside securely behind the internal firewall
- Installs a single SSL digital certificate on the Secure Gateway node instead of installing on every host that needs to be accessed
- Compatible with HTML5 client browsers supported by InTouch Access Anywhere

Architecture

Secure Gateway acts as a gateway between users in remote locations and applications in the control network. Secure Gateway can be installed in a DMZ to route traffic between a business network and an HMI SCADA network.

The following diagram illustrates how the Secure Gateway uses a single port for secured remote access. All communication related web traffic and session protocols are tunneled through the SSL based Secure Gateway connection.



Chapter 2

Installation

This chapter describes the process for installing the Secure Gateway. It includes prerequisites needed for installation, a step-by-step procedure, details for configuration, and instructions for uninstalling the Secure Gateway.

Prerequisites

The Secure Gateway requires Windows Server 2003 or higher.

.NET Framework 4 Full Installation is also required and can be downloaded from Microsoft's website, at:

<http://www.microsoft.com/en-us/download/details.aspx?id=17851>

Secure Gateway uses port 443 by default. This is a common port that is also used by IIS, so check for port conflicts.

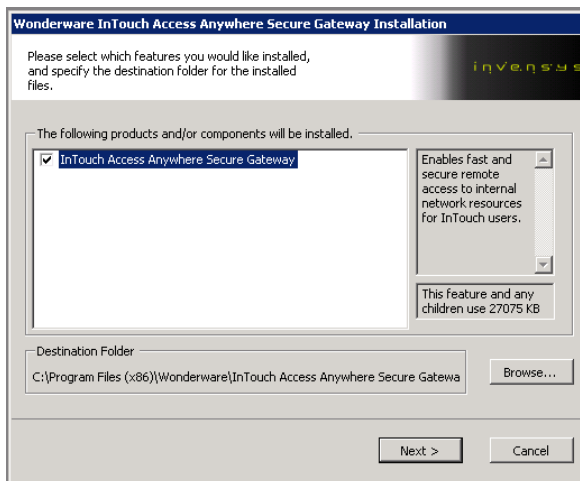
The following ports need to be configured on the network.

- Port 443 is required between the external network and the Secure Gateway server; this value is adjustable.
- For InTouch Access Anywhere Server: Port 8080 is required between the Secure Gateway Server and the InTouch Access Anywhere Server; this value is adjustable.

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

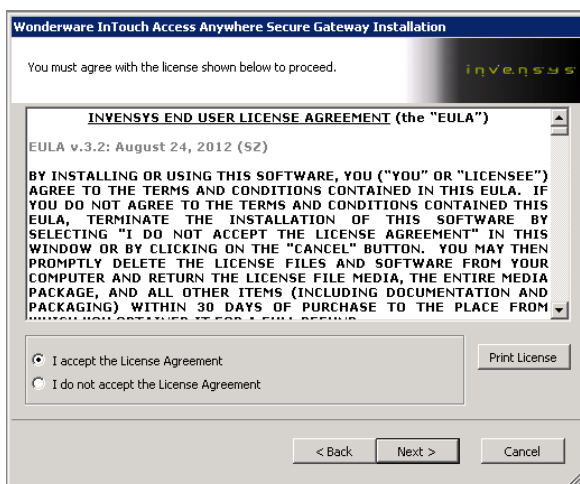
Secure Gateway Installation

- 1 To install the Secure Gateway, launch the installer on a machine running Windows 2003 or higher. Some machines may require authorization to perform the installation.



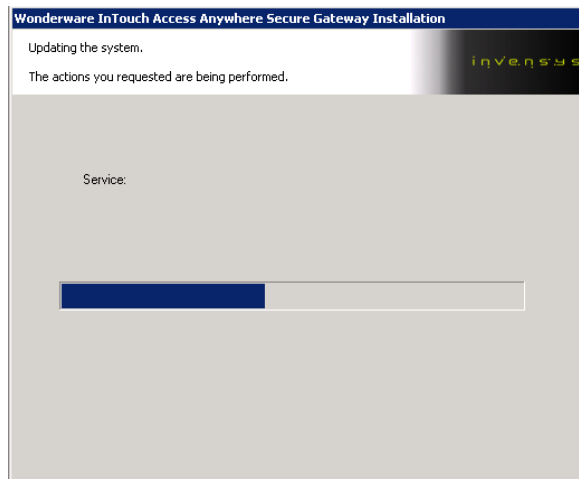
The dialog allows the administrator to specify the installation path by clicking the **Browse** button. We recommend keeping the default installation path.

- 2 Click **Next**.
- 3 Accept the Invensys End User License Agreement.



4 Click Next.

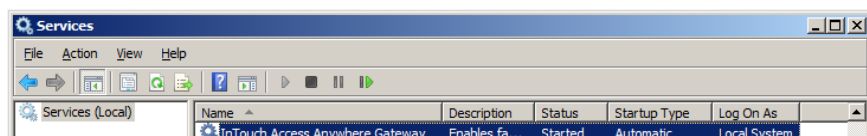
Installation will proceed.

**5 Click Finish.**

Secure Gateway Configuration

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

The Secure Gateway runs as a service, and can be stopped and restarted from the Microsoft Windows Services Manager:

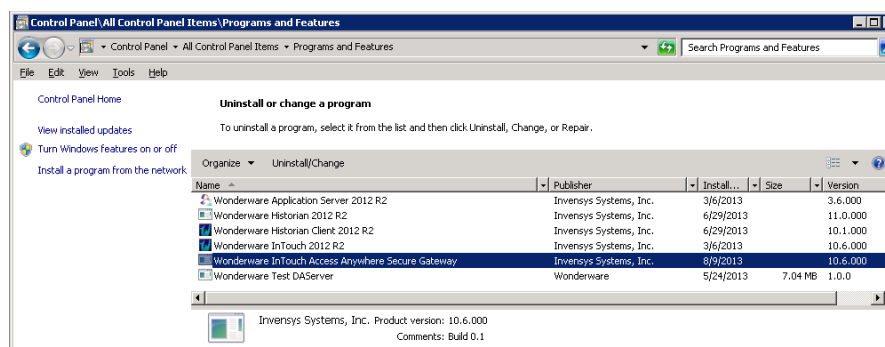


The service is configured to run automatically on system startup. If the service is stopped or is unable to listen on its configured port, clients will be unable to connect to hosts through the gateway and an error message will be written into the Windows application event log.

Important: If Microsoft 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, the Secure Gateway will not operate properly.

Uninstalling the Secure Gateway

Uninstall the Secure Gateway by using the Control Panel **Add/Remove Programs** or **Programs and Features**. Select the Wonderware InTouch Access Anywhere Secure Gateway and click **Uninstall**.



Chapter 3

Secure Gateway Post Installation

This chapter describes the process of connecting to the InTouch Access Anywhere Server through the Secure Gateway and how to configure the Secure Gateway Node.

Connecting to an InTouch Access Anywhere Server through the Secure Gateway

For the sake of the installation procedure the following steps will assume the InTouch Access Anywhere Server is installed on Node 1 and InTouch Access Anywhere Secure Gateway is installed on Node 2.

Access the InTouch Access Anywhere Server through the InTouch Access Anywhere Secure Gateway node.

When you navigate to <https://<node2 name>/>, the following page appears:



To access InTouch Access Anywhere Server on Node1, enter the machine name or IP address of Node1 in the **InTouch Access Anywhere Server** field and click **Next**.

There are two possible scenarios:

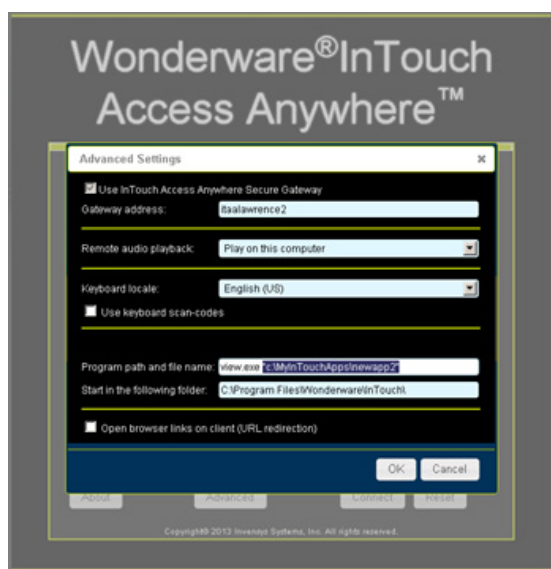
Scenario 1: InTouch Access Anywhere Secure Gateway node (Node2) has not yet been configured to expose the InTouch applications list.

In this scenario, you will be guided to a default page. Perform the following steps to connect to the InTouch application you want to open:

- 1 Enter correct resolution of the last application opened in WindowViewer on Node1 in the **Screen Resolution** field.



- 2 Click **Advanced**. The **Advanced Settings** dialog appears.



- 3 In the **Program path and filename** field, enter "view.exe" and the path for the InTouch application you want to open. For example:
view.exe "c:\MyInTouchApps\newapp2"

Important: Note that the path is enclosed within quotation marks and separated from view.exe

- 4 In the **Start in the following folder** field, enter the InTouch installation path.

Scenario 2: Secure Gateway node is configured to expose the InTouch Applications list.

In this scenario, you will be directed to a page that looks similar to the start page for accessing an InTouch Access Anywhere Server. In this case, select the application you want to open in WindowViewer, then click **Connect**.



Configuring the Secure Gateway Node to Expose InTouch Applications

You can display a list of your InTouch applications in the InTouch Access Anywhere Server, accessed through the Secure Gateway.

- 1 From Node1, where the InTouch Access Anywhere Server is installed, clone (copy and paste) the Start.html page located in the following directory:
<InTouch Access Anywhere Server installation folder>\WebServer\AccessAnywhere\
- 2 Rename the cloned file and go to Node2. Paste the file under <InTouch Access Anywhere Secure Gateway installation folder>\Ericom Secure Gateway\WebServer\AccessAnywhere\ folder on the Gateway node (i.e. Node 2).

Note: The start page can be renamed to any valid file name but for better readability, we recommend prefixing the file name, with the InTouch Access Anywhere server name. For example, if the server name is Master01, the start page should be renamed to Master01_start.html.

3 Open Start.html and locate the following html element:

```
<select id="ITAAServerList" name="ITAAServerList"
style="visibility:hidden">
    <!-- A sample option element
    <option ServerName="Master01" IPAddress="xx.x.xx.xx"
StartPageName="Master01_Start.html"/>
    -->
</select>
```

4 Add an option element under the select element (an example is given) and update the property values as follows:

- The ServerName property value should be set to InTouch Access Anywhere server name (Node1 in our example).
- The IPAddress property value should be the IP Address of the server. Setting the value will allow the page to be accessed when you use IPAddress instead of ServerName.
- The StartPageName property value should be set to the start page name from step 2 above.

5 Save the changes.

Now you will be able to see the Application Name list with all the InTouch applications available at the InTouch Access Anywhere Server node.



Chapter 4

Configuration Portal

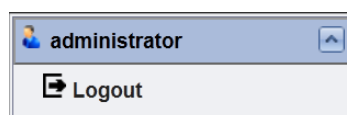
The InTouch Access Anywhere Secure Gateway includes a Configuration Portal which allows the administrator to adjust any related settings. To access the Configuration Portal page, use a web browser and navigate to the Secure Gateway's configuration URL:

<https://<SG-server-address>:<port-number>/admin>

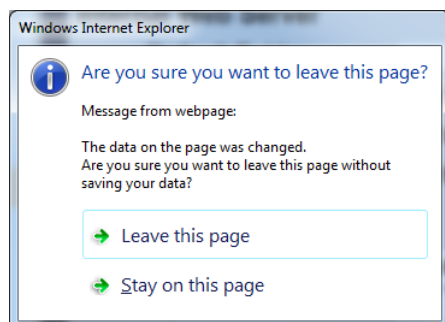
Login is available to members of the local Administrators group on the InTouch Access Anywhere Secure Gateway server. All logins are audited in the Secure Gateway log file. Administrators are strongly advised to impose a strong passwords policy for Secure Gateway user names.



To log out of the Configuration Portal, click **Logout**.

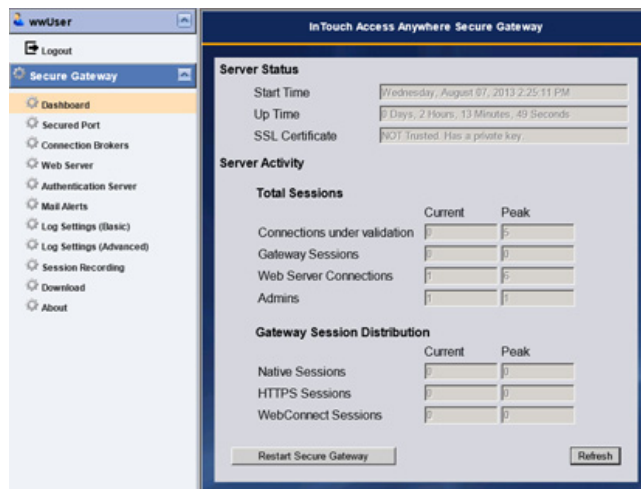


After making changes to any settings, click **Save**. If a different page is selected and the settings are not saved, a warning dialog will appear. Click **Leave this Page** to continue and cancel any changes. Click **Stay on this page** to return to the current page to save changes.



Dashboard

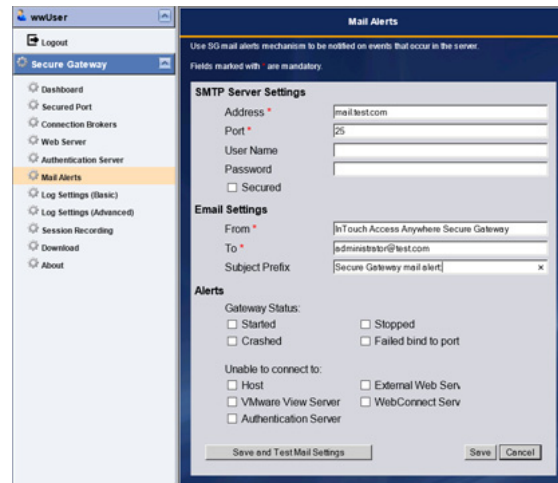
Secure Gateway Configuration Dashboard displays useful statistics related to the Secure Gateway operation. Open this page to view server uptime, SSL certificate status, session activity, and to restart the Secure Gateway Server service.



Mail Alerts

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

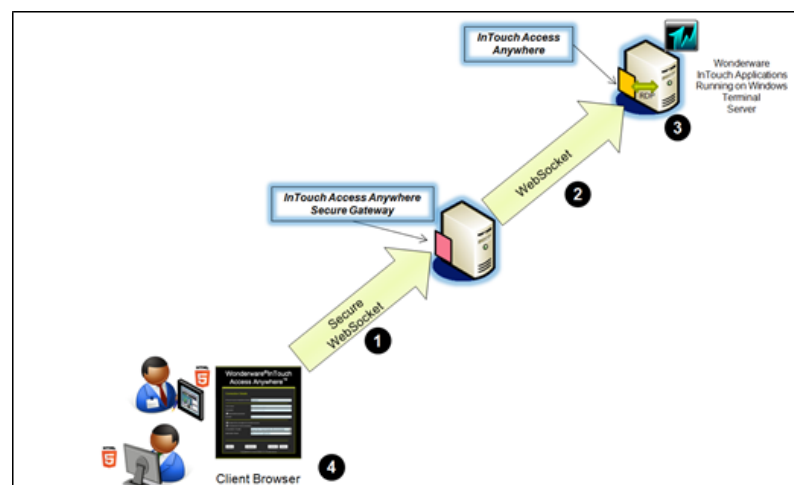
Click **Save** or **Save and Test Mail Settings** to apply the configuration.



Other configuration pages will be covered in the following chapters.

InTouch Access Anywhere HTML5 Client Configuration

InTouch Access Anywhere can use the Secure Gateway to provide secured connections between HTML5 Web clients and InTouch Access Anywhere servers. The following diagram shows how these components work together.



In this configuration, the client browser always establishes a secure WebSocket connection to the Secure Gateway. The Gateway then establishes a WebSocket connection to the InTouch Access Anywhere server.

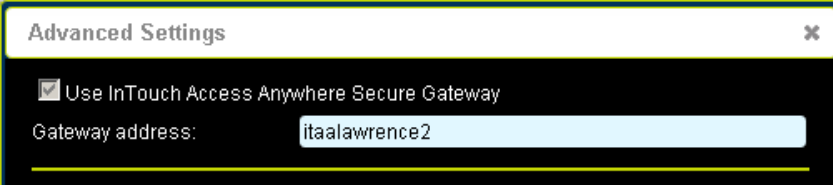
Whether the WebSocket connection between the Gateway and the InTouch Access Anywhere server can be secured or not is based on a configuration setting in the InTouch Access Anywhere client (check the box marked **Enable SSL** for the InTouch Access Anywhere web configuration).

Configuration

Follow these steps to enable the use of a Secure Gateway with InTouch Access Anywhere:

At the client browser, click the Advanced button in the Connection Details page.

Select **Use InTouch Access Anywhere Secure Gateway** and provide the Gateway address:



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. The configuration settings are also defined in the section "Built-InAuthentication Server" on page 24

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

High Availability

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

The load balancer will provide one address for end users. 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.

SSO Form Post

When using a third-party authentication entity (such as an SSL VPN) that supports Form Post, the user can sign on to an InTouch Access Anywhere session using the authenticated credentials. The Secure Gateway 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://sq-address/AccessAnywhere/sso>

Note: The Secure Gateway will auto-redirect the request to the respective default page (start.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:

Label	Name	Value	User modifiable?
<input type="checkbox"/>	cookie-prefix	esg-cookie-prefix EAN_	Not modifiable
<input type="checkbox"/>	Username	login <USER>	Not modifiable
<input type="checkbox"/>	Password	password <PASSWORD>	Not modifiable
<input type="checkbox"/>	autostart	autostart yes	Not modifiable
<input type="checkbox"/>	anserveraddress	address 192.168.0.88	Not modifiable

The value "esg-cookie-prefix" in the graphic above defines the Access Anywhere cookie prefix in the Single Sign-on form. For InTouch Access Anywhere 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, 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 Access Anywhere Secure Gateway: <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="esgcookieprefix" 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 Access Anywhere Secure Gateway: " &
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>
```

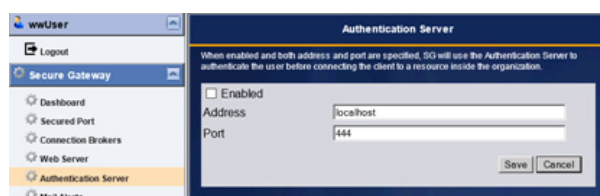
Built-In Authentication Server

The Secure Gateway includes an Authentication Server which provides a layer of security by authenticating end-users before they contact any internal resource (for example, the InTouch Access Anywhere Server).

The Authentication Server is installed on a server that is a member of the domain and which is employed to authenticate users.

Note: 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.

Chapter 5

Port and SSL Certificate

The InTouch Access Anywhere Secure Gateway includes a signed certificate. Certain web browsers may display a security warning when a signed certificate is detected. To remove the warning, install a trusted certificate purchased from a trusted certificate authority (for example, VeriSign).

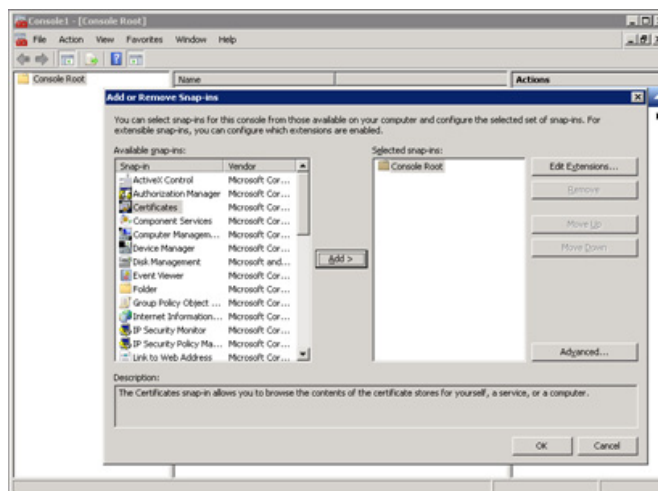
Important: The signed certificate must have a private key associated with it. A .CER file may not have a private key. Use a signed certificate that includes a private key, which usually has a .PFX extension.

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

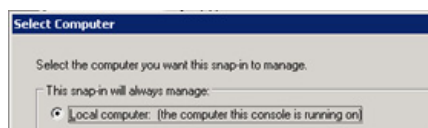
To add, view, or modify certificates, perform the following:

- 1** Run mmc.exe
- 2** Go to **File | Add/Remove Snap-in**.

3 Add Certificates and select **Computer account**.

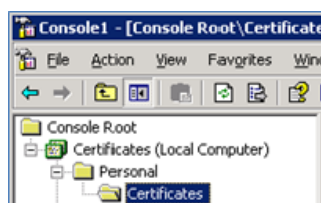


4 Select **Local Computer**.



5 Click **Finish** and then **OK**.

6 Browse **Certificates | Personal | Certificates** folder to view all the available certificates that can be used by the Secure Gateway.



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

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

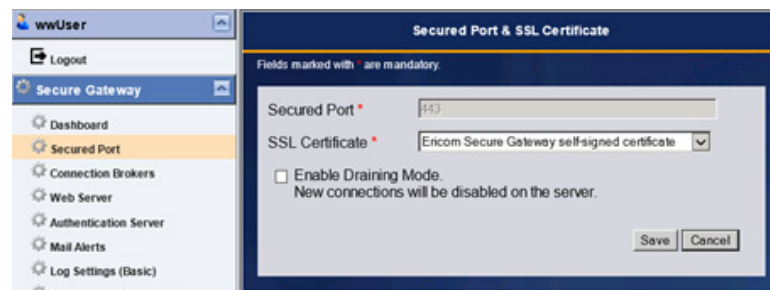
```
<add key="CertificateThumbprint" value="<enter trusted certificate thumbprint value here>" />
```

Configure the Secured Port and SSL Certificate

In the Configuration Dashboard, use the Secured Port & SSL Certificate page to modify the port that will be used by the Secure Gateway.

Important: Before configuring the port, make sure it is not already in use.

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



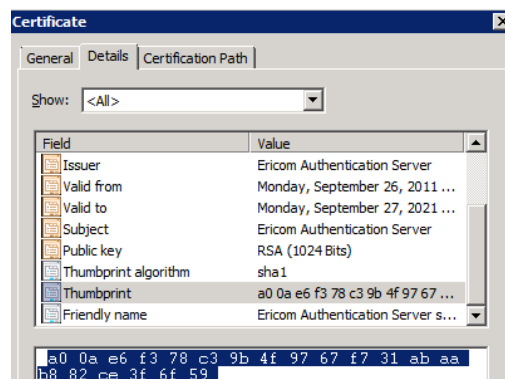
Manually Configure a Trusted Certificate

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.

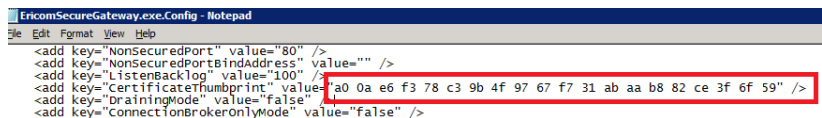
Method 2: Add the thumbprint value to the configuration file by performing the following:

- 1 Go to the **Certificate Details** tab and highlight **Thumbprint**.



- 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 paste 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, a "Connection failed" error message will appear upon attempting a connection.

Configure Failover Gateways

Multiple Secure Gateways can be configured as a failover chain in the **InTouch Access Anywhere** web client. This will provide redundancy for the Secure Gateway function. Alternate Gateways will be automatically used when the primary one is unavailable. If the connection to the first Secure Gateway on the list fails, the request will be redirected to the next server on the list.

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

The following is a sample list of servers:

Us-bl2008r2;securegateway.domainname.com;192.168.0.3:4343

- The primary gateway is Us-bl2008r2 over port 443.
- The second Secure Gateway is securegateway.domainname.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).

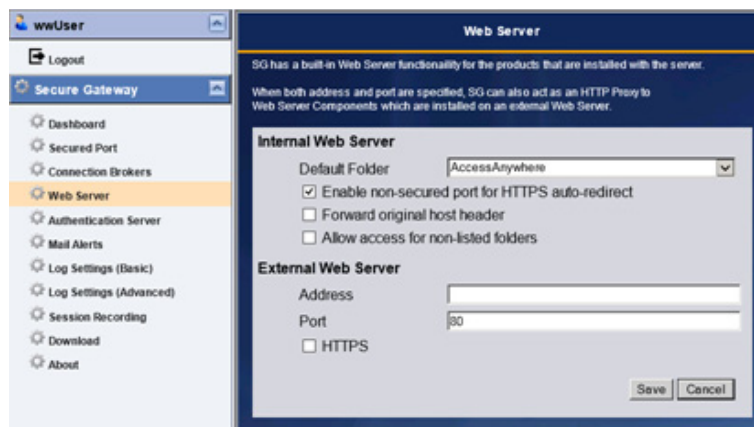
Note: Maintain uptime for the servers at the front of the list to ensure the fastest login time. If the primary server is unavailable, end-users will experience longer login time, as the login process must wait for the primary server to timeout before attempting to connect to a failover server.

Chapter 6

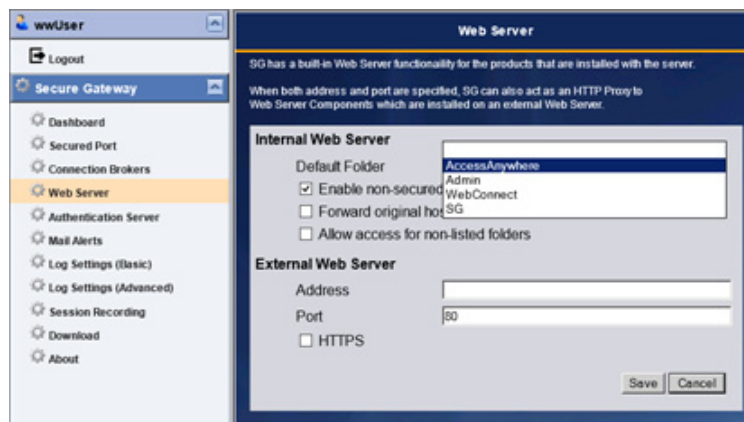
Built-In Web Server

The Secure Gateway has a built-in Web server which supports the ability to host the web pages for certain products such as InTouch Access Anywhere. The built-in Web server cannot be disabled and always listens on the Secure Gateway port.

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



Click the drop down box to select 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 InTouch Access Anywhere Server is selected, when the user navigates to `https://<sg-server-address>:<port-number>/` the URL will automatically redirect to:

`https://<sg-server-address>:<port-number>/AccessAnywhere/start.html`

Note: The Secure Gateway could technically be used to host non-related pages, but this is not officially supported. Hosted web pages should be of basic static content.

External Web Server

The InTouch Access Anywhere Secure Gateway also has a built-in Web server proxy.

Note: Using the Secure Gateway to proxy to pages other than InTouch Access Anywhere is not officially supported.

Connecting to the Web Server

To connect to an InTouch Access Anywhere server available through the Secure Gateway Web server, open a browser and navigate 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/AccessAnywhere/start.html`

The following URL's are available by default.

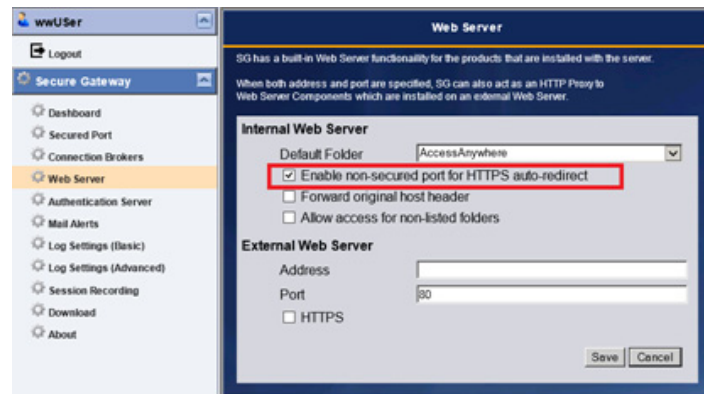
Secure Gateway Welcome Page	https://server:port/ or https://server:port/welcome.html
InTouch Access Anywhere Server	https://server:port/AccessAnywhere/start. html

HTTP Redirect

The InTouch Access Anywhere Secure Gateway Web server listens on port 80 by default. This way, HTTP references to the server will automatically redirect to the HTTPS URL.

Note: 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 (see below).



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

Disabling HTTP/HTTPS Filtering

Certain types of network traffic will sometimes be blocked by firewalls. Port 443 on most firewalls are initially reserved for HTTP (and HTTPS) based communication. 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 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 when the Web Application Portal and InTouch Access Anywhere are used together.

This table denotes the protocol used by a connection method:

Communication Type	Protocol Used
Web Application Portal login	HTTP/HTTPS
Application Zone login	TCP
InTouch Access Anywhere RDP session	HTTPS (Secure Gateway required)

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
AccessAnywhere	8/7/2013 2:25 PM	File folder	
Admin	8/7/2013 2:25 PM	File folder	
Blaze	8/7/2013 2:25 PM	File folder	
MyCustom	8/7/2013 4:20 PM	File folder	
SG	8/7/2013 2:25 PM	File folder	
View	8/7/2013 2:25 PM	File folder	
welcome.html	7/26/2013 12:16 PM	HTML Document	

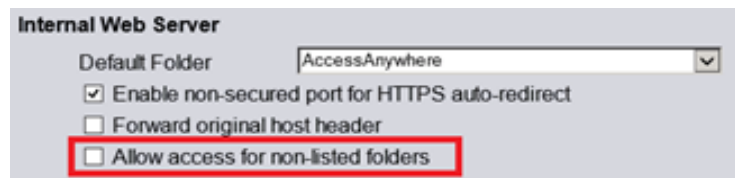
For example, the settings below will configure the following:

- 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 Blaze and MyCustom folders.


```
<internalWebServerSettings>
<Folders default_folder="View"
allow_access_for_non_listed_folders="false">
<add folder_name="AccessAnywhere" default_page="start.html"
allow_access="true"/>
<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 Secure Gateway 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="true"`).



Chapter 7

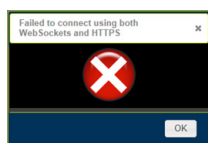
Known Limitations

This chapter lists a number of known behaviors and limitations. Please refer to *InTouch Access Anywhere ReadMe* for a more detailed list of current known issues in Secure Gateway.

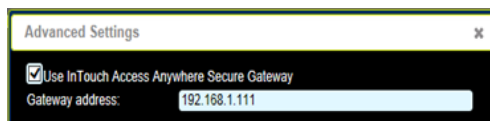
Common Error Messages

Most browsers will require a trusted certificate when establishing an encrypted session.

If you see an error message similar to that in the figure below, there could be a problem with the certificate on the InTouch Access Anywhere Secure Gateway server.



If this error appears, check the address that is being used for the InTouch Access Anywhere Secure Gateway. If it is an IP address, like the image shown below, it may pose a problem.



Rather than using the IP address, use a domain name that matches a trusted certificate that has been configured in the InTouch Access Anywhere Secure Gateway.

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

In addition, install a trusted certificate on the InTouch Access Anywhere Secure Gateway that matches sg.test.com or *.test.com

Obtaining Log Files

If you require technical support, the Secure Gateway log files may be requested.

Note: The logs require a special viewer which can be downloaded from the Download page

The current log file is accessible using the Configuration page under the Download tab. The actual log detail levels may be set under the two log pages (Log Settings - Basic and Log Settings- Advanced).

Consult with a support engineer on which settings to enable.

