

AVEVA™

**InTouch Access Anywhere Secure
Gateway Administrator Manual**



AVEVA

© 2020 AVEVA Group plc and its subsidiaries. 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 AVEVA. No liability is assumed with respect to the use of the information contained herein.

Although precaution has been taken in the preparation of this documentation, AVEVA assumes no responsibility for errors or omissions. The information in this documentation is subject to change without notice and does not represent a commitment on the part of AVEVA. The software described in this documentation is furnished under a license agreement. This software may be used or copied only in accordance with the terms of such license agreement.

Archestra, Aquis, Avantis, Citect, DYNsIM, eDNA, EYESIM, InBatch, InduSoft, InStep, IntelaTrac, InTouch, OASyS, PIPEPHASE, PRiSM, PRO/II, PROVISION, ROMeo, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, Termis, WindowMaker, WindowViewer, and Wonderware are trademarks of AVEVA and/or its subsidiaries. An extensive listing of AVEVA trademarks can be found at: <https://sw.aveva.com/legal>. All other brands may be trademarks of their respective owners.

Publication date: Thursday, November 19, 2020

Contact Information

AVEVA Group plc
High Cross
Madingley Road
Cambridge
CB3 0HB. UK

<https://sw.aveva.com/>

For information on how to contact sales and customer training, see <https://sw.aveva.com/contact>.

For information on how to contact technical support, see <https://sw.aveva.com/support>.

Contents

Welcome	5
Documentation Conventions	5
Technical Support	6
Chapter 1 Introduction.....	7
Introduction About the Secure Gateway	7
Architecture	7
Chapter 2 Installation	9
Installation About Installing the Secure Gateway	9
Installation Overview	9
Installation Prerequisites.....	9
Resolving Secure Gateway Conflicts	10
Secure Gateway Installation	11
Other Secure Gateway Installation Configurations	11
Secure Gateway and Authentication Servers on a Windows Workstation	12
Install the Secure Gateway and Authentication Server Separately or Together	12
Uninstalling the Secure Gateway	13
Chapter 3 Secure Gateway Post Installation.....	15
Connecting to an InTouch Access Anywhere Server through the Secure Gateway	15
Configuring the Secure Gateway Node to Point to a Single InTouch Access Anywhere Server	17
Configuring the Secure Gateway Node to Point to Multiple InTouch Access Anywhere Servers	18
Chapter 4 Configuration Portal	21
Configuration Portal About the Configuration Portal	21
Dashboard.....	22
Mail Alerts	22
InTouch Access Anywhere HTML5 Client Configuration	24
Configure the Access Anywhere Server to Work with the Secure Gateway	24
Whitelist Security	25
Configuring the Origin Header Parameter for Whitelist Security	27
Configure Session Cookie Timeout	28
Advanced Configuration	28
High Availability	28
Restricting Access To and From a Secure Gateway	29
Built-In Authentication Server.....	29

Disabling Authentication Server with Brokers	30
Chapter 5 Port and SSL Certificate	33
Port and SSL Certificate About Port and SSL Certificate	33
Manually Add a Trusted Certificate	37
Configure the Secured Port and SSL Certificate	38
Configure Failover Gateways	39
Chapter 6 Built-In Web Server	41
Built-In Web Server About the Built-In Web Server	41
External Web Server	42
Connecting to the Web Server	42
HTTP Redirect	42
Disabling HTTP/HTTPS Filtering	43
Advanced Configuration	43
Preventing Access to Non-Listed Folders	44
Chapter 7 Known Limitations	45
Common Error Messages	45
Obtaining Log Files	46

Welcome

Use AVEVA™ InTouch Access Anywhere Secure Gateway to access InTouch applications hosted on Remote Desktop Servers via HTML5-compatible web browsers.

This manual assumes the reader has knowledge of the following:

- 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 Remote Desktop Server (RDP Session Host) or Windows workstation with remote access enabled.
- RDS - Remote Desktop Services, which includes the Remote Desktop Protocol (RDP).
- 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.aveva.com for more information on this and other 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

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

Before contacting Technical Support, refer to the relevant section(s) in this documentation for a possible solution to your 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 Technical Support case number assigned to your problem, if this is an ongoing problem.

CHAPTER 1

Introduction

About the Secure Gateway

AVEVA InTouch Access Anywhere Secure Gateway is a complementary component of InTouch Access Anywhere that provides secure, remote access to InTouch applications.

Secure Gateway provides the following benefits:

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

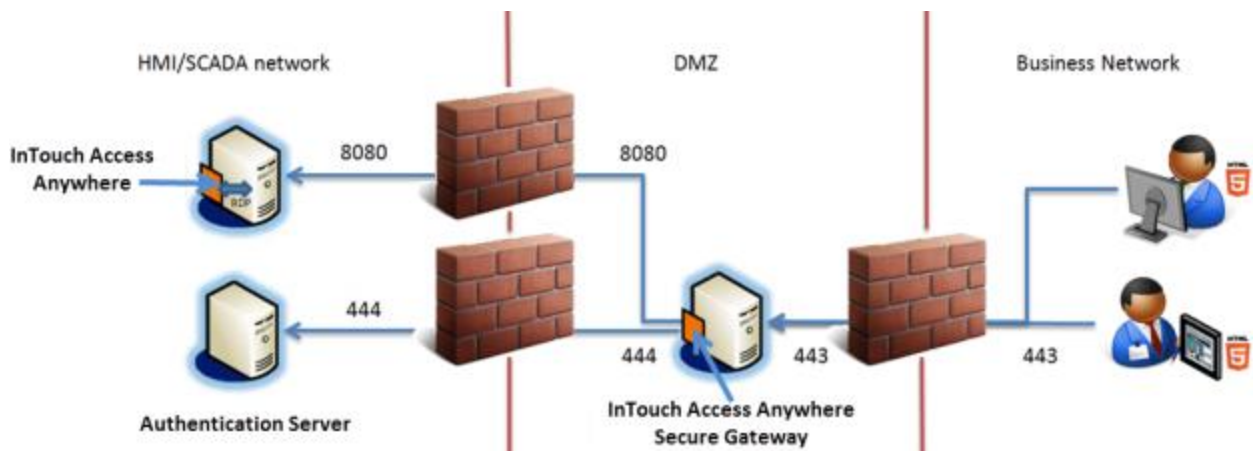
Important

InTouch Access Anywhere is offered as two separate products based on how the product components are installed. InTouch Access Anywhere is included in the suite of products that are part of System Platform. InTouch Access Anywhere Version components are installed by selecting them from the list of the System Platform product installer. InTouch Access Anywhere is the stand-alone version delivered on a single CD. After selecting the Setup.exe file on the CD, a menu appears to select the InTouch Access Anywhere components to be installed.

Functionally, the two versions of InTouch Access Anywhere are the same. This manual describes how to install, manage, and monitor the Secure Gateway for both versions of InTouch Access Anywhere.

Architecture

Secure Gateway acts as a gateway between users in remote locations and InTouch applications running in a control network. The following diagram shows the recommended architecture of the Secure Gateway in a production environment. The Secure Gateway uses a single port for secured remote access to InTouch applications. All web traffic from an external business network is tunneled through an SSL-based connection of the Secure Gateway placed in a DMZ.



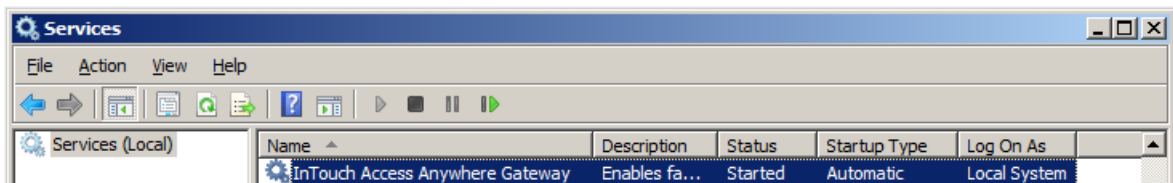
CHAPTER 2

Installation

About Installing the Secure Gateway

This chapter describes how to install the Secure Gateway. It describes installation prerequisites, several step-by-step installation procedures, and how to uninstall a Secure Gateway.

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



The Secure Gateway service is configured to run automatically when the computer starts. If the service stops or is unable to listen on its configured port, clients will be unable to connect to InTouch applications through the gateway. An error message will be written into the Windows application event log.

Note: InTouch Access Anywhere belongs to the suite of products included with System Platform. This book describes how to perform an independent stand-alone installation of the InTouch Access Anywhere Secure Gateway. For instructions to install the Secure Gateway from the System Platform installation media, see the *System Platform Installation Guide*.

Installation Overview

- It is recommended to install the Authentication Server on the safe side of the firewall, while the Secure Gateway should be installed on a separate computer inside the DMZ. The Authentication Server authenticates InTouch Access Anywhere users before granting them access to InTouch applications.

The Authentication Server is disabled by default to be consistent with earlier versions of InTouch Access Anywhere. For more information about enabling the Authentication Server, see *Built-In Authentication Server* on page 29.

- The Secure Gateway is installed with a self-signed certificate. Some web browsers may show a security warning when a self-signed certificate is detected.

Install a trusted certificate on the Secure Gateway to eliminate security warnings. For more information about installing and configuring a trusted certificate on the Secure Gateway, see *Port and SSL Certificate* on page 33.

Installation Prerequisites

The computer hosting the Secure Gateway must meet the following prerequisites before installation.

- Any existing instance of Secure Gateway must be uninstalled from the computer before installing a new version.
- The Secure Gateway must be installed on a computer running a supported version of Windows, which includes:
 - Windows 10 Professional or Enterprise (build 1607 and later) 32 or 64 bit

- Windows 8.1 Enterprise, Professional
- Windows 2012 Data Center 64-bit
- Windows 2012 R2 Standard and Data Center 64-bit
- Windows 2016 Standard and Data Center 64-bit
- Windows Server 2019 LTSC Data Center - Desktop Experience, IoT - Desktop Experience, Standard - Desktop Experience
- .NET Framework 4.6.2 Full Installation or later must be installed on the host computer if you are completing a stand-alone installation of InTouch Access Anywhere.

Note: If you are installing InTouch Access Anywhere from System Platform, the installer verifies the current, installed versions of .NET on the computer. When only earlier versions of .NET are detected, the installer automatically updates the computer to the required .NET version.

The different versions of .NET installed on the computer can be verified by looking at the following registry key:

```
HKLM\SOFTWARE\Microsoft\.NETFramework
```

If you need to install .NET, you can download it from the *Microsoft .NET download site* (<https://www.microsoft.com/net/download/windows>).

- The following ports must be configured on the computer hosting the Secure Gateway:
 - Port 443 is required between an external network and the Secure Gateway server. This is a common port that is also used by Microsoft Internet Information Services (IIS), and / or by Remote Desktop, if Remote Desktop itself is enabled. Check for port conflicts. The port can be changed.
-
- Important:** If Microsoft IIS is running on the same server that will host the Secure Gateway, 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 does not operate properly.
-
- Port 8080 is required between the Secure Gateway Server and the InTouch Access Anywhere Server. The port can be changed.
 - The Secure Gateway includes an HTTP proxy that listens on port 80 by default. The port can be disabled after installing the Secure Gateway.

Resolving Secure Gateway Conflicts

System Platform and InTouch Access Anywhere Secure Gateway uses several ports for communication. A complete list of ports used by System Platform products and components is available in the System Platform Installation Guide. The System Management Server is a required component for running System Platform products. By default, it uses port 443, the same as the Secure Gateway default. Therefore, a conflict results if you are installing any other System Platform component products on the same node as the Secure Gateway. You must change the port number for either the System Management Server or the Secure Gateway. If you change the System Management Server port, you must also change the port number for the System Monitor. In addition, other System Platform nodes must be configured to use the same System Management Server port.

To change the port number for the InTouch Access Anywhere Secure Gateway:

1. Locate the Secure Gateway configuration file, `EricomSecureGateway.Config` and open it for editing. The default file location is: `C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway`

2. Change the value for the SecuredPort to a different, unused port number. The Secure Gateway does not permit port sharing.
3. Save the file.

Secure Gateway Installation

InTouch Access Anywhere belongs to the suite of products included with System Platform. This book describes how to perform an independent stand-alone installation of Secure Gateway. For instructions to install the Secure Gateway from the System Platform installation media, see the *System Platform Installation Guide*.

This section describes the procedure to install the Secure Gateway on a computer running a supported version of Windows server. The Secure Gateway supports other installation configurations. For more information, see *Other Secure Gateway Installation Configurations* on page 11.

After verifying all installation prerequisites, start the installation procedure.

Note: Secure Gateway cannot be upgraded by installing a newer version on a computer hosting an existing version. The existing version of Secure Gateway must be uninstalled first before attempting to install another version on the same computer. For instructions to uninstall Secure Gateway, see *Uninstalling the Secure Gateway* on page 13.

To install InTouch Access Anywhere Secure Gateway

1. Log on as a Windows administrator to the computer that will host the Secure Gateway server.
2. Run **setup.exe** from the CD-InTouchAA folder of the InTouch Access Anywhere installation disc.
A dialog box appears with options to install the InTouch Access Anywhere server, Secure Gateway, or the Authentication server.
3. Select **InTouch Access Anywhere Secure Gateway** and click **Next**.
A dialog box appears with an option to customize the installation by installing the Secure Gateway in another folder location. Otherwise, the Secure Gateway is installed to the default installation folder, C:\Program Files (x86).
4. Accept the license agreement by selecting the **I have read and accept the terms of the license agreement** option, and then click **Agree**.
The **Ready to Install the Application** screen appears.
5. Review the installation details and click **Install**.
6. Click **Finish** after the installer indicates that the **Installation has completed successfully**.

Other Secure Gateway Installation Configurations

InTouch Access Anywhere 17.2 and later versions provide other installation configurations for the Secure Gateway, the Authentication server, and the Authentication server.

- Install the Secure Gateway and the Authentication server on a workstation running Windows 10.
For more information, see *Secure Gateway and Authentication Servers on a Windows Workstation* on page 12
- Install the Secure Gateway and the Authentication server on separate computers or on a single computer.
For more information, see *Install the Secure Gateway and Authentication Server Separately or Together* on page 12
- Install the Access Anywhere server, the Secure Gateway, and the Authentication Server on a single computer running a supported version of Windows server.

For more information, see the *InTouch Access Anywhere Server Administrator Manual*.

Secure Gateway and Authentication Servers on a Windows Workstation

The Secure Gateway and Authentication servers can be installed separately or together on a Windows workstation running 32-bit or 64-bit versions of Windows 10 Professional or Enterprise, Build 1607 and later.

To install the Secure Gateway on a Windows workstation

1. Log on as a Windows administrator of the Windows 10 workstation that will host the Secure Gateway server.
2. Run **setup.exe** from the CD-InTouchAA folder of the InTouch Access Anywhere installation disc.
A dialog box appears with options to install the InTouch Access Anywhere server, Secure Gateway, or the Authentication server.
3. Select **InTouch Access Anywhere Secure Gateway** and click **Next**.
A dialog box appears with an option to customize the installation. You can select other InTouch Access Anywhere servers to install with Secure Gateway and change the default installation folder.
4. Click **Next**.
5. Accept the license agreement by selecting the **I have read and accept the terms of the license agreement** option, and then click **Agree**.
The **Ready to Install the Application** screen appears.
6. Review the installation details and click **Install**.
7. Click **Finish** after the installer indicates that the **Installation has completed successfully**.

Install the Secure Gateway and Authentication Server Separately or Together

The Authentication Server provides an additional layer of security by authenticating end-users before they can contact the Access Anywhere server. 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 logon through the Authentication Server. The Authentication server is an optional InTouch Access Anywhere component and is disabled by default.

InTouch Access Anywhere includes options to install the Secure Gateway and the Authentication server together on a single computer or on separate computers. Follow these requirements when installing the Authentication server:

- The Authentication Server must be installed on a computer that is a member of the domain that it will use to authenticate users.
- The Authentication server can only be configured for one domain at a time.
- The Authentication server should be installed on the safe side of a firewall rather than the DMZ for best security practice.

To install the Secure Gateway and Authentication server on the same or separate computers

1. Log on as a Windows administrator of the computer that will host either the Secure Gateway, the Authentication server, or both.

Note: *Installation Prerequisites* on page 9 lists the versions of Windows supported by the Secure Gateway and the Authentication server.

2. Run **setup.exe** from the CD-InTouchAA folder of the InTouch Access Anywhere installation disc.

A dialog box appears with options to install the InTouch Access Anywhere server, Secure Gateway, or the Authentication server

3. Select how you want to install the Secure Gateway and the Authentication server.

Install the Secure Gateway and the Authentication server on separate computers

- Install the Secure Gateway by following the steps described in *Secure Gateway Installation* on page 11. The Authentication server must be configured by setting options from the Secure Gateway Configuration portal.
- Install the Authentication server on another computer that meets the requirements listed above this procedure.

Install the Secure Gateway and the Authentication server together on the same computer

- Select the Secure Gateway and Authentication server options from the installation dialog box and following the installation instructions.

4. After installing the Authentication server and the Secure Gateway, see *Built-In Authentication Server* on page 29 for descriptions of the options to configure the Secure Gateway to work with an Authentication server.

Uninstalling the Secure Gateway

To upgrade to a later version of Secure Gateway, you must first remove any existing version of Secure Gateway currently installed on a computer.

To uninstall Secure Gateway

1. Open the Windows Control Panel **Programs and Features** option that shows a list of applications installed on the computer.
2. Select InTouch Access Anywhere Secure Gateway from the list.
3. Right-click to show the **Uninstall/Change** option.
4. Click to select the **Uninstall/Change** option.

The **Modify, Repair or Remove installation** dialog box appears.

5. Select **Remove** and click **Next**.

A dialog box requests confirmation that you want to uninstall Secure Gateway.

6. Click **Uninstall** to remove Secure Gateway from the computer.

A message appears after Secure Gateway has been successfully uninstalled from the computer.

CHAPTER 3

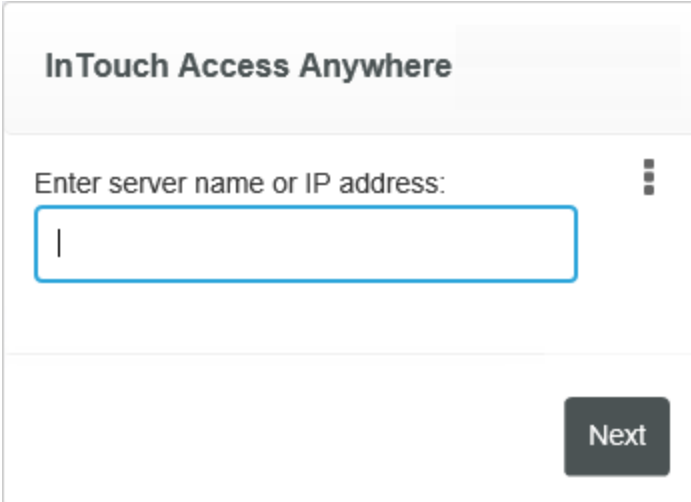
Secure Gateway Post Installation

This chapter describes how to configure the Secure Gateway node to connect to an InTouch Access Anywhere Server.

Connecting to an InTouch Access Anywhere Server through the Secure Gateway

The following logon procedures assume the InTouch Access Anywhere Server is installed on Node 1 and InTouch Access Anywhere Secure Gateway is installed on Node 2.

You access the InTouch Access Anywhere server by first going through the InTouch Access Anywhere Secure Gateway node. When you navigate to `https://<node2 name>/`, the **Connection Details** page appears:



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

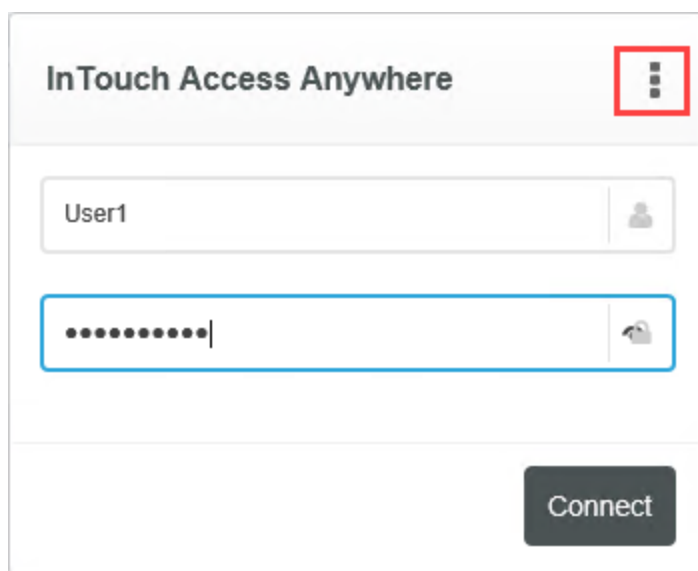
After providing your logon credentials and clicking **Connect**, there are two possible log on scenarios:

Scenario 1: InTouch Access Anywhere Secure Gateway node (Node2) does not show a list of InTouch applications

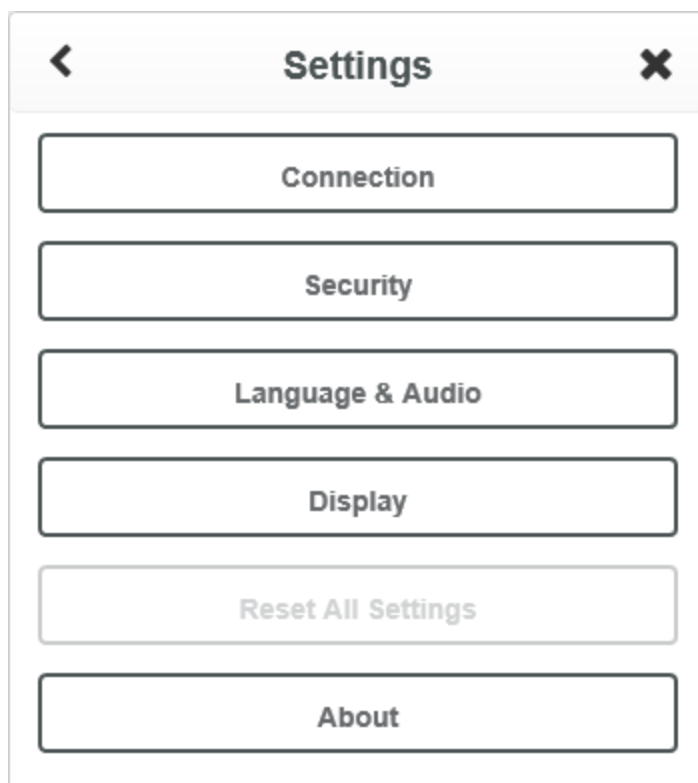
You can perform the following steps when you have a single InTouch Access Anywhere Server and will always run the same InTouch application.

To connect to the InTouch application you want to open:

1. Click the Settings icon .



The **Advanced Settings** dialog appears.



2. Click the **Connection** option.

3. In the **Program path and filename** field, enter **view.exe** followed by the path to the InTouch application you wish to start on the server, enclosed within quotation marks (as shown below). If the path is not supplied, then WindowViewer will start with the last application it was running (as specified by the per-user win.ini file).

The InTouch installation path is populated by default in the **Start in the following folder** field.

Scenario 2: Secure Gateway node shows a list of InTouch applications

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 Point to a Single InTouch Access Anywhere Server

If your Secure Gateway points to a single InTouch Access Anywhere Server, you do not need to specify the name of the server in the start.html file. Use the following procedure to show a list of InTouch applications available from a single InTouch Access Anywhere Server.

To display a list of InTouch applications from a single InTouch Access Anywhere Server

1. On Node 2, where the Secure Gateway is installed, go to the start.html file in the following directory:
C:\ProgramFiles (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway\WebServer\Access Anywhere
2. Rename the start page to StartOriginal.html.
3. On Node 1, where the InTouch Access Anywhere Server is installed, copy the Start.html file from:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\start.html

4. On Node 2, paste the Start.html from Node 1 in the following directory:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway\WebServer\Access Anywhere

You can now see the Application Name list with all InTouch applications available on the single Node 1 InTouch Access Anywhere Server.

Configuring the Secure Gateway Node to Point to Multiple InTouch Access Anywhere Servers

The application list does not populate automatically when accessing the Server through the Secure Gateway. Use the following procedure to display a list of InTouch applications when pointing to multiple InTouch Access Anywhere Servers through the Secure Gateway.

If your Secure Gateway is only configured to host one InTouch Access Anywhere Server, see *Configuring the Secure Gateway Node to Point to a Single InTouch Access Anywhere Server* on page 17 for details on how to make the Application Name list visible from the logon page.

To configure the Secure Gateway to point to multiple InTouch Access Anywhere servers

1. From Node1, where the InTouch Access Anywhere Server is installed, copy the Start.html page located in the following directory:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\start.html

2. Rename the cloned file and go to Node2, where InTouch Access Anywhere Secure Gateway is installed. Paste the file in the following directory:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway\WebServer\Access Anywhere

Note: The start page can be renamed to any valid file name, but for better readability and compatibility, 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 the original Start.html file on the Secure Gateway node and locate the following html element:

```
<select id="ITAAServerList" name="ITAAServerList" style="display:none">>
    <!-- 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 an IP value enables the page to be accessed when you use IPAddress instead of ServerName.
 - The StartPageName property value should be set to the renamed start page name from step 2 above.
5. Save the changes to the Start.html file

6. Repeat the above steps for each additional InTouch Access Anywhere Servers.

Now you can see the **Application Name** list with all InTouch applications available on the InTouch Access Anywhere Server node.

CHAPTER 4

Configuration Portal

About the Configuration Portal

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

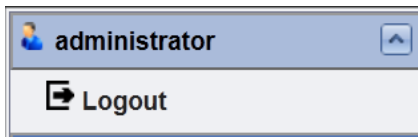
`https://<SG-server-address>:<port-number>/admin`

Accessing the Configuration Portal is restricted to only members of the local Administrators group of the InTouch Access Anywhere Secure Gateway server. All log ons are audited in the Secure Gateway log file. Administrators are strongly encouraged to enforce a strong password policy for Secure Gateway administrators.

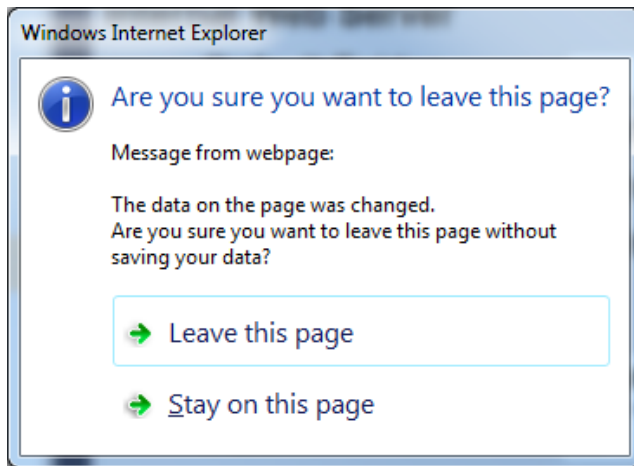


The screenshot shows the login page for the Access Anywhere Secure Gateway Configuration Portal. The page has a dark blue background with a lighter blue gradient. At the top, the title "Access Anywhere Secure Gateway Configuration Portal" is displayed in yellow text. Below the title, there are three white input fields for "User name", "Password", and "Domain". A white "Login" button is positioned below the "Domain" field.

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.

The screenshot shows the 'Server Information' section of the configuration dashboard. On the left is a navigation sidebar with 'Gateway Settings' expanded and 'Dashboard' selected. The main content area is titled 'Server Information' and contains the following data:

Server Status

- Start Time: Tuesday, December 15, 2015 11:51:33 AM
- Up Time: 0 Days, 2 Hours, 5 Minutes, 4 Seconds
- SSL Certificate: NOT Trusted. Has a private key.

Server Activity

Total Sessions

	Current	Peak
Connections under validation	1	15
Gateway Sessions	0	2
Web Server Connections	7	16
Admins	2	2

Gateway Session Distribution

	Current	Peak
Native Sessions	0	2
HTTPS Sessions	0	0
WebConnect Sessions	0	0

At the bottom of the main area, there are two buttons: 'Restart Server' and 'Refresh'.

Mail Alerts

Secure Gateway can be configured to send e-mail alerts when specified system events occur. To configure mail alerts, enter the SMTP information of the e-mail server. Then, check the events that trigger an e-mail alert.

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

The screenshot shows the 'Mail Alerts' configuration page. On the left is a navigation menu with 'Gateway Settings' expanded to show 'Mail Alerts' selected. The main content area is titled 'Mail Alerts' and contains the following sections:

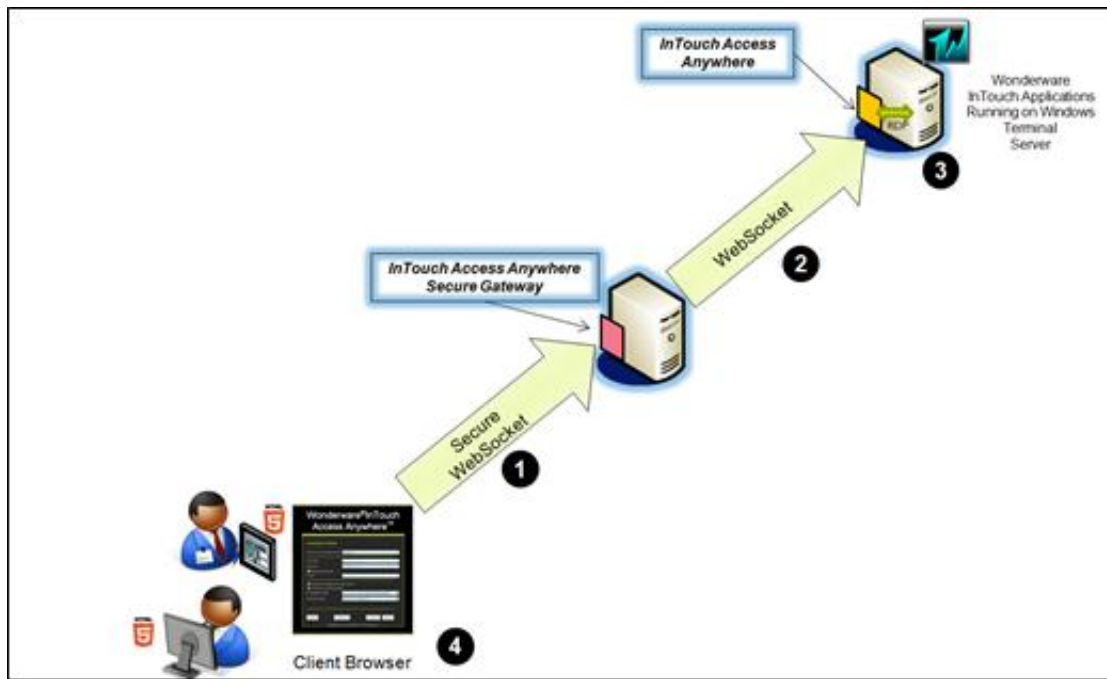
- SMTP Server Settings:** Includes fields for Address (marked with *), Port (set to 25), User Name, Password, and a 'Secured' checkbox.
- Email Settings:** Includes fields for From (marked with *), To (marked with *), and Subject Prefix (set to 'InTouch Secure Gateway mail alert:').
- Alerts:** A group of checkboxes for 'Gateway Status' (Started, Stopped, Crashed, Failed bind to port) and 'Unable to connect to:' (Host, External Web Server, VMware View Server, WebConnect Server, Authentication Server).

At the bottom of the form are three buttons: 'Save and Test Mail Settings', 'Save', and 'Cancel'.

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, a 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).

Configure the Access Anywhere Server to Work with the Secure Gateway

The InTouch Access Anywhere server includes a set of **Security** options that indicate a Secure Gateway should be used and the address of the computer hosting the Secure Gateway.

The Access Anywhere server always establishes a secure WebSocket connection to the Secure Gateway. The Secure Gateway then establishes a WebSocket connection to the Access Anywhere server.

To configure the Access Anywhere server to work with the Secure Gateway

1. Log on to the computer hosting the Access Anywhere server.
2. Show the Start page by entering the following URL in a web browser.
`https://localhost:8080`
3. Click the Advanced Settings icon  on the Start page and select the **Security** option.

The WebSocket connection between the Secure Gateway and the Access Anywhere server can be secured by selecting the **Enable SSL encryption for remote session** option.

4. Select **Use InTouch Secure Gateway** and enter the IP address or name of the server hosting the Secure Gateway in the **Gateway address** field.

The screenshot shows a configuration window titled "Security". At the top left is a back arrow, and at the top right is a close "X" button. Below the title bar, there are two checked checkboxes: "Enable SSL encryption for remote session" and "Use InTouch Secure Gateway". Underneath, there is a section labeled "Gateway Address" with a text input field containing the IP address "10.228.97.238".

Whitelist Security

You can configure two types of whitelists:

- End-user address and range
- Target host address and range

The target host whitelist is enabled by default, while the client whitelist is disabled by default. When a whitelist is enabled, a list of IP addresses must be specified.

To enable a type of whitelist, change the enabled setting from "false" to "true". For example:

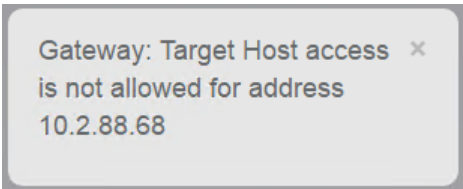
```
<add key="ClientWhitelistByIPAddressesEnabled" value="false"/>  
<add key="ClientWhitelistByIPAddressesEnabled" value="true"/>
```

Note: The enabled setting is set to "true" by default for InTouch Access Anywhere.

IP addresses are entered in the standard format, for example 10.2.88.1, and are separated by semicolons (;).

IP address ranges are defined placing the lower IP address to the left of, the character "-", and the upper IP address to the right of it. For example: 10.2.88.1-10.2.88.5

The IP addresses of each Access Anywhere Server must be configured in the EricomSecureGateway.Config file, or you will be prompted by an error message:



Note: This is an example IP address. This value will be associated with the InTouch Access Anywhere host you are trying to connect to.

The following values show an example for how each type of whitelist would be configured in the EricomSecureGateway.Config file:

- End-user Address and Range:

```
<add key="ClientWhitelistAllowedIPv4Addresses" value="10.2.88.1-10.2.88.5;10.2.88.10" />
```

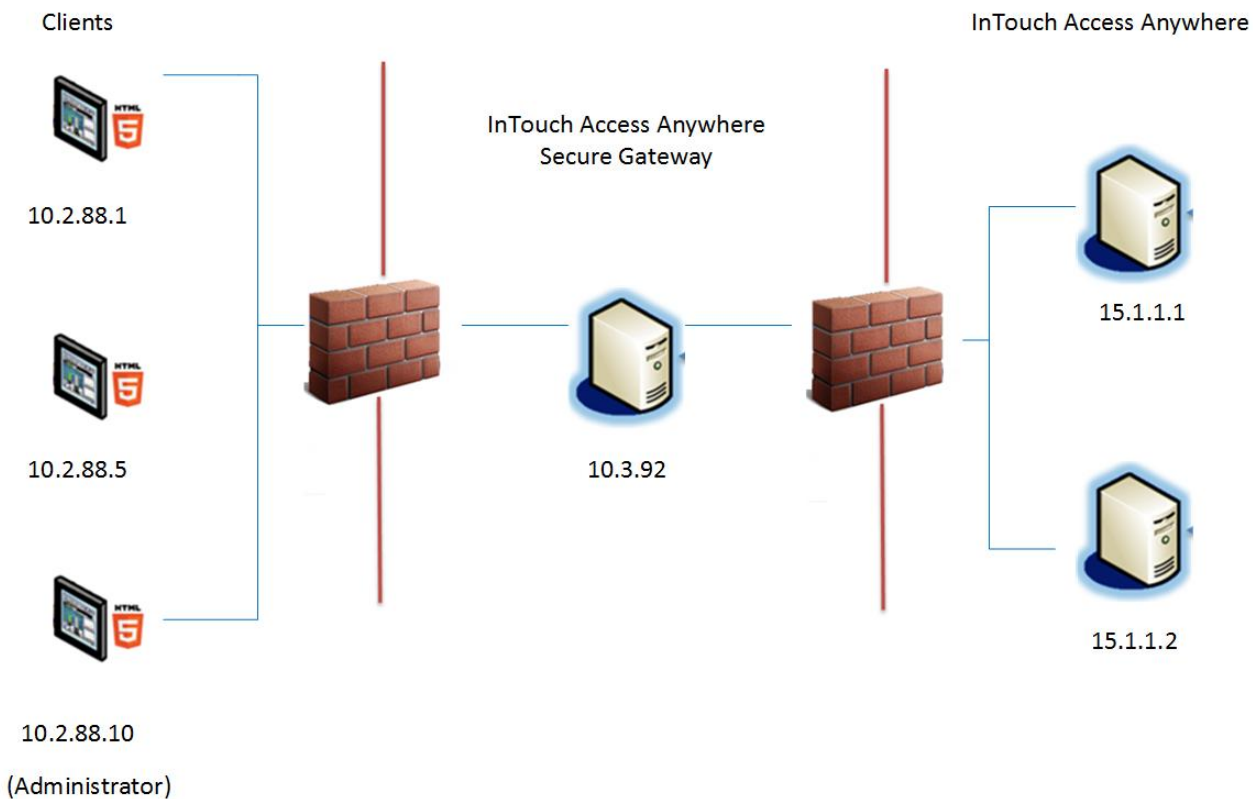
The IP Address of each client node is included.

- Target Host Address and Range

```
<add key="TargetHostWhitelistAllowedIPv4Addresses" value="15.1.1.1;15.1.1.2" />
```

The IP Address of each InTouch Access Anywhere Server(s) connecting through the Gateway.

The following diagram illustrates an example whitelist security configuration for clients, the Gateway, and the Access Anywhere Server. The IP addresses of all whitelisted clients are represented.



The list of all the configuration options is:

```

<Section name="Visitor">
  <Property name="HandshakeTimeoutSeconds" type="int" value="60" />
  <Property name="ClientWhitelistByIPAddressesEnabled" type="bool"
value="false" />
  <Property name="ClientWhitelistAllowedIPv4Addresses" type="string"
value="" />
  <Property name="ClientWhitelistAllowedIPv6Addresses" type="string"
value="" />
  <Property name="RelayServerWhitelistByIPAddressesEnabled" type="bool"
value="false" />
  <Property name="RelayServerWhitelistAllowedIPv4Addresses" type="string"
value="" />
  <Property name="RelayServerWhitelistAllowedIPv6Addresses" type="string"
value="" />
  <Property name="TargetHostRestrictedToRelayServerIPEnabled" type="bool"
value="false" />
  <Property name="TargetHostWhitelistByIPAddressesEnabled" type="bool"
value="true" />
  <Property name="TargetHostWhitelistAllowedIPv4Addresses" type="string"
value="" />
  <Property name="TargetHostWhitelistAllowedIPv6Addresses" type="string"
value="" />
  <Property name="OriginHTTPHeaderWhitelistAddresses" type="string"
value="" />
  <Property name="HostHTTPHeaderWhitelistAddresses" type="string"
value="" />
</Section>
<Section name="Admin">
  <Property name="InactivityTimeoutMinutes" type="int" value="5" />
  <Property name="WhitelistByIPAddressesEnabled" type="bool" value="true"
/>
  <Property name="WhitelistAllowedIPv4Addresses" type="string" value="" />
  <Property name="WhitelistAllowedIPv6Addresses" type="string" value="" />
</Section>

```

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.

Configuring the Origin Header Parameter for Whitelist Security

You can configure a parameter to whitelist the origin header field in incoming HTTP requests to the InTouch Access Anywhere Gateway. The Gateway will check for this parameter upon connection request to the host. If the "origin" HTTP header exists in the connection request, it will verify that it is in the list of trusted addresses. If there is no match, the Gateway will deny the connection request to the host.

Use the following parameter to whitelist the origin header field:

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

where value is the Gateway IP address or node name. For example:

```
<Property name="OriginHTTPHeaderWhitelistAddresses" type="string"
value="10.010.01.11" />
```

or

```
<Property name="OriginHTTPHeaderWhitelistAddresses" type="string"
value="ProdSGtwy" />
```

If there is a load balancer or proxy server in front of the Gateway, then the value address in this parameter refers to the load balancer or proxy server. In this case, the address can be any URL. For example:

```
<Property name="OriginHttpHeaderWhitelistAddresses" type="string" value="http://URL"/>
```

For detailed information about HTTP origin header specifications, see section 7 and 8 of the *Internet Engineering Task Force* <https://tools.ietf.org/html/rfc6454#section-7>

Configure Session Cookie Timeout

A session cookie is generated when browser clients connect to the InTouch Access Anywhere Secure Gateway.

Use the following parameter to configure the session cookie timeout in the `EricomSecureGateway.Config` file:

```
<Property name="ClientSessionCookieTimeoutMinutes" type="int" value="60" />
```

Note: The default timeout period is sixty minutes. Do not set this value to 0. A value of 0 disables the cookie timeout interval.

If you try to connect by means of a Websocket or HTTPS (if enabled) and the cookie has expired, the connection will be rejected. You will need to reload the page to re-attempt the login.

The following details apply to the session cookie lease:

- A cookie is cached in the InTouch Access Anywhere Gateway the first time an end-user's browser requests a page.
- The cookie lease duration is defined based on "ClientSessionCookieTimeoutMinutes" value.
- The lease is maintained on the Access Anywhere Server side, not in the browsers, so all browsers are treated as a single browser from your device.
- The cookie value and lease are per client (IP address), so multiple browsers on the same device will use the same cookie value and the same lease.
- The cookie lease duration is not extended each time a page is retrieved. A cookie lease expires only after the configured duration.

This cookie lease duration requires reloading the page after each expiration to contact the Gateway.

Advanced Configuration

All configurable settings related to the Secure Gateway can be found in the `EricomSecureGateway.exe.config` file. This is a text file that can be modified with a text editor. The configuration settings are also defined in the section *Built-In Authentication Server* on page 29.

Changing parameter values marked as "Reloadable" do not require a service restart. "Not Reloadable" parameters only become effective after restarting the InTouch Access Anywhere Secure Gateway service.

High Availability

To provide high availability of the Secure Gateway, 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 are redirected to an available Secure Gateway based on built-in weighting criteria. A basic round-robin load balancer can be used, but it may not detect whether a Secure Gateway is active or not.

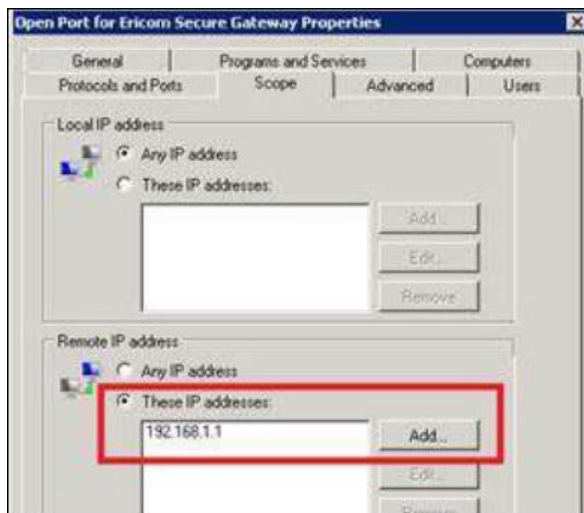
Restricting Access To and From a Secure Gateway

Use the Windows Firewall Scope rules to restrict incoming connections to the Secure Gateway server.

To restrict incoming connections to the Secure Gateway

1. Access the Port rules for Secure Gateway.
2. Click the **Scope** tab.
3. In the **Remote IP address** section, click Add.
4. Enter the IP address(es) from which you wish to allow connections.

In the example below, only connections originating from 192.168.1.1 can connect to the Secure Gateway.

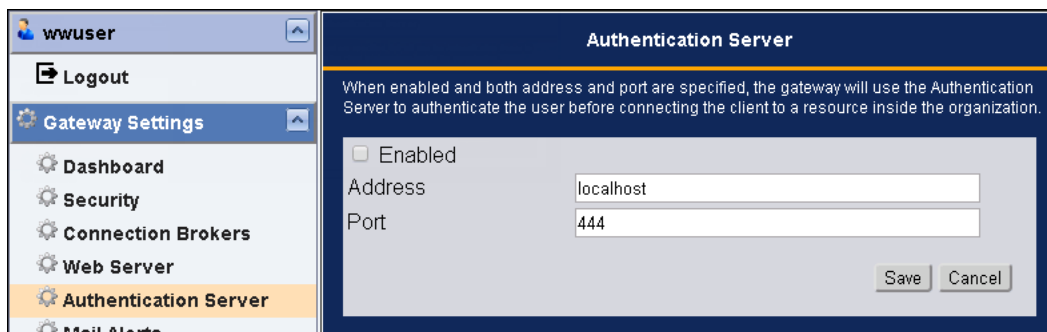


Built-In Authentication Server

The Secure Gateway includes an Authentication Server that provides a layer of security by authenticating end-users before they can access any internal resource. The Authentication Server is disabled by default and should be installed on a computer on the safe side of the firewall 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 Secure Gateway **Configuration** page to modify some of the settings of the Authentication Server:



Other configuration settings are specified in the EricomSecureGateway.Config file, which is located at

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway

The user configurable settings are located under the **Authentication Server** section of the EricomSecureGateway.Config file and defined in the following table.

Setting	Description
Enabled	Boolean value to enable the Authentication Server or not. True enables the Authentication Server. The default is False.
Address	The IP address of the computer hosting the Authentication Server. Localhost is the default.
Port	This is the port on which the Authentication Server listens. 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. The default port is 444.
CertificateDnsIdentity	The connection between the Secure Gateway and the Authentication Server is secured. In case the Authentication Server is not using its default certificate, this parameter must be updated to include the DNS identity of the alternate certificate.
MaxClockSkewMinutes	The maximum difference in minutes between the clocks of the Secure Gateway and the Authentication Server. The default is 180.
KeepAliveFreqSeconds	The keep alive interval in seconds that maintains the connection between the Authentication Server and the Secure Gateway. The default is 30.

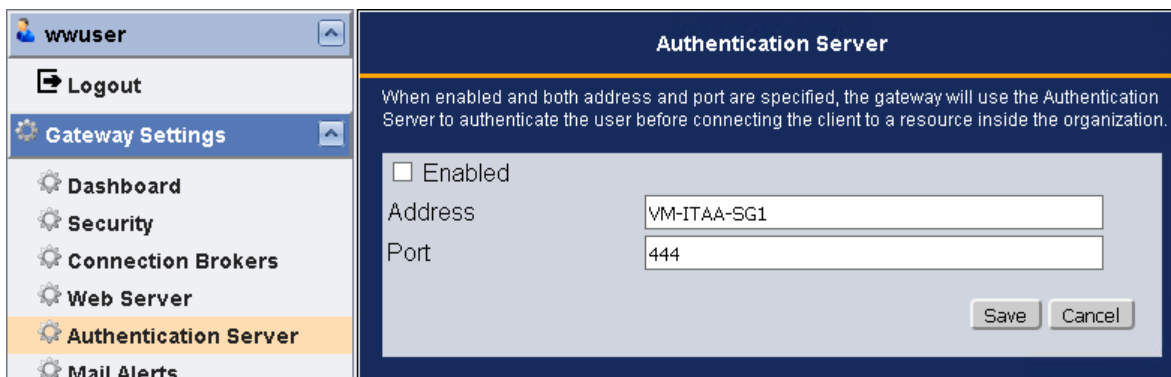
When an Authentication Server is enabled, only domain users will be able to authenticate. Local system users (such as Administrator) will not be able to log on through the Authentication Server.

Disabling Authentication Server with Brokers

When all access is through a connection broker and not from any stand-alone clients, the Authentication Server should be disabled, and the "broker only mode" enabled.

To disable the Authentication Server

1. At the **Authentication Server** page of the Secure Gateway portal, clear the **Enabled** check box to disable the Authentication Server.



2. Make the following changes to EricomSecureGateway.Config file:
 - a. Under <AuthenticationServer>, change <add key="Enabled" value="true"/> to <add key="Enabled" value="false"/>

```
<Section name="AuthenticationServer">
```

```
  <Property name="Enabled" type="bool" value="false" />
```

- b. Under <Security>, change <add key="ConnectionBrokerOnlyMode" value="false"/> to

```
<Section name="Security">
```

```
  <Property name="CertificateFindBy" type="X509FindType" value="FindByExtension" />
```

```
  <Property name="CertificateFindValue" type="string" value="1.2.840.113556.1.8000.2554.57748.52896.21682.18417.45066.8514989.679433.2" />
```

```
  <Property name="ConnectionBrokerOnlyMode" type="bool" value="true" />
```

Making these changes prevents any connections from stand-alone clients through the Secure Gateway. All users will log in only through a connection broker.

CHAPTER 5

Port and SSL Certificate

About Port and SSL Certificate

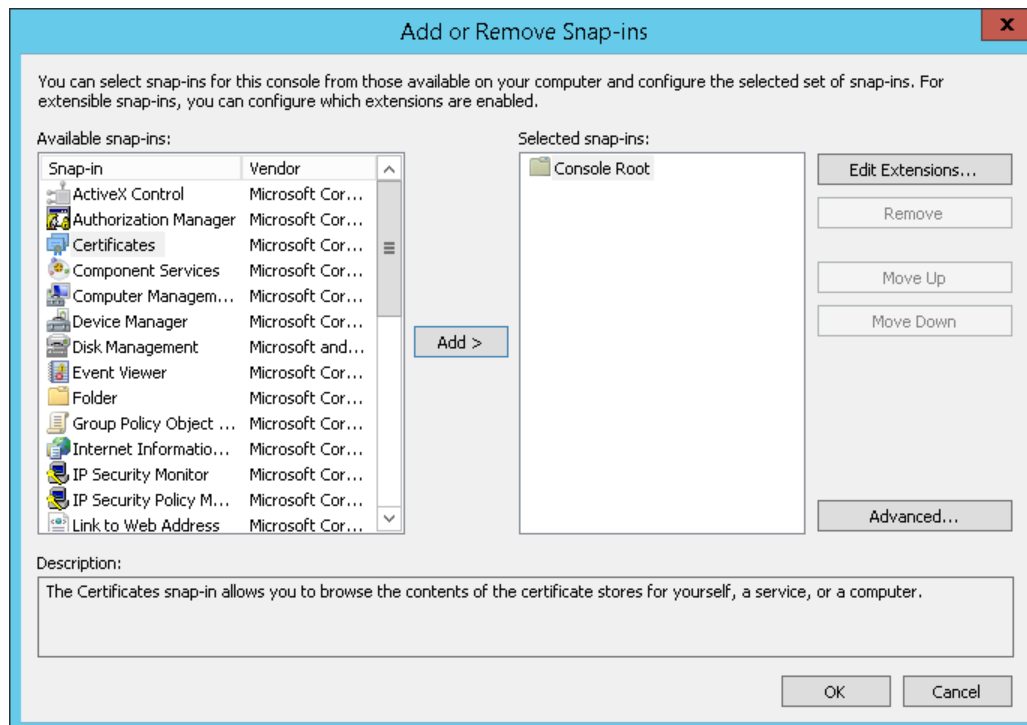
The InTouch Access Anywhere Secure Gateway includes a self-signed certificate. Some web browsers may show a security warning when a self-signed certificate is detected. To remove the warning, install a trusted certificate purchased from a trusted certificate authority (for example, VeriSign).

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), which is accessible using the Microsoft Management Console (MMC).

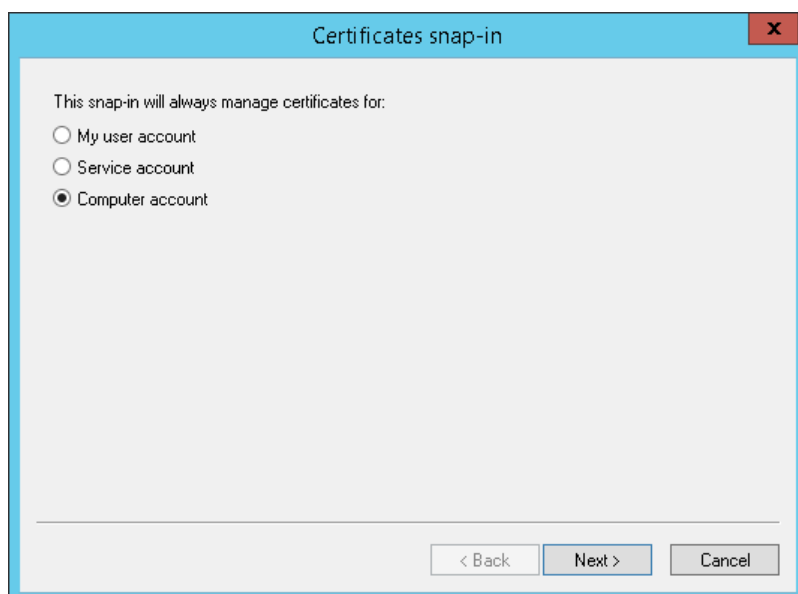
To add, view, or modify certificates

1. Log on as an administrator to the computer hosting the Secure Gateway.
2. From the Windows **Command Prompt**, run the `mmc.exe` command to show the MMC.
3. Select the **File** option from the menu bar and select **Add Remove Snap-in** to show the **Add or Remove Snap-ins** dialog box.



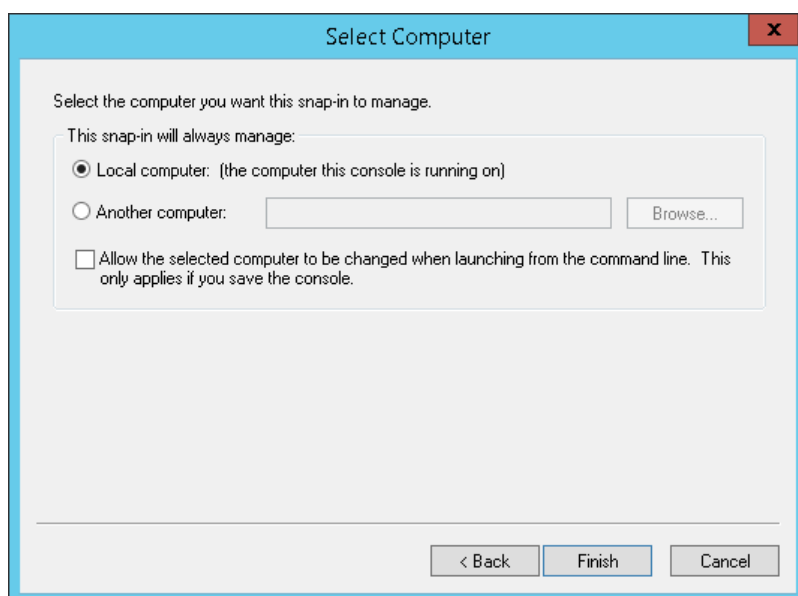
4. Select **Certificates** from the **Available snap-ins** area and select **Add**.

5. Select **Computer Account** from the **Certificates snap-in** dialog box and click **Next**.



The **Select Computer** dialog box appears with options to select a computer account.

6. Select **Local Computer**.

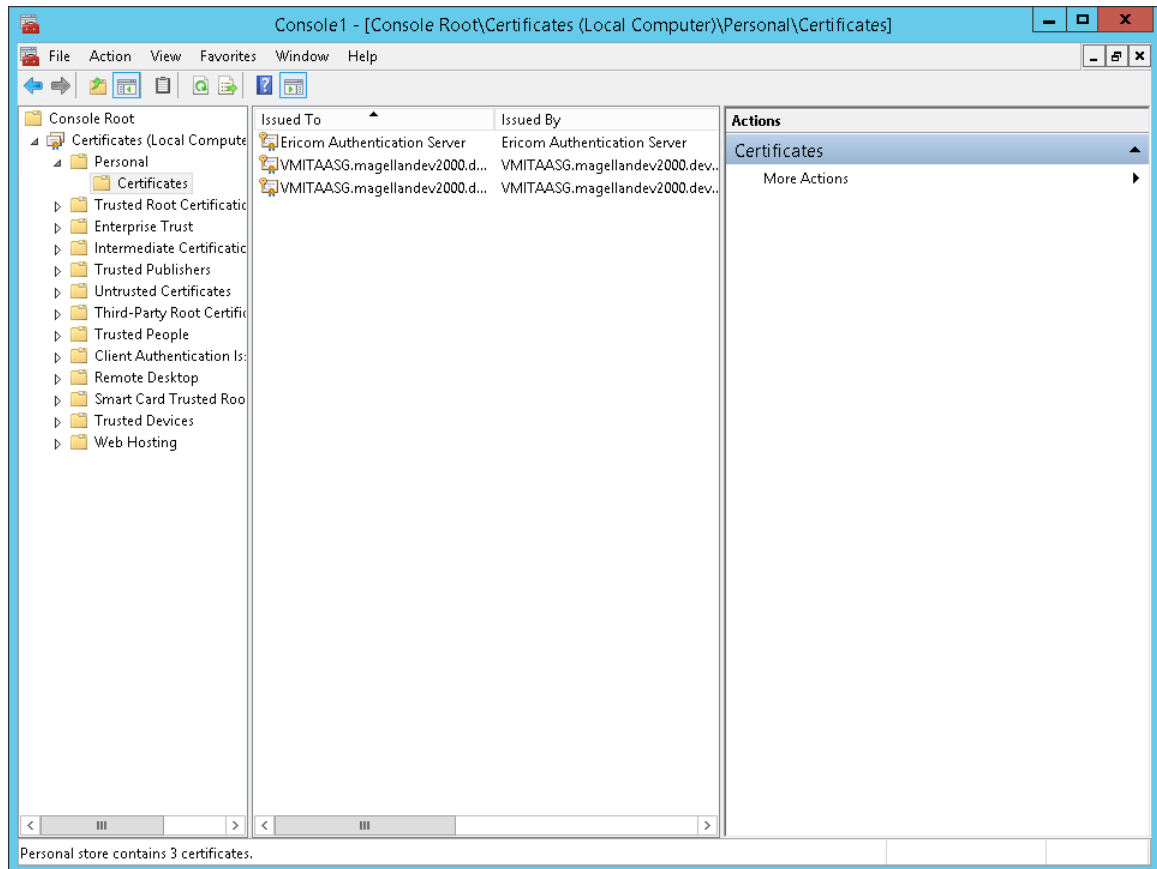


7. Click **Finish** and then **OK**.

The Console Root shows Certificates (Local Computer) option.

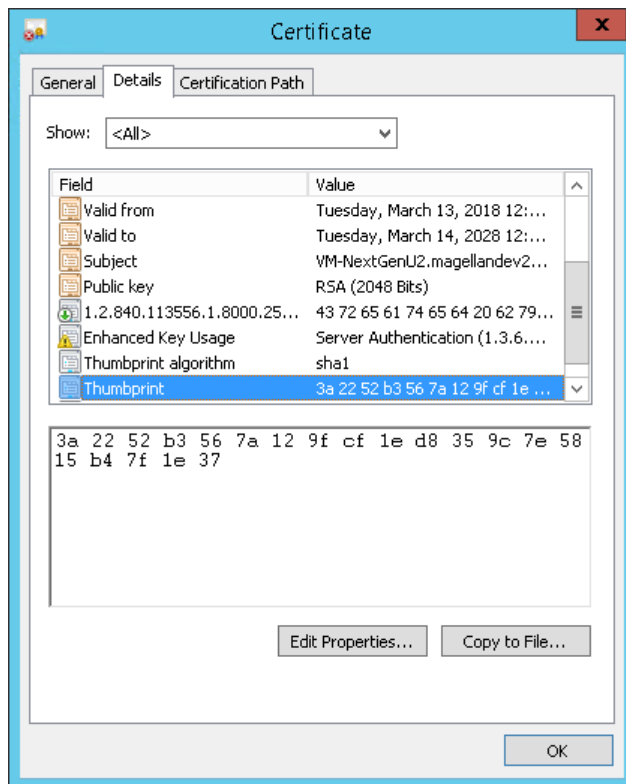
8. Select the icon to the left of the **Certificates (Local Computer)** option to expand the list of sub options.

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



10. If a trusted certificate is used with Secure Gateway, place it in the same location as the Secure Gateway **Certificates | Personal | Certificates**.
11. Browse the **Certificates | Personal | Certificates** folder of the MMC to show a list of certificates.
12. Double-click on the trusted certificate that you want to use with the Secure Gateway.
13. Select the **Details** tab and highlight **Thumbprint**.

The Thumbprint value appears beneath the list of certificate properties.



14. Select the entire thumbprint value.
15. Press CTRL+C to copy it.
The Thumbprint can also be manually typed in.
16. Click **OK** to close the dialog.
17. Open the EricomSecureGateway.Config file, which is located in the following folder of the computer hosting Secure Gateway:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Secure Gateway\InTouch Access Anywhere Secure Gateway

18. Locate the Security section of the file.

```
<Section name="Security">
    <Property name="CertificateFindBy" type="X509FindType"
value="FindByThumbprint" />
    <Property name="CertificateFindValue" type="string"
value="3A2252B3567A129FCF1ED8359C7E5815B47F1E37" />
```

19. Ensure the value of the CertificateFindBy property value is set to FindByThumbprint.
20. Delete the existing Thumbprint from the CertificateFindValue property value field.
21. Press CTRL+V to paste the new Thumbprint in the value field of the CertificateFindValue property.

All blank spaces in the thumbprint are removed after pasting it as the value of the CertificateFindValue property.

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

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.

Manually Add a Trusted Certificate

Another way to add a trusted certificate thumbprint is to dump the certificate values and copy the identify thumbprint to the EricomSecureGateway.Config file. When you are using the extension identity of a certificate, the `CertificateFindBy` property value of the EricomSecureGateway.Config file should be set to "FindByExtension".

To add a certificate thumbprint to the EricomSecureGateway.Config file

1. Place a X509 certificate at a known location of the computer running Secure Gateway.
2. Open a Command prompt window and enter the certutil command in the following form:

```
C:\Temp>certutil -dump CertificateName.cer
```

where `CertificateName` is the actual name of the certificate.

3. Find the Certificate Extensions 2 location of the output from the certutil command.

The identify string appears immediately beneath Certificate Extensions 2

```
Certificate Extensions: 2
```

```
1.2.840.113556.1.8000.2554.57748.52896.21682.18417.45066.8514989.679433.2
: Flags = 0, Length = 1a
```

4. Copy the identity string.
5. Edit the EricomSecureGateway.Config file and locate the Security section of the file.

```
<Section name="Security">
```

```
  <Property name="CertificateFindBy" type="X509FindType"
value="FindByThumbprint" />
```

```
  <Property name="CertificateFindValue" type="string" value=
```

6. Change `FindByThumbprint` to `FindByExtension` and copy the identity string as the value of the `CertificateFindBy` property.

```
<Section name="Security">
```

```
  <Property name="CertificateFindBy" type="X509FindType"
value="FindByExtension"/>
```

```
  <Property name="CertificateFindValue" type="string" value=<Certificate
Identity Thumbprint Goes Here> />
```

Example:

```
<Section name="Security">
```

```
  <Property name="CertificateFindBy" type="X509FindType"
value="FindByExtension"/>
```

```
  <Property name="CertificateFindValue" type="string"
value="1.2.840.113556.1.8000.2554.57748.52896.21682.18417.45066.8514989.6
79433.2"/>
```

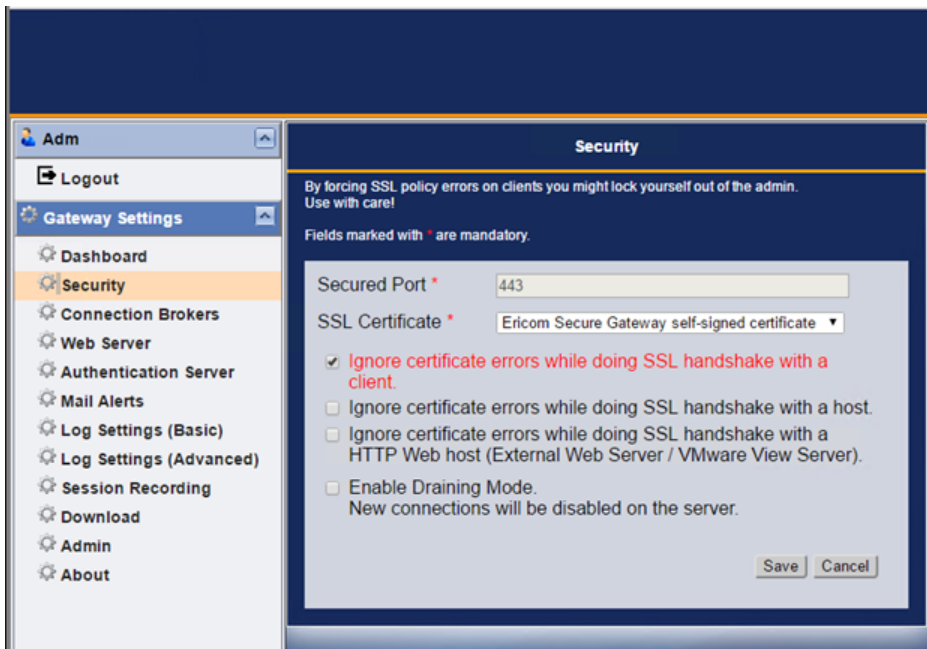
Configure the Secured Port and SSL Certificate

In the Secure Gateway Configuration dashboard, select the **Security** page to modify the port and SSL certificate that will be used by the Secure Gateway.

Note: Before configuring the port, make sure it is not currently in use. For more information, see *Resolving Secure Gateway Conflicts* on page 10.

From the **SSL Certificate** field, select the desired SSL certificate to be used by 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.

Configure the desired security options. The **Ignore certificate errors while doing SSL handshake with a client** option is selected by default.



The options are as follows:

Note: The recommended deployment method is to have none of the above options checked. The most secure method is to leave all security features enabled.

- Ignore certificate errors while doing SSL handshake with a client:** this option refers to the certificate verification between any clients connecting to the InTouch Access Anywhere Gateway.

If this option is checked, you will not be prompted with a certificate error if a connecting client's trusted certificate is not recognized on the Access Anywhere Gateway node
- Ignore certificate errors while doing SSL handshake with host:** this option refers to the certificate verification between the Access Anywhere Gateway and the Access Anywhere Server. If the Access Anywhere Server does not have a trusted certificate recognized on the Access Anywhere Gateway node, the connection will be rejected.

If this option is checked, you will not be prompted with a certificate error if the Access Anywhere Server's certificate is not recognized on the Gateway node.
- Enable Draining Mode:** this option will disable new connects being made to the Access Anywhere Server, and old connects will be closed out.

Configure Failover Gateways

Multiple Secure Gateways can be configured as a failover chain in the **InTouch Access Anywhere** web client. A failover chain provides improved reliability with redundant Secure Gateways. Alternate Gateways automatically become active when the primary Gateway is unavailable. If the connection to the first Secure Gateway on the list fails, the request is 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 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 logon time. If the primary server is unavailable, end-users will experience delays as the log on process must wait for the primary server to time out before attempting to connect to a failover server.

CHAPTER 6

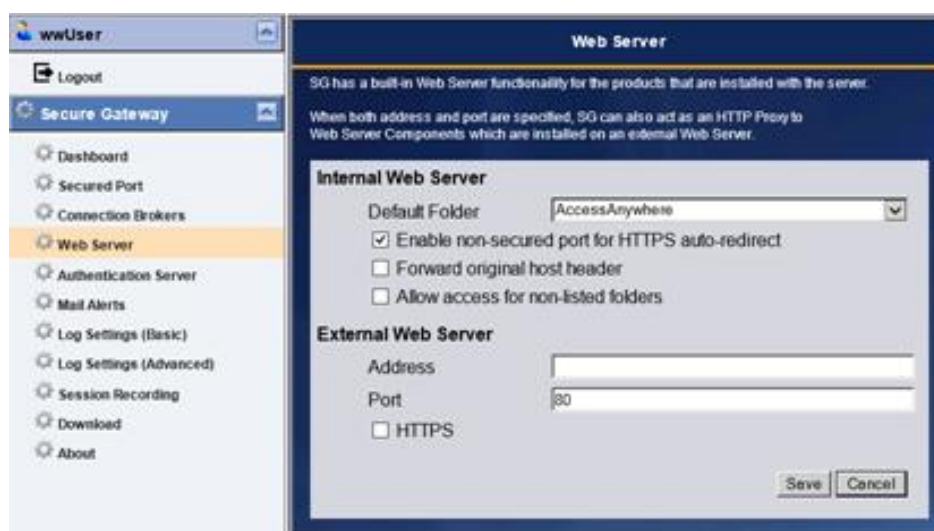
Built-In Web Server

About the Built-In Web Server

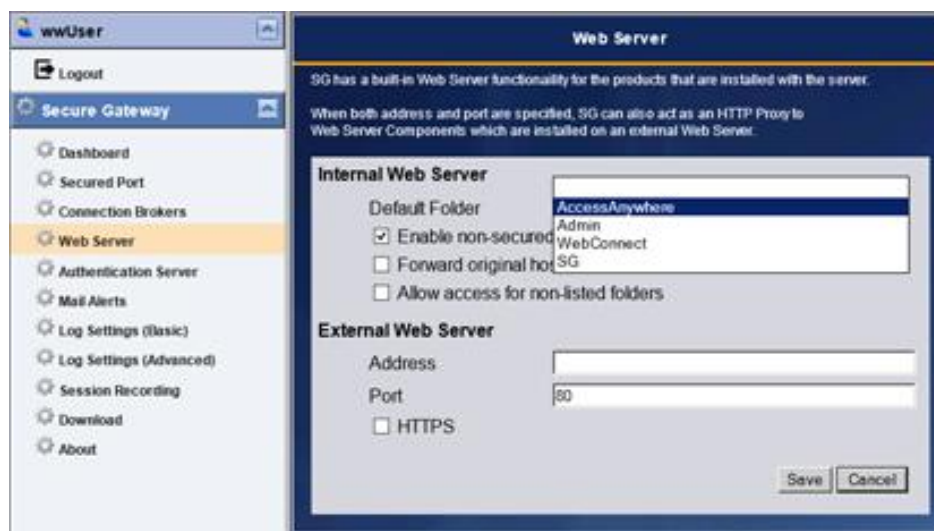
The Secure Gateway has a built-in web server to host web pages for InTouch Access Anywhere. The built-in Web server cannot be disabled and always listens on the Secure Gateway port.

To configure the Web server

1. Open the **Configuration** tool and show the **Web Server** page.



2. Click the **Default Folder** drop down list to select the default URL for the built-in web server.
3. 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 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/AccessAnywhere/start.html

The following URLs are available by default.

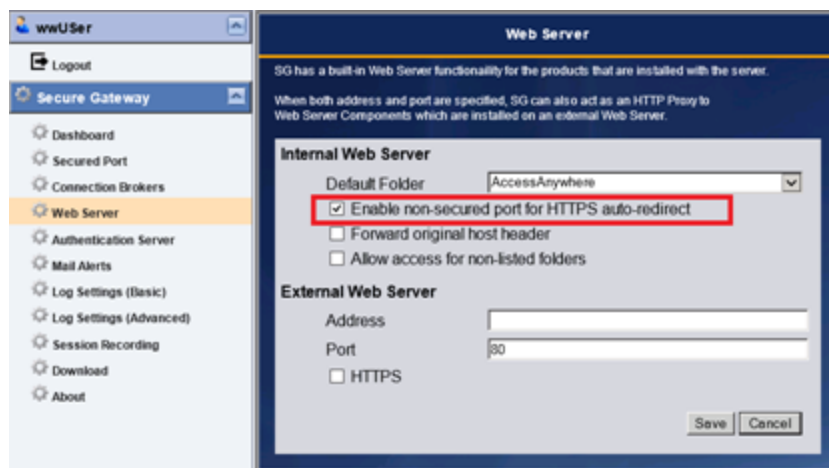
Secure Gateway Welcome Page	https://server:port/ https://server:port/welcome.html
InTouch Access Anywhere Server	https://server:port/AccessAnywhere/start.html

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 is not supported.

To enable this feature, select the option: **Enabled non-secured port for HTTPS auto-redirect** (see below).



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

Disabling HTTP/HTTPS Filtering

Certain types of network traffic are blocked by firewalls. Port 443 on most firewalls is initially reserved for HTTP (and HTTPS) based communication. Most firewalls have a rule to filter out any non-HTTP data. 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.Config file before making any changes.

To configure the settings of the built-in Web server, open the EricomSecureGateway.Config file 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	1/3/2018 7:59 PM	File folder	
 Admin	1/3/2018 7:59 PM	File folder	
 Blaze	1/3/2018 7:59 PM	File folder	
 SG	1/3/2018 7:59 PM	File folder	
 welcome.html	12/29/2017 10:50 ...	HTML File	1 KB

For example, the settings below will configure the following:

- Sets the View folder as the default folder
- Sets the view.html as the default document for the View folder
- Restricts access to any unlisted folders in the directory
- Prohibits access to the Blaze and MyCustom folders.

```
<<Section name="InternalWebServer">
  <Property name="Enabled" type="bool" value="true" />
  <Property name="ForwardOriginalHostHeader" type="bool" value="false" />
  <Property name="ForwardFaviconRequest" type="bool" value="false" />
  <Property name="XFrameOptions" type="string" value="" />
  <Property name="ContentSecurityPolicy" type="string" value="" />
  <Property name="AccessControlAllowOrigin" type="string" value="*" />
  <Property name="ClientSessionCookieTimeoutMinutes" type="int"
value="60" />
```

```
<Property name="AllowAccessForNonListedFolders" type="bool"
value="false" />
<Property name="DefaultFolder" type="string" value="AccessAnywhere" />
<Property name="FolderList" type="list (WebServerFolder)">
  <Value>AccessAnywhere,start.html,True</Value>
  <Value>Blaze,blaze.zip,True</Value>
  <Value>Admin,login.html,True</Value>
  <Value>WebConnect,start.html,True</Value>
  <Value>SG,,True</Value>
</Property>
</Section>
```

Preventing Access to Non-Listed Folders

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



Internal Web Server

Default Folder: AccessAnywhere

Enable non-secured port for HTTPS auto-redirect

Forward original host header

Allow access for non-listed folders

CHAPTER 7

Known Limitations

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

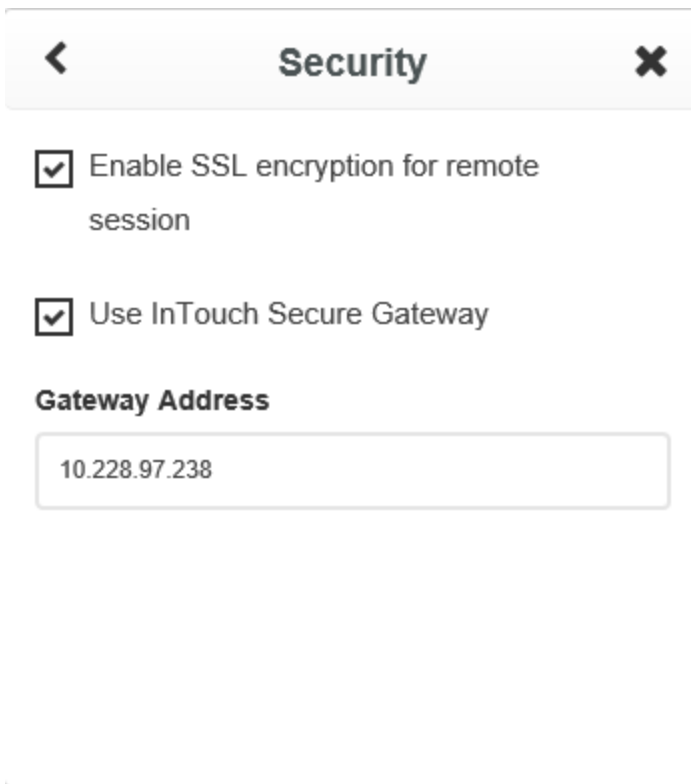
Common Error Messages

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

If you see an error message similar to 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 the 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, 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 diagnostic information saved in the log file can be set under the two log pages (Log Settings - Basic and Log Settings - Advanced).

Consult with a support engineer on which settings to enable.

