Wonderware®
InTouch Access Anywhere™ Secure Gateway
Administrator Manual
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 Schneider Electric Software, LLC. 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, Schneider Electric Software, LLC 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 Schneider Electric Software, LLC. 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.

© 2015 Schneider Electric Software, LLC. All rights reserved.

Schneider Electric Software, LLC
26561 Rancho Parkway South
Lake Forest, CA 92630 U.S.A.
(949) 727-3200

http://software.schneider-electric.com/

ArchestrA, Avantis, DYNSIM, EYESIM, Foxboro, Foxboro Evo, I/A Series, InBatch, InduSoft, IntelaTrac, InTouch, PIPEPHASE, PRO/II, PROVISION, ROMeo, Schneider Electric, SIM4ME, SimCentral, SimSci, Skelta, SmartGlance, Spiral Software, VISUAL FLARE, WindowMaker, WindowViewer, and Wonderware are trademarks of Schneider Electric SE, its subsidiaries, and affiliated companies. An extensive listing of Schneider Electric Software, LLC trademarks can be found at: http://software.schneider-electric.com/legal/trademarks/. 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
Installation Overview ............................................................ 9
Installation Prerequisites ...................................................... 10
Secure Gateway Installation .................................................. 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 Show a List of InTouch Applications ......................................................... 15

Chapter 4  Configuration Portal ................................. 17
Dashboard .............................................................................. 18
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Alerts</td>
<td>19</td>
</tr>
<tr>
<td>InTouch Access Anywhere HTML5 Client Configuration</td>
<td>19</td>
</tr>
<tr>
<td>Configuration</td>
<td>20</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>22</td>
</tr>
<tr>
<td>High Availability</td>
<td>22</td>
</tr>
<tr>
<td>SSO Form Post</td>
<td>22</td>
</tr>
<tr>
<td>Sample Page to POST Values</td>
<td>23</td>
</tr>
<tr>
<td>Sample Page to Receive POST Values</td>
<td>24</td>
</tr>
<tr>
<td>Restricting Access To and From a Secure Gateway</td>
<td>24</td>
</tr>
<tr>
<td>Built-In Authentication Server</td>
<td>26</td>
</tr>
<tr>
<td>Disabling Authentication Server with Brokers</td>
<td>27</td>
</tr>
<tr>
<td>Chapter 5 Port and SSL Certificate</td>
<td>29</td>
</tr>
<tr>
<td>Configure the Secured Port and SSL Certificate</td>
<td>31</td>
</tr>
<tr>
<td>Manually Configure a Trusted Certificate</td>
<td>32</td>
</tr>
<tr>
<td>Configure Failover Gateways</td>
<td>34</td>
</tr>
<tr>
<td>Chapter 6 Built-In Web Server</td>
<td>35</td>
</tr>
<tr>
<td>External Web Server</td>
<td>36</td>
</tr>
<tr>
<td>Connecting to the Web Server</td>
<td>37</td>
</tr>
<tr>
<td>HTTP Redirect</td>
<td>37</td>
</tr>
<tr>
<td>Disabling HTTP/HTTPS Filtering</td>
<td>38</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>38</td>
</tr>
<tr>
<td>Preventing Access to non-listed Folders</td>
<td>39</td>
</tr>
<tr>
<td>Chapter 7 Known Limitations</td>
<td>41</td>
</tr>
<tr>
<td>Common Error Messages</td>
<td>41</td>
</tr>
<tr>
<td>Obtaining Log Files</td>
<td>42</td>
</tr>
</tbody>
</table>
Use Wonderware® InTouch Access Anywhere™ Secure Gateway to access Wonderware InTouch® applications hosted on Remote Desktop Servers via HTML5-compatible web browsers.

This manual assumes the reader has 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 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.wonderware.com for more information on this and other Wonderware products.

Documentation Conventions

This documentation uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Capitals</td>
<td>Paths and file names.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Menus, commands, dialog box names, and dialog box options.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Code samples and display text.</td>
</tr>
</tbody>
</table>

Technical Support

Wonderware Technical Support offers a variety of support options to answer any questions on Wonderware 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 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 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
Secure Gateway acts as a gateway between users in remote locations and InTouch applications running in a control network. Secure Gateway can be installed in a DMZ to route traffic between an external business network and an internal HMI SCADA network.

The following diagram illustrates how a Secure Gateway uses a single port for secured remote access to InTouch applications. All web traffic from an external business network is tunneled through a SSL-based Secure Gateway connection.
Chapter 2

Installation

This chapter describes how to install the Secure Gateway. It describes installation prerequisites, a step-by-step installation procedure, 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:

![Services window]

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.

Installation Overview

- An Authentication Server is installed on the same computer as the Secure Gateway. 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 26
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 29.

Installation Prerequisites

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

- The Secure Gateway must be installed on a computer running a 64-bit version of a supported Windows server operating system. For more information, refer to the readme file.

- .NET Framework 4 Full Installation must be installed on the host computer, which can be downloaded from Microsoft's website at: http://www.microsoft.com/en-us/download/details.aspx?id=17851

- 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.
  - 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.

**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.
Secure Gateway Installation

After verifying all installation prerequisites, start the installation procedure.

**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 Wonderware InTouch Access Anywhere installation disc.

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

**Note:** You cannot install the InTouch Access Anywhere Secure Gateway on the same computer as InTouch or the InTouch Access Anywhere 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).

**Customize the installation folder**

- a) Select **Customize Installation**, and then click **Next**.
- b) Click **Browse** to select a folder or click **Make New Folder** to create a folder to install the Secure Gateway.
- c) Click **OK**.

**Select the default installation folder**

- a) Click **Next**.

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**.

---

**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 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:

![Connection Details](192.160.2.101

user2

Password

Connect

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 login 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.**

Perform the following steps to connect to the InTouch application you want to open:

1. Click the **Advanced** button. The **Advanced Settings** dialog appears.
2. Click 3 to access the third page of the settings.
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).
Configuring the Secure Gateway Node to Show a List of InTouch Applications

You can display a list of your InTouch applications on the InTouch Access Anywhere Server that can be accessed through a 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).

Scenario 2: Secure Gateway node is 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 Show a List of InTouch Applications

You can display a list of your InTouch applications on the InTouch Access Anywhere Server that can be accessed through a 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 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 Start.html and locate the following html element:

```html
<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 an IP 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 can see the Application Name list with all InTouch applications available on the InTouch Access Anywhere Server node.
Chapter 4

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 URL:

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

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

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 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.

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).

**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:

- **RDP Host**
- **Domain**
- ** ✓ Enable SSL encryption for remote session**
- ** ✓ Use InTouch Secure Gateway**
- **Gateway address:**
  - **localhost**
- ** ✓ Compression and Acceleration**
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 26.

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.

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:

![Diagram of Single Sign-on form]

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**

```html
<form name="cookieform" method="post"
action="/AccessAnywhere/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"/> -->
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

```html
<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>
```

Restricting Access To and From a Secure Gateway

Ericom documentation mentions "Terminal Servers" here too. I assumed those should be removed.

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. It is disabled by default.

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 `<External Servers Settings>` section and defined in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Boolean value to enable the Authentication Server or not. True enables the Authentication Server.</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address of the Authentication Server.</td>
</tr>
<tr>
<td>Port</td>
<td>This is the numerical value of the port over 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.</td>
</tr>
</tbody>
</table>
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 standalone clients, the Authentication Server should be disabled, and the "broker only mode" enabled.

1. At the Configuration page, clear the **Enabled** check box to disable the Authentication Server.

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

   b. Under `<Appsettings>`, change `<add key="ConnectionBrokerOnlyMode" value="false"/>` to `<add key="ConnectionBrokerOnlyMode" value="true"/>

This will prevent any connections from standalone clients through the Secure Gateway. All users will login only through a connection broker.
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. From the Windows **Command Prompt**, 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 the available certificates that can be used by the Secure Gateway.

![Image of Certificates folder]

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.


5. Delete the existing Thumbprint and press CTRL+V to paste the new Thumbprint into the file. All spaces will be ignored.

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. 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

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, open the Configuration tool and show the Web Server page.
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 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 URL’s are available by default.

|----------------------|----------------------------------------------------------|

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.exe.Config file using: `<add key="EnableNonSecuredPortForHttpsAutoRedirect" value="false" />` in the `<appSettings>` 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:

<table>
<thead>
<tr>
<th>Communication Type</th>
<th>Protocol Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Portal login</td>
<td>HTTP/HTTPS</td>
</tr>
<tr>
<td>Application Zone login</td>
<td>TCP</td>
</tr>
<tr>
<td>InTouch Access Anywhere RDP session</td>
<td>HTTPS (Secure Gateway required)</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>AccessAnywhere</td>
<td>8/7/2013 2:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Admin</td>
<td>8/7/2013 2:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>Blaze</td>
<td>8/7/2013 2:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>MyCustom</td>
<td>8/7/2013 6:20 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>8/7/2013 2:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>8/7/2013 2:25 PM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>welcome.html</td>
<td>7/25/2013 1:15 AM</td>
<td>HTML Document</td>
<td></td>
</tr>
</tbody>
</table>
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.

```xml
<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 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").
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.