Wonderware

InTouch® Access Anywhere Server Administrator Manual

10/13/14

Invensys is a Schneider Electric company.

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

http://www.wonderware.com

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

Contents

Welcome

Use InTouch® Access Anywhere™ to access Wonderware® InTouch applications hosted on Terminal Servers with HTML5 compatible web browsers. Follow the instructions in this book to begin using InTouch Access Anywhere.

This manual assumes knowledge of the following:

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

Important terminology used in this book include the following:

- RDP - Remote Desktop Protocol. A remote display protocol developed by Microsoft. RDP is a standard component of Microsoft Windows.
- RDP Host - a Windows system that can be remotely accessed using Microsoft RDP, such as a Terminal Server (RDS Session Host) or Windows workstation with remote access enabled.
- HTML5 - a new update to the HTML specification. Extends HTML with new features and functionality for communication, display, etc.
- WebSocket - a bi-directional, full-duplex communication mechanism introduced in the HTML5 specification.
- SSL - Secure Sockets Layer. A cryptographic protocol that provides communications security over the Internet.

Documentation Conventions

This documentation uses the following conventions:

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

Technical Support

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

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

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

Chapter 1

Overview

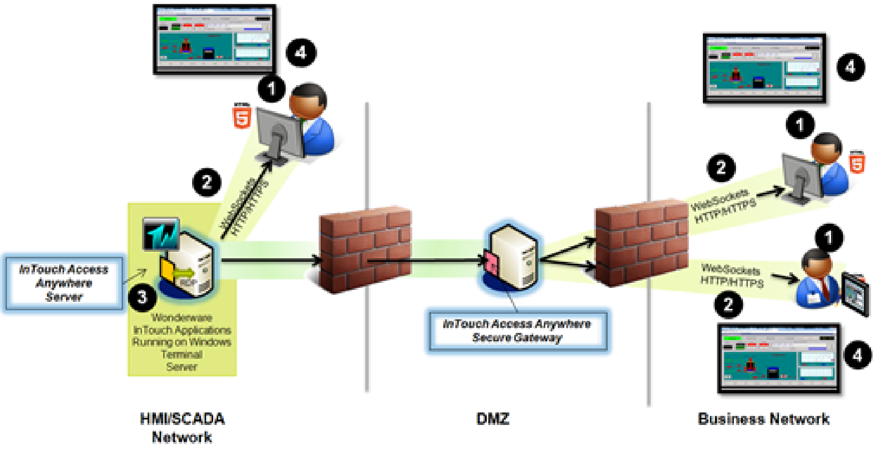
InTouch Access Anywhere provides remote access to Wonderware InTouch applications from any HTML5 compatible web browser on any device, leveraging Remote Desktop technology. Any browser that supports HTML5 canvas can be used as the client. HTML5 WebSockets are typically required for InTouch Access Anywhere.

Architecture

InTouch Access Anywhere is comprised of the following installable components:

- The **InTouch Access Anywhere Server** (WebSocket server) is installed on the RDP host where Wonderware InTouch resides. This includes a collection of web resources (HTML files, CSS, JavaScript, images, etc.).
- The **InTouch Access Anywhere Secure Gateway** is an optional component installed separately on a machine in a DMZ to enable access beyond a firewall. This is the recommended architecture when you want users on the business side of your operation to be able to access InTouch applications running on the HMI SCADA network.

The following diagram illustrates how the components of InTouch Access Anywhere work together:


4
1
2
WebSockets
HTTP/HTTPS
InTouch Access Anywhere Server
3
RDP
Wonderware InTouch Applications Running on Windows Terminal Server
InTouch Access Anywhere Secure Gateway
4
1
2
WebSockets
HTTP/HTTPS
1
WebSockets
HTTP/HTTPS
2
4
HMI/SCADA Network
DMZ
Business Network

1 Initiate an InTouch Access Anywhere connection by directing the browser to the start page hosted on the web server (http://<machinename>:8080/). The Start.html page is displayed in the web browser using HTTP/HTTPS.

2 The browser opens a WebSocket connection to the InTouch Access Anywhere Server, which is running on the RDP host itself.

Note: If the optional InTouch Access Anywhere Secure Gateway is installed, the InTouch Access Anywhere Server browser session will connect through it.

3 The InTouch Access Anywhere Server translates the WebSocket communication to and from RDP, thus establishing a connection from the browser to the RDP host itself.

4 The browser then displays the content of the remote application.

RDP Compression and Acceleration

InTouch Access Anywhere contains technology for RDP compression and acceleration, which enhances remote desktop performance over the network and Internet. There are three main features to this technology:

- Image compression

  Image compression compresses images before transmitting them to the browser for rendering. The level of compression is dependent on the acceleration/quality level selected by the user (a default value can be configured by the administrator).

- Packet shaping

  Packet shaping optimizes the network messages to improve network utilization and performance.

- Whole frame rendering

  Whole frame rendering means that the display is updated as a whole rather than in blocks, as performed by standard RDP. This is especially noticeable when watching video or over slow network connections. Coupled with the other optimization features, this results in a smoother display that more closely resembles the functionality on local desktops.

Licensing

InTouch Access Anywhere is licensed only for use with InTouch WindowViewer running under an InTouch 2012 R2 TSE Concurrent license. Per Device licenses are not supported.

There is no need to request any additional licensing or perform any activation procedures.

Every session opened with a browser using InTouch Access Anywhere consumes a remote desktop session.

Chapter 2

Installation and Configuration

This chapter describes the installation and configuration of the InTouch Access Anywhere Server. It includes he requirements that need to be met for InTouch Access Anywhere to be functional, prerequisites for installation, and detailed information of the installation and configuration process.

Before Installation

Prior to installing InTouch Access Anywhere, the following requirements must be met:

- Your Windows server operating system is supported by InTouch 2012 R2.
- Wonderware InTouch 2012 R2 has been installed.
- The corresponding TSE Concurrent license is in place.
- Remote Desktop Services have been properly configured.
- Add view.exe to the RemoteApp list and configure it to allow command-line arguments.

Because InTouch Access Anywhere leverages Remote Desktop Services, it is important that you verify that this functionality is properly configured and tested prior to installing InTouch Access Anywhere.

Note: For best display results with InTouch Access Anywhere, allow InTouch applications to be launched using their original resolution.

Tip: For more information on verifying Remote Desktop Services, see "Getting Started Quickly" on page 14, procedure 4.

Getting Started Quickly

Basic installation of InTouch Access Anywhere takes approximately five minutes and makes Wonderware InTouch applications on a Windows RDP host (server) accessible from an HTML5 compliant web browser. The InTouch Access Anywhere Server is installed with Wonderware InTouch HMI. For detailed installation instructions, see the *Wonderware System Platform Installation Guide*.

The following are steps to install and use InTouch Access Anywhere in five minutes:

1. Run the InTouch Access Anywhere Server installer.
2. Click **Next** through all the dialog boxes, accept the End User License Agreement (EULA), and then click **Finish**.
3. Configure (or disable) the Windows Firewall for use with InTouch Access Anywhere.
   a. Go to the Windows Control Panel and open Windows Firewall.
   b. Click **Allow Program or Feature**.
   c. Click **Allow another program**.
   d. Click **Browse** and navigate to <drive>:\Program Files (x86)\Wonderware\InTouch Access Anywhere\AccessNowServer32.exe.
   e. Click **Add** and then **OK**.

4 Before using InTouch Access Anywhere to connect to your TSE server, log on using a standard Remote Desktop Client, select an application from the InTouch Application Manager, and launch it in WindowViewer. This configures the initial setup and allows InTouch Access Anywhere clients to determine the list of available InTouch applications.

The InTouch Access Anywhere Server can be used immediately after installation.

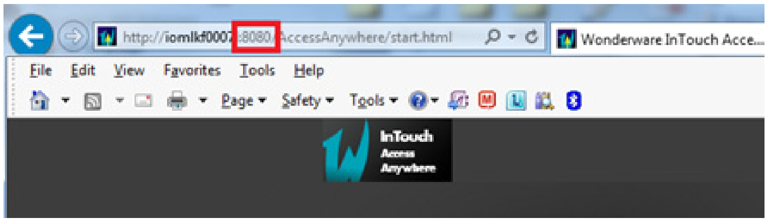
5 Open an HTML5-compliant browser and point to the URL of the InTouch Access Anywhere Server:

http://machinename:8080/

This URL automatically redirects to the full URL:

http://machinename:8080/AccessAnywhere/start.html

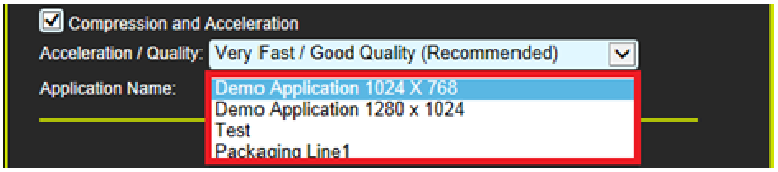
The InTouch Access Anywhere Server port must be specified in the URL to tell the browser to use the web server that is built into the InTouch Access Anywhere Server service. HTTPS may also be used.



http://iomlkf0007:8080/AccessAnywhere/start.html

6 Once the InTouch Access Anywhere Server web page appears, enter the user credentials and make your selections.

One of the choices you will be shown is the list of InTouch applications available at the host system.

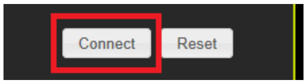


☑ Compression and Acceleration

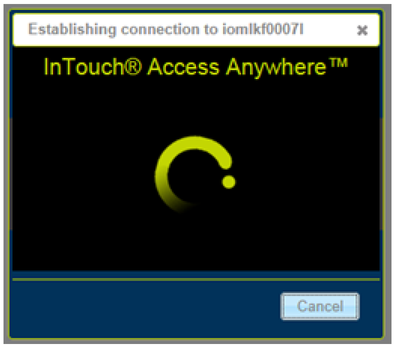
Acceleration / Quality: Very Fast / Good Quality (Recommended)

Application Name:
Demo Application 1024 X 768
Demo Application 1280 x 1024
Test
Packaging Line1

7 Once you have entered your credentials and made your selections, click the **Connect** button.



The connection dialog will appear momentarily while the web browser connects to the RDP host where the InTouch Access Anywhere Server is installed.


Establishing connection to iomlkf0007l
InTouch® Access Anywhere™
Cancel

InTouch WindowViewer will be launched at the remote node and will display the selected InTouch Application.

Note: Once connected, closing the InTouch application will log off and end the session. Closing the browser will simply disconnect from the session.

Prerequisites

The InTouch Access Anywhere Server is compatible with all released server versions of Windows supported by Wonderware InTouch 2012 R2. InTouch Access Anywhere Server must be installed on the RDP server where Wonderware InTouch 2012 R2 resides. The InTouch Access Anywhere Server should have minimum impact on the RDP host's performance and scalability.

The InTouch Access Anywhere Server itself includes a built-in web server. This includes a copy of the InTouch Access Anywhere web components.

Important: InTouch Access Anywhere leverages RDP and translates RDP to WebSockets. Therefore, RDP access must be enabled on the host that will be used with InTouch Access Anywhere.

Configure Firewalls

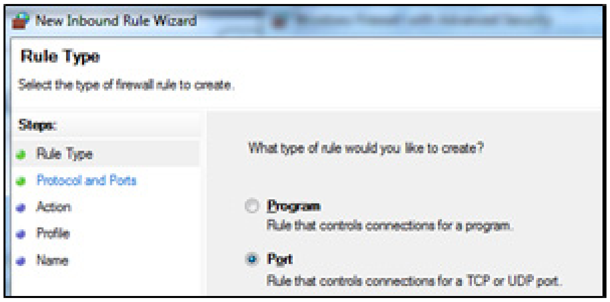
By default, the client (browser) connects to the InTouch Access Anywhere Server using port 8080 for both encrypted and unencrypted WebSocket communication. This port number can be changed using the InTouch Access Anywhere Server Configuration utility. To enable direct connection from the client to the InTouch Access Anywhere Server (without using the Secure Gateway), the server must be directly accessible from the client using that port.

If the Windows firewall is enabled on the same computer where the InTouch Access Anywhere Server is installed, make sure to configure it to enable the InTouch Access Anywhere client connection.

1 On Windows 2008 Server, go to **Control Panel** and then **Windows Firewall**.

2 Select **Advanced Settings** and select **Inbound Rules**.

3 Click **New Rule**.



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

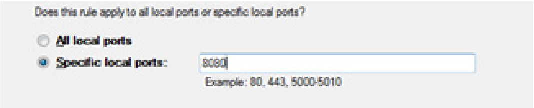
What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

● Port
Rule that controls connections for a TCP or UDP port.

4 Select **Port** and click **Next**.

5 Enter the specific port: 8080.



Does this rule apply to all local ports or specific local ports?

○ All local ports

● Specific local ports: 8080

Example: 80, 443, 5000-5010

6 Click **Next** and select **Allow the connection**.

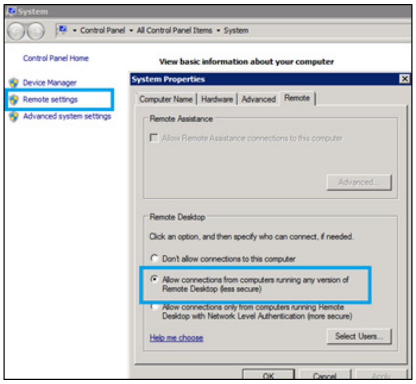
7 Click **Next** and select to apply the rule on the **Domain**, **Private**, and **Public** networks.

8 Click **Next**, assign a name for the rule, and click **Finish**.

Disable Network Level Authentication

InTouch Access Anywhere does not currently support Network Level Authentication (NLA). If this is enabled on the RDP Host, it must be disabled under the remote settings properties.

To use InTouch Access Anywhere with the RDP host, select **Allow connection from computers running any version**.



Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Bind Service to All Network Interfaces

In a virtual network environment, it is recommended to bind the InTouch Access Anywhere Server to use all virtual network interfaces, rather than just one virtual network interface controller (NIC). Network interfaces used by InTouch Access Anywhere Server must be accessible by the target group of users.

InTouch Access Anywhere Server

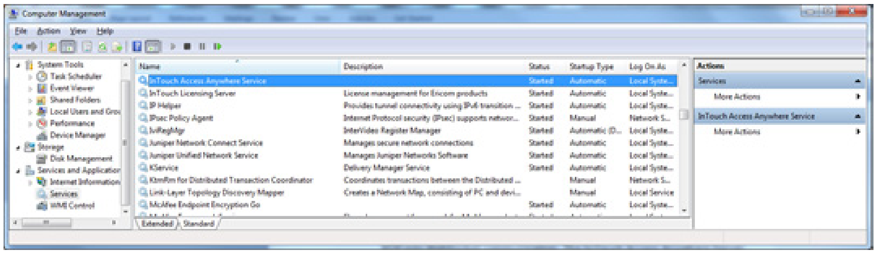
InTouch Access Anywhere Server is the server-side service that translates RDP into WebSocket communication. The InTouch Access Anywhere Server is installed on the RDP host.

The InTouch Access Anywhere client interface, running inside the browser, connects to this service using WebSockets directly or through the Secure Gateway.

Installation

Launch the install on the desired RDP host. When prompted, accept the License Agreement and then click **Install** to perform the installation. At the end of the process, click **Finish**.

The InTouch Access Anywhere Server runs as a service and can be started and stopped from the Windows Services Manager.



Name	Description	Status	Startup Type	Log On As
InTouch Access Anywhere Service		Started	Automatic	Local Syste...
InTouch Licensing Server	License management for Ericom products	Started	Automatic	Local Syste...
IP Helper	Provides tunnel connectivity using IPv6 transition ...	Started	Automatic	Local Syste...
IPsec Policy Agent	Internet Protocol security (IPsec) supports networ...	Started	Manual	Network S...
IviRegMgr	InterVideo Register Manager	Started	Automatic (D...	Local Syste...
Juniper Network Connect Service	Manages secure network connections	Started	Automatic	Local Syste...
Juniper Unified Network Service	Manages Juniper Networks Software	Started	Automatic	Local Syste...
KService	Delivery Manager Service	Started	Automatic	Local Syste...
KtmRm for Distributed Transaction Coordinator	Coordinates transactions between the Distributed ...		Manual	Network S...
Link-Layer Topology Discovery Mapper	Creates a Network Map, consisting of PC and devi...		Manual	Local Service
McAfee Endpoint Encryption Go		Started	Automatic	Local Syste...

The service is configured to run automatically on system startup. If the service is stopped or is unable to listen on its default port (8080), clients will not be able to connect to that host. Make sure to configure firewalls and proxies between the end point devices and the server-side component to allow communication using port 8080, or use the InTouch Access Anywhere Secure Gateway.

Note: InTouch Access Anywhere Server cannot be installed on systems where the host name contains non-English characters. Also, InTouch Access Anywhere Server and InTouch Access Anywhere Secure Gateway cannot be installed on the same machine.

Uninstalling InTouch Access Anywhere Server

InTouch Access Anywhere cannot be removed via the Control Panel. To uninstall InTouch Access Anywhere Server, you need to run the original install and select InTouch Access Anywhere Server to be removed.

InTouch Access Anywhere Server Configuration

The Server Configuration console presents a series of tabs that allow the administrator to configure various settings for the server service.

The Configuration console only works on systems with Microsoft Internet Explorer 7 or later.

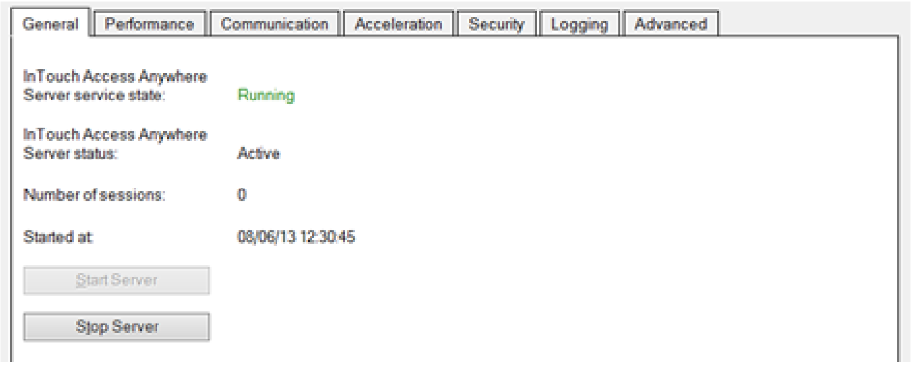
In general, changing the InTouch Access Anywhere Server configuration is not required. It is recommended to use the default settings.

Note: It is recommended to hide the Server Configuration application from end users to prevent unexpected changes to the server's settings.

The following sections describe the different tabs in the InTouch Access Anywhere Server configuration.

General

The **General** tab provides functions to start and stop the InTouch Access Anywhere Server service. For certain configuration changes, a service restart is required. This page also displays the number of active InTouch Access Anywhere Server client sessions connected to this system.



InTouch Access Anywhere Server service state: Running

InTouch Access Anywhere Server status: Active

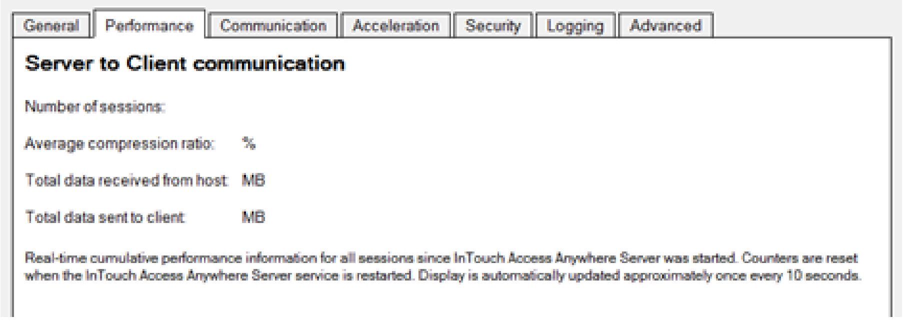
Number of sessions: 0

Started at: 08/06/13 12:30:45

Note: Whenever the InTouch Access Anywhere Server service is restarted, all sessions on the server will be disconnected.

Performance

This tab displays current performance statistics related to InTouch Access Anywhere connections.



Server to Client communication

Number of sessions:

Average compression ratio: %

Total data received from host: MB

Total data sent to client: MB

Real-time cumulative performance information for all sessions since InTouch Access Anywhere Server was started. Counters are reset when the InTouch Access Anywhere Server service is restarted. Display is automatically updated approximately once every 10 seconds.

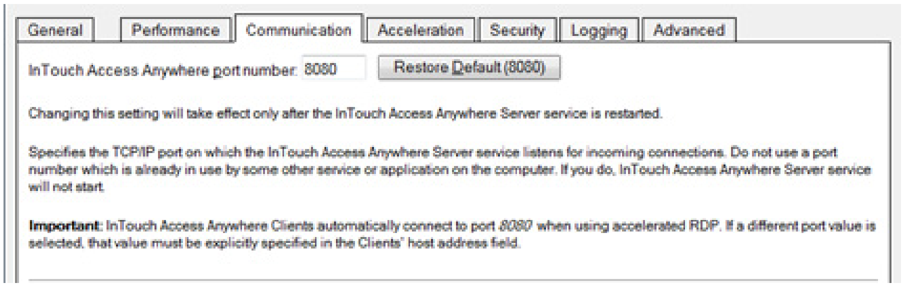
Communication

This tab provides functions to change the InTouch Access Anywhere Server listening port and the address of the host running RDP.

When using an InTouch Access Anywhere Server listening port other than the default (8080), the port number must be explicitly specified in the client address field (for example, http://<machine name>:5678/).

When running InTouch Access Anywhere Server on a machine with multiple network cards, change the RDP host address from localhost to the IP or DNS address of the network card that has RDP access to the system.

Changes to both settings require a service restart. This can be done via the **General** tab or using the Microsoft Service Manager.



InTouch Access Anywhere port number: 8080

Changing this setting will take effect only after the InTouch Access Anywhere Server service is restarted.

Specifies the TCP/IP port on which the InTouch Access Anywhere Server service listens for incoming connections. Do not use a port number which is already in use by some other service or application on the computer. If you do, InTouch Access Anywhere Server service will not start.

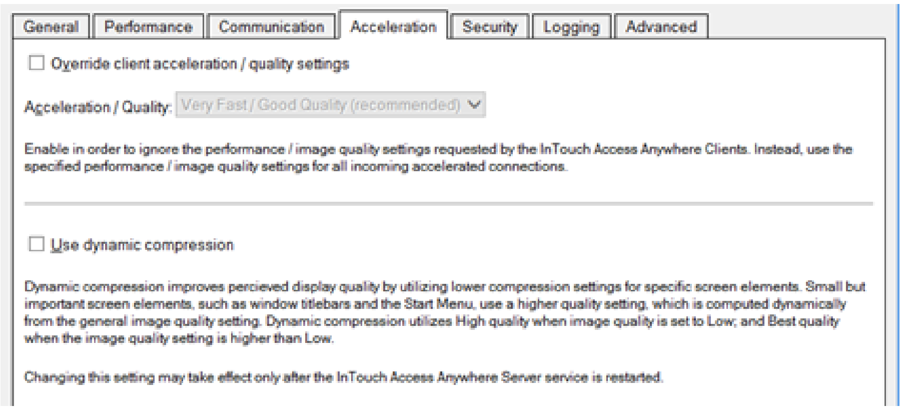
Important: InTouch Access Anywhere Clients automatically connect to port *8080* when using accelerated RDP. If a different port value is selected, that value must be explicitly specified in the Clients' host address field.

Acceleration

This tab provides functions to force the Acceleration/Quality level and disable dynamic compression. When the **Override client acceleration/quality settings** checkbox is checked, all sessions will use the configured setting, and all client settings will be ignored. When selecting or clearing this setting, the service must be restarted for the change to go into effect. When the setting is enabled, changing the acceleration level does not require a service restart, but active users must reconnect to use the new setting.

Dynamic Compression identifies small graphical objects on the screen (such as toolbar icons, taskbar icons, Start Menu icons, etc.) and compresses them. The most quality compression occurs when image quality is set to Low and the best quality compression occurs when image quality is set to higher than Low. All other graphical objects are compressed at the selected quality. This provides the visual impression of a high quality remote desktop session.

By default, this feature is enabled. To disable, clear the **Use dynamic compression** box.



□ Override client acceleration / quality settings

Acceleration / Quality: Very Fast / Good Quality (recommended)

Enable in order to ignore the performance / image quality settings requested by the InTouch Access Anywhere Clients. Instead, use the specified performance / image quality settings for all incoming accelerated connections.

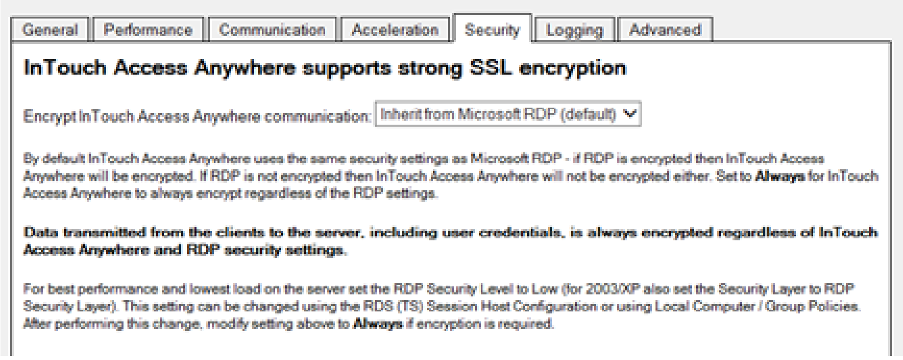
□ Use dynamic compression

Dynamic compression improves percieved display quality by utilizing lower compression settings for specific screen elements. Small but important screen elements, such as window titlebars and the Start Menu, use a higher quality setting, which is computed dynamically from the general image quality setting. Dynamic compression utilizes High quality when image quality is set to Low; and Best quality when the image quality setting is higher than Low.

Changing this setting may take effect only after the InTouch Access Anywhere Server service is restarted.

Security

This page configures the InTouch Access Anywhere Server security settings.



InTouch Access Anywhere supports strong SSL encryption

Encrypt InTouch Access Anywhere communication: Inherit from Microsoft RDP (default)

By default InTouch Access Anywhere uses the same security settings as Microsoft RDP - if RDP is encrypted then InTouch Access Anywhere will be encrypted. If RDP is not encrypted then InTouch Access Anywhere will not be encrypted either. Set to **Always** for InTouch Access Anywhere to always encrypt regardless of the RDP settings.

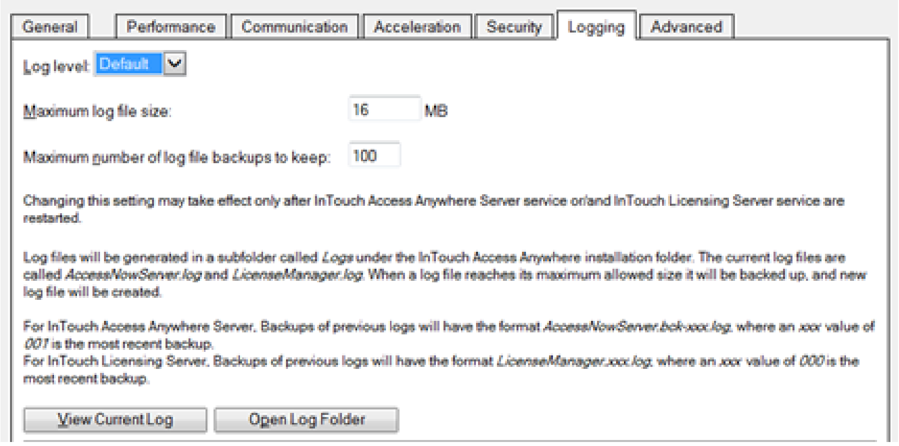
Data transmitted from the clients to the server, including user credentials, is always encrypted regardless of InTouch Access Anywhere and RDP security settings.

For best performance and lowest load on the server set the RDP Security Level to Low (for 2003/XP also set the Security Layer to RDP Security Layer). This setting can be changed using the RDS (TS) Session Host Configuration or using Local Computer / Group Policies. After performing this change, modify setting above to **Always** if encryption is required.

Note: InTouch Access Anywhere provides integrated 128-bit SSL encryption. For best performance, set the host's RDP Security Encryption level to Low and change the Encrypt InTouch Access Anywhere communication to Always. Using this configuration, InTouch Access Anywhere SSL encryption will be used instead of the RDP encryption. Do not set this if users will be connecting directly to RDP regularly, as those sessions will end up using Low encryption.

Logging

This tab provides functions to enable/disable certain logging features. Technical Support may request a debugging log for diagnostic purposes. The debugging log is enabled here.



Log level: Default

Maximum log file size: 16 MB

Maximum number of log file backups to keep: 100

Changing this setting may take effect only after InTouch Access Anywhere Server service or/and InTouch Licensing Server service are restarted.

Log files will be generated in a subfolder called *Logs* under the InTouch Access Anywhere installation folder. The current log files are called *AccessNowServer.log* and *LicenseManager.log*. When a log file reaches its maximum allowed size it will be backed up, and new log file will be created.

For InTouch Access Anywhere Server, Backups of previous logs will have the format *AccessNowServer.bck-xxx.log*, where an *xxx* value of *001* is the most recent backup.
For InTouch Licensing Server, Backups of previous logs will have the format *LicenseManager.xxx.log*, where an *xxx* value of *000* is the most recent backup.

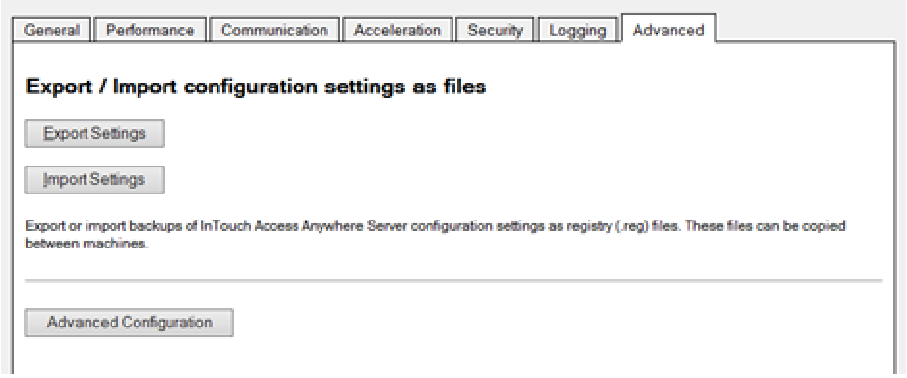
Advanced (For Administrator Use Only)

This page provides access to advanced Server settings that are stored in the system's registry.

Export Settings exports the InTouch Access Anywhere Server Registry key to the user's home folder (for example, My Documents).

Import Settings imports previously saved InTouch Access Anywhere Server Registry settings.

Advanced Configuration adds all configurable Registry key settings to the Registry. By default, only settings that are changed from the default value are saved into the Registry.



Export / Import configuration settings as files

Export or import backups of InTouch Access Anywhere Server configuration settings as registry (.reg) files. These files can be copied between machines.

InTouch Access Anywhere Web Component

The web component contains the resources that are used by the web browser to display an interface for the user to connect to their remote application or desktop. These resources include HTML pages, JavaScript and CSS files and graphic images. Review Chapter 4, "Advanced Configuration," to modify the appearance and behavior of the web component interface.

Installation with InTouch Access Anywhere Server

The InTouch Access Anywhere web components are automatically installed along with the InTouch Access Anywhere Server. The web components may be found in the InTouch Access Anywhere Server folder:

<drive letter>:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere

Modifying the InTouch Access Anywhere Interface

The InTouch Access Anywhere Server start page is comprised of a group of images. Any of the standard images may be edited and replaced with a custom image. It is recommended to keep the new image as close to the same dimensions as the original image. The following is the default logo image:

InTouch
Access
Anywhere

The path to the resources folder where the images are stored is similar to:

C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\resources

Note: Backup the resources folder before making any modifications. To roll-back to the original files, simply copy the original resources folder back to the original location.

InTouch Access Anywhere image files that are commonly customized include the following:

File Name	Description
Ericom.jpg	Logo image at the upper left-hand corner of the InTouch Access Anywhere Server landing page.
globe.jpg	Partial background image for the InTouch Access Anywhere Server landing page. This will appear as a watermark image behind the InTouch Access Anywhere Server interface.
HTML5_Logo_64.png	Small logo at the upper right-hand corner of the InTouch Access Anywhere Server landing page

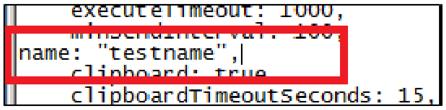
Customizations performed on the InTouch Access Anywhere page not herein described are not supported by our Technical Support, as they are beyond the scope of a standard implementation.

Modifying the Name of the Connection

The InTouch Access Anywhere connection name uses the RDP Host address by default. This label may be modified to a custom string.

To change the connection's name:

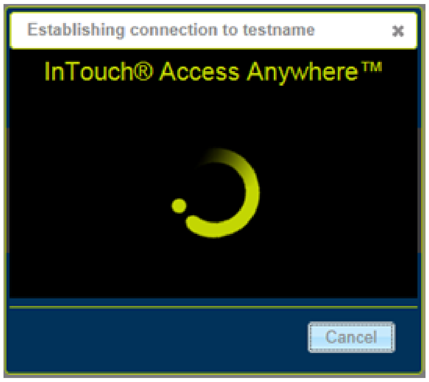
1. Open the config.js file and add the name setting if it does not exist.
2. Set the name setting to the desired string. In this example, testname will be used as the new connection name:



```
    executeTimeout: 1000,
    winSendInterval: 100,
name: "testname",
    clipboard: true
    clipboardTimeoutSeconds: 15,
```

Note: The name setting may also be set using the following cookie: EAN_name.

3 Once the name parameter is set, the new label will appear in the connection's browser tab and in the **Establishing connection** dialog box.


Establishing connection to testname
InTouch® Access Anywhere™
Cancel

Secure Connections

This section describes secure connection communication between WebSockets to both remote desktops and to the InTouch Access Anywhere Secure Gateway.

Secured WebSocket Communication to Remote Desktops

The InTouch Access Anywhere Server installation includes a self-signed certificate for secure SSL connections. Some browsers, such as Google Chrome, allow self-signed certificates for SSL-encrypted WebSocket connections.

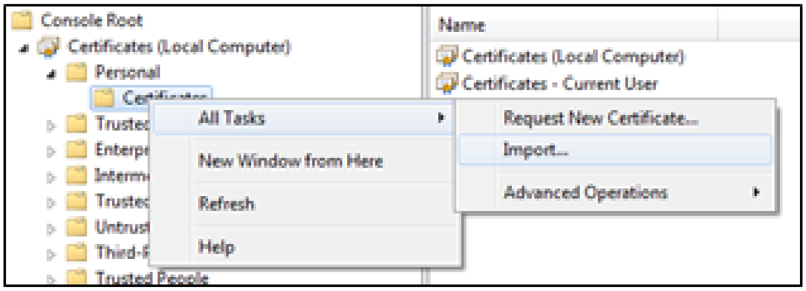
Opera browsers will notify the user that the server certificate is not signed and prompt the user to continue.

Chrome, Safari 5.x, and Firefox do not allow secure SSL connections using a self-signed certificate. In order to provide connectivity from these browsers, a trusted certificate must be imported into the InTouch Access Anywhere Server or into the InTouch Access Anywhere Secure Gateway if it is being used as a proxy for InTouch Access Anywhere Server. A trusted certificate must be purchased from a trusted certificate authority (for example, VeriSign).

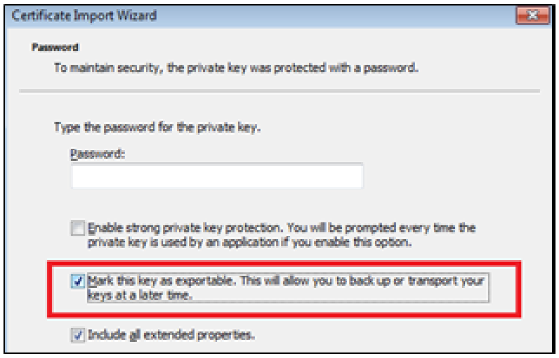
Note: The DNS address of the InTouch Access Anywhere Server or Secure Gateway server must match the certificate name. If a wildcard certificate is being used, the domain must match. For example, if the certificate is for *.acme.com, the server name must end with acme.com.

To import a trusted certificate into the InTouch Access Anywhere Server, perform the following steps using the Microsoft Certificate Manager:

1 Import the trusted certificate to the Computer (Personal | Certificates) store.



2 Mark the certificate as exportable during the import.


Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

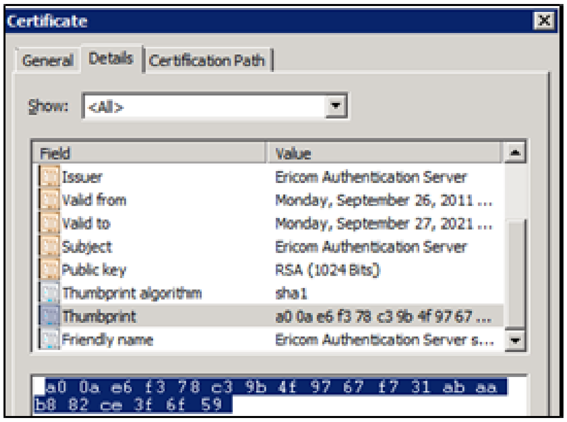
Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

3 Go to the Certificate's **Details** tab and highlight the **Thumbprint**.


Certificate

General | Details | Certification Path

Show: <All>

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

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

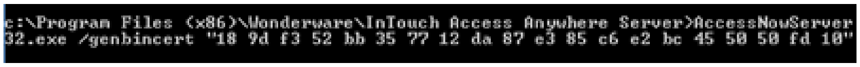
4 Copy the thumbprint (CTRL+c).

5 Stop the InTouch Access Anywhere Server service.

6 Using the Command Prompt (cmd.exe), go to the folder that contains AccessNowServer32.exe.

7 Run: AccessNowServer32.exe/genbincert <thumbprint of certificate to export enclosed in quotation marks>.

The following is an example import command with thumbprint in quotation marks:



```
c:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server>AccessNowServer
32.exe /genbincert "18 9d f3 52 bb 35 77 12 da 87 e3 85 c6 e2 bc 45 50 50 fd 10"
```

8 Once the thumbprint is properly imported, a notification will appear confirming the BIN certificate has been successfully created.

9 Start the InTouch Access Anywhere Server service and it will be ready for use.

Secured WebSocket Connection Using InTouch Access Anywhere Secure Gateway

The connection between the InTouch Access Anywhere Server browser client and the InTouch Access Anywhere Secure Gateway is always secured. The InTouch Access Anywhere Secure Gateway is installed with a self-signed certificate by default, but supports trusted certificates as well. Please refer to *InTouch Access Anywhere Secure Gateway Administrator Manual* for full instructions on how to install and configure it for use with InTouch Access Anywhere.

Benefit of Using a Trusted Certificate

Certain browsers require that HTTPS or SSL connections be made only when a trusted certificate is present. Install a trusted certificate in the InTouch Access Anywhere Secure Gateway or InTouch Access Anywhere Server to ensure safe and reliable connections from a wide range of web browsers.A trusted certificate must be purchased from a trusted certificate authority (i.e. VeriSign).

Chapter 3

Configuring Mobile and Special Devices

Google Chromebooks

InTouch Access Anywhere operates on Google Chromebook and Chromebox just like it does with a Google Chrome browser. The following are tips to keep in mind when using InTouch Access Anywhere with a Chromebook or Chromebox.

Function	How to Perform
Mouse Left-click	Click the Chromebook trackpad with one finger.
Mouse Right-click	Click the Chromebook trackpad with two fingers.
Scrolling a document or website	Drag two fingers on the Chromebook trackpad up or down to scroll.
Configure Chromebook	In the address field, enter: `chrome://settings.`

Chromebook Keyboard

The Chromebook keyboard lacks several keys that are used by Windows. ChromeOS provides standard mappings that use existing keys with the ALT button to represent certain missing keys. InTouch Access Anywhere supports these key combinations:

Command	**Key Combination**
Delete (DEL)	ALT+Backspace
Page Up	ALT+Up
Page Down	ALT+Down
Home	CTRL+ALT+Up
End	CTRL+ALT+Down

In addition, InTouch Access Anywhere provides special non-standard mappings for additional key combinations on ChromeOS.

Command	**Key Combination**
F1	CTRL+1
F2, ..., F12	CTRL+2, ..., 12
ALT+TAB	ALT+"
ALT+SHIFT+TAB	ALT+SHIFT+’
CTRL+Home	CTRL+ALT+Left
CTRL+End	CTRL+ALT+Right

Tablets and Smartphones

InTouch Access Anywhere will operate on tablets or smartphone devices with an HTML5 compliant browser (see list of browsers in *InTouch Access Anywhere Readme*). Browser versions that have been tested and their specific behaviors are detailed in the *InTouch Access Anywhere User Guide.*

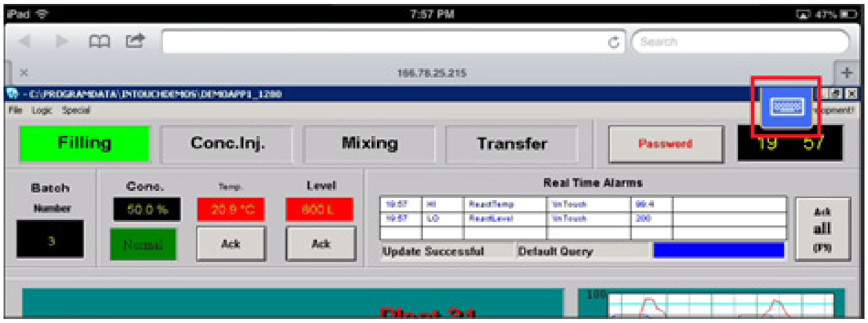
When you design InTouch applications for use with InTouch Access Anywhere, remember that touch interfaces may have different requirements and capabilities than a hardware keyboard and mouse. For example, Input animations should not need to invoke InTouch or Windows keyboard, as mobile devices have their own.

Touch gestures are used to do the work that a mouse would do in a desktop or laptop. Built-in software keyboards are used instead of physical keyboards. Because there is no mouse, certain mouse events do not have an equivalent on a touch device. Software keyboards in mobile devices do not have F1-F12, CTRL, or ALT keys. When using InTouch Access Anywhere to view your applications remotely, it is important to be aware of these differences.

With existing InTouch applications that make use of mouse events and keys or key combinations without a supported equivalent, you may want to modify your application to use alternate application events.

The following list provides tips on using InTouch Access Anywhere from a tablet or smartphone device where a physical keyboard and mouse are not available. Functionality will vary across different devices and certain commands may not be available.

- Single Tap performs a left click.
- Single long Tap performs a right-click.
- Tap + Hold + Drag performs a select then drag/scroll function.
- Double Tap, or tapping once with two fingers, performs a double-click.
- Tap with three fingers sends Back command to a remote browser.
- Swipe down with three fingers is Page Up.
- Swipe up with three fingers is Page Down.
- Drag left or right with three fingers performs a left arrow and right arrow respectively.
- Tap the keyboard icon (upper right-hand corner of window) to open/close the virtual keyboard.



- Swipe and pinch gestures will apply to the InTouch Access Anywhere session (for example, pinch in to perform a zoom in).

Note: (iOS only) When saving an InTouch Access Anywhere icon to the iOS desktop, the shortcut will open the InTouch Access Anywhere session in full-screen mode. The browser's toolbar will be hidden to make more remote desktop area available.

HTTPS Mode

For environments where WebSockets support is not available, InTouch Access Anywhere can work in HTTPS mode such that all communication will be sent via HTTPS only. HTTPS mode will only be used if WebSockets is not available. WebSockets will be used when available as it will provide better performance. HTTPS mode is required when using Microsoft Internet Explorer 9 or with SSL VPN's that only proxy HTTPS traffic.

To enable this feature, the InTouch Access Anywhere Secure Gateway is required. The InTouch Access Anywhere Server web pages must be delivered using the web server built into the InTouch Access Anywhere Secure Gateway (files are located under the Webserver/InTouch Access Anywhere folder). Perform the following to enable InTouch Access Anywhere for HTTPS support.

1. Install the InTouch Access Anywhere Server on the desired RDP Host.
2. Install the Secure Gateway in a separate machine located in a DMZ. The Secure Gateway must be installed on a server that is accessible by the target end-user group(s).
3. To connect to the InTouch Access Anywhere Server using HTTPS, enter the InTouch Access Anywhere URL of the Secure Gateway (the Secure Gateway includes the InTouch Access Anywhere web component): https://<securegatewayaddress>/InTouch Access Anywhere/start.html
4. Enter the parameters for the target InTouch Access Anywhere Server in the start.html page.
5. Upon connection, if HTTPS mode is active a '-' symbol will then be shown as a prefix to the address in the browser tab.

Note: HTTPS mode requires a browser that supports Canvas. Older browsers, such as Microsoft Internet Explorer 8 (or earlier), are not supported.

Chapter 4

Advanced Configuration

InTouch Access Anywhere easily integrates with other web pages and portals. InTouch Access Anywhere can accept configuration settings from other pages or directly from a web server. These settings can also be displayed in the InTouch Access Anywhere start page for the user to view and modify, or trigger an automatic connection.

Static Configuration of Config.js

An administrator can modify configuration settings for InTouch Access Anywhere by editing the config.js file that is installed as part of the InTouch Access Anywhere web component. This is a JavaScript file that can be modified using any text editor, such as Windows Notepad.

Important: Always backup the original config.js file before making any changes. This will ensure easy roll-back to the original configuration.

Most settings in the file have the following format:

name: value,

The value can be a number, a flag (true or false), or text enclosed in quotation marks. Some settings are prefixed by a double slash (//) which means they are disabled. Remove the double slash in order to set a value for the setting. JavaScript rules apply in this file and certain characters need to be escaped (for example, backslash). Once the settings are configured, save the file and the next user will have the new settings applied.

Refer to the Settings Table later in this chapter for a description of each setting.

Passing Credentials Using Form POST

User credentials may be passed to InTouch Access Anywhere using the form POST method. This functionality is used to provide SSO (single sign-on) from an outside source that has already authenticated the user (such as an SSL VPN).

The InTouch Access Anywhere Secure Gateway is required in order to use form POST with InTouch Access Anywhere. Please refer to *InTouch Access Anywhere Secure Gateway Administrator's Manual* for detailed instructions.

Define Configuration Groups

All users share the configuration settings defined in the config.js configuration file. It is possible to specify special settings that will override the global settings for certain groups of users. Multiple configuration groups are defined in the configuration file.

For example, if the Marketing group will have clipboard redirection and printing enabled, change config.js as follows:

```
var defaults = { / this already exists in the file

        …

        "Marketing": {// bold text are new additions

remember: false,

audiomode:0

        },

};
```

Note: The double quotation marks surrounding Marketing must be identical. It may be necessary to delete them and re-type them if the text was copied from another source. Also, the last setting of the configuration group should not have a ',' at the end. This comma will be placed after the closing bracket '}'.

In the URL to be used by the Marketing group, add the settings parameter:

http://<machine name>:8080/InTouch Access Anywhere/start.html?**settings=Marketing**

Settings Precedence

When the InTouch Access Anywhere client starts, it reads configuration information from a variety of sources. If two or more sources contain different values for the same setting, the value that InTouch Access Anywhere will use is determined by the following precedence order:

Highest Precedence to Lowest Precedence

- URL parameters
- Cookies
- Saved settings from previous session
- config.js

For example, if the gateway_address is specified to be "server1" in config.js but "server2" in a cookie (EAN_ gateway_address), then the value "server2" will be used.

If the setting override Saved is set to true in config.js, then any settings predefined in the config.js file will override previously used settings, and the precedence order will change slightly:

Highest Precedence to Lowest Precedence

- URL parameters
- Cookies
- config.js
- Saved settings from previous session

Settings Table

The config.js file contains the following configuration settings. Setting names are case sensitive. When settings are specified using cookies, their names are prefixed by EAN_.

overrideSaved	False (default) settings that the user changes are preserved between sessions and override values set in config.js. Change to true for config.js to override preserved settings.
onlyHTTPS	By default, InTouch Access Anywhere first attempts to connect using WebSockets. If the Secure Gateway is used with InTouch Access Anywhere, the connection will fall back to HTTPS when WebSockets are not available. If this setting is set to true, HTTPS is used immediately.

noHTTPS	By default, InTouch Access Anywhere first attempts to connect using WebSockets. If the Secure Gateway is used with InTouch Access Anywhere, the connection will fall back to HTTPS when WebSockets are not available. If this setting is set to true, only WebSockets will be used and HTTPS fallback will be disabled.
hidden	A comma or space-separated list of field names as they appear in config.js. For example, "username,password,domain". The listed fields will be hidden so that the user will not be able to modify them. To hide a button, such as the **Advanced** button, prefix the button text with the word `show`. For example, "`showAdvanced, showAbout`" hides both the **Advanced** and **About** buttons. All hidden variables will ignore previously saved settings.
settings (URL parameter only)	Name of the Configuration Group to be used.
wsport	The default WebSocket port that will be used by the client. The value specified in the file (8080 by default) will be used for both encrypted and unencrypted WebSocket communication. The user can override this value by explicitly specifying a port address in the client user interface (UI). For backward compatibility with older versions of InTouch Access Anywhere Server, this behavior can be modified. If singlePort is set to false, then the port value specified is only for encrypted communication. The value specified in the file plus one (8081 by default) will be used for unencrypted WebSocket communication.
gwport	The default gateway port that will be used if it is not explicitly specified in the address field.

dialogTimeoutMinutes	Timeout period, in minutes, after which an inactive dialog is automatically closed and the session is logged off. This is only relevant for dialogs that have a logoff button.
sessionTimeoutMinutes	Timeout period, in minutes, after which an inactive session is disconnected. This timeout is reset whenever the user clicks on the keyboard or a mouse button. The default value is 0, which disables this feature.
specialkeys	Enables support for special RDP key combination commands, such as CTRL+ALT+END which starts the Windows NT Security dialog box (similar to local CTRL+ALT+DEL). For the list of combination keys, see: http://support.microsoft.com/kb/186624
chromeKeys	True (default) supports special ChromeOS keys combinations.
showDownload	True displays a link in the connection dialog to download the InTouch Access Anywhere Server installer.
clipboardSupport	True (default) enables clipboard functionality; set to false to disable it.
clipboardTimeoutSeconds	The delay duration before the clipboard image automatically fades out.
clipboardUseFlash	True (default) uses Flash when available for one-click copy into local clipboard.
clipboardKey	Key to open clipboard paste dialog, set to false to disable.
console	False (default), set to true to enable RDP console mode.
settingsURL	URL of the connection settings file.

endURL	URL to open to after the InTouch Access Anywhere session has ended (# value closes window). If there is a prefix with the symbol ^ then this sets the value of window.location instead of top.location. This is useful when the InTouch Access Anywhere session is embedded in a frame.
address	Address of InTouch Access Anywhere Server. This is always blank for the standard configuration.
fulladdress	Address of RDP host. This is always blank for the standard configuration.
username	Username to pass into the InTouch Access Anywhere session.
password	Password to pass into the InTouch Access Anywhere session (entered as clear text in config.js file).
domain	Domain to pass into the InTouch Access Anywhere session.
remember	False (default) determines whether the user's password will be saved in the InTouch Access Anywhere page for future use. Set to true to enable password saving (not recommended for kiosk usage).
encryption	False determines if encryption will be enabled from the InTouch Access Anywhere client to the server.
blaze_acceleration	True determines if RDP acceleration will be used.
blaze_image_quality	Sets the quality level using a numeric. For example: 40 (fair quality), 75, 95 (best).
resolution	Sets the resolution size of the InTouch Access Anywhere session. The value set must be a valid option under the InTouch Access Anywhere screen resolution setting. For example: "1024,768". For Full Screen, use: screen.

use_gateway	False (default), set to true to use a Secure Gateway for remote access.
gateway_address	Defines the address and port of the Secure Gateway. For example: secure.acme.com:4343
useScancodes	No longer in use, see: convert_unicode_to_scancode
convert_unicode_to_scancode	False (default), set to true when using certain applications that send characters as scancodes (for example, VMware vSphere Client, or any application where you may have issues typing text). This setting will generate scancodes based on the selected locale.
leaveMessage	The message shown to the user after navigating away from an active session.
audiomode	0 enables audio redirection (default). 1 plays audio on remote computer. 2 disables audio redirection.
name	Defines a custom string for the connection name. By default, the RDP Host address is used.
minSendInterval	Specifies the minimum duration between mouse position messages sent from the client when the mouse button is pressed. Units are in milliseconds.

Note: These settings take effect only after the user starts a new session. In some cases, the local browser must be closed and reopened before changes take effect. The local browser cache may also need to be cleared.

Embedding InTouch Access Anywhere in an iframe

To embed InTouch Access Anywhere within a third-party web page using the iframe mechanism, place an iframe tag within the containing page, and have the SRC attribute of the iframe reference the InTouch Access Anywhere URL.

For example:

```
<body>
```

```
    <h1>Embedded InTouch Access Anywhere</h1>

    <iframe
src="http://127.0.0.1:8080/AccessAnywhere/start.html"
style="width:1024px; height:768px"></iframe>

</body>
```

When the InTouch Access Anywhere session ends, it can be configured to send the browser to a specified URL using the endURL setting.

- Specify a simple URL to redirect the iframe.
- Prefix the URL with ^ to redirect the iframe's parent (container).
- Prefix the URL with $ to redirect the top-most container.
- Specify # and the URL will close the browser tab.

Chapter 5

SSL VPN Configuration

InTouch Access Anywhere is compatible with most SSL VPNs. SSL VPNs that do not support WebSockets will require the Secure Gateway (SG) as well. Juniper IVE version 7.4 supports WebSockets, so the SG is not required.

InTouch Access Anywhere has been tested with Juniper's SA SSL VPNs and the documentation in this section is based on Juniper's administration pages. Configuration with other third-party SSL VPN appliances is similar to the procedures described here (differences are mostly in terminology).

Web Proxy with Juniper Version 7.4

Juniper version 7.4 natively supports WebSockets. InTouch Access Anywhere links are published in the Juniper web interface as web applications. To publish a new InTouch Access Anywhere connection, go to the Juniper Admin page and complete the following procedure:

1. Go to Resource Profiles | Web | New Web Application Resource Profile.
2. Enter the Name of the InTouch Access Anywhere connection that the users should see.
3. In the **Base URL** field, enter the InTouch Access Anywhere URL.
4. Click **Save** and **Continue**.
5. In the **Roles** dialog, add all roles that should have access to the InTouch Access Anywhere link and click **Save Changes**.
6. In the **Bookmarks** tab, enter the desired label for the connection.

7 When you log into Juniper, the InTouch Access Anywhere link will be displayed under the Web bookmarks section (for example, My Server and InTouch Access Anywhere). Click on the link to connect to an application or desktop published with InTouch Access Anywhere.

Web Proxy with Older Juniper Versions

Juniper versions prior to 7.4, and most other SSL VPNs, do not support native WebSockets. Such SSL VPNs require HTTPS Mode (see "HTTPS Mode" on page 32) to run InTouch Access Anywhere. HTTPS mode is enabled by installing the Secure Gateway.

To use InTouch Access Anywhere and the Secure Gateway

1 Go to Resource Profiles | Web | New Web Application Resource Profile.

2 Enter the Name of the InTouch Access Anywhere connection that the users should see.

3 Enter the Gateway's InTouch Access Anywhere URL address as the Base URL.

4 Click **Save**.

5 Go to Autopolicy: Web Access Control.

6 Edit the automatically entered address and delete the subfolder "InTouch Access Anywhere".

Instead of https://GWaddress.com:443/InTouch Access Anywhere/*, the correct resource is https://GWaddress.com:443/*.

7 Click **Save** and **Continue.**

8 At the **Roles** dialog, add all roles that should have access to the InTouch Access Anywhere link and click **Save Changes**.

9 When you log into Juniper, the InTouch Access Anywhere link will be displayed under the Web bookmarks section (for example, InTouch Access Anywhere Connection to RDP Host). Simply click on the link to connect to an application or desktop published with InTouch Access Anywhere.

Note: If the link is not translating properly, make sure that there is not a Passthrough Proxy policy defined for the Gateway Server (where the web component is hosted on).

Single Sign-on (SSO) Using Cookies

In the Single Sign-on Config, set "Remote SSO".

Set "Send the following data as request headers" to the InTouch Access Anywhere URL.

Set the desired cookies, for example:

- EAN_username=<USER> (this passes the username)
- EAN_password=<PASSWORD> (this passes the password)
- EAN_autostart=true (this auto starts the connection, "bypassing" the start page)

Note: Other InTouch Access Anywhere parameters may also be passed as cookies

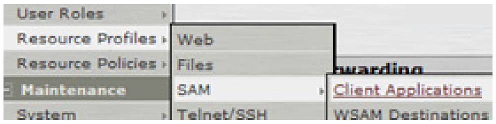
Network Connect

Juniper's Network Connect mode opens a VPN tunnel to the private network. When using Network Connect, simply enter the InTouch Access Anywhere parameters as if they were on the private network.

JSAM and WSAM

The Java and Windows Secure Access Manager provide additional security by limiting access on the private network to only the assigned resources. The InTouch Access Anywhere parameters will be masked by Juniper and will not be directly accessible by the end user. To configure InTouch Access Anywhere for JSAM, go to the Juniper Admin page and do the following (WSAM configuration is similar to the JSAM procedure below):

1 Publish a JSAM Client Application Profile by going to Resource Profiles | SAM | Client Applications.



2 Click **New Profile** and enter the parameters:

- **Type**: JSAM
- **Application**: Custom
- **Name**: Enter desired label here
- **Servers Name**: <enter address of InTouch Access Anywhere Server>

- **Server Port**: <enter InTouch Access Anywhere port # (default is 8080)>
- **Client Loopback IP**: Juniper's aliased address for the InTouch Access Anywhere Server

Important: This address must be entered as the InTouch Access Anywhere address for Juniper users.

- **Client Port**: Juniper's aliased port for the InTouch Access Anywhere Server

Important: This port must be entered as the InTouch Access Anywhere port for Juniper users. The default port 8080 may be used here if it does not create a port conflict.

3 Click **Save** and **Continue**.

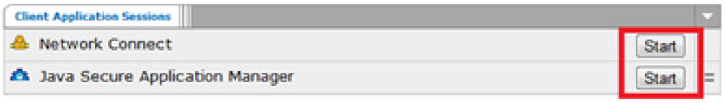
4 Select the Roles that will have access to this JSAM application.

5 Click **Save Changes**.

The application is ready for use.

Auto-starting JSAM and WSAM Upon Login

You may have to manually start a Client Application Session upon login:



Network Connect — Start

Java Secure Application Manager — Start

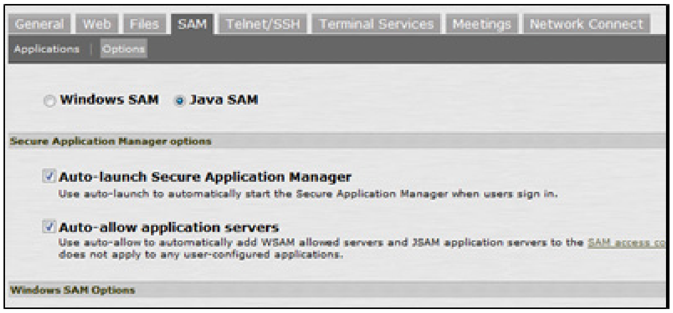
To have the JSAM or WSAM applet launch on login to Juniper, go to the Juniper **Admin** page and do the following:

1 Click on User Roles | <select desired Role> | General.

2 Verify that the **Secure Application Manager** is checked.

3 Click **Options**.

4 Check the **Auto-launch Secure Application Manager** option:



○ Windows SAM ● Java SAM

Secure Application Manager options

☑ Auto-launch Secure Application Manager
Use auto-launch to automatically start the Secure Application Manager when users sign in.

☑ Auto-allow application servers
Use auto-allow to automatically add WSAM allowed servers and JSAM application servers to the SAM access co
does not apply to any user-configured applications.

Windows SAM Options

5 Click **Save Changes** and the next time a user logs in the SAM will automatically start.

Chapter 6

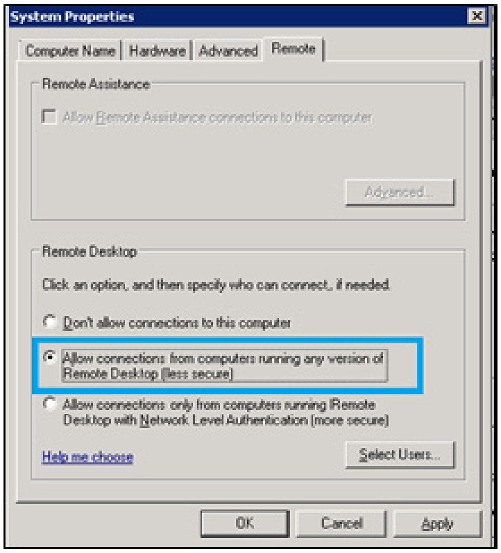
Known Limitations

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

Networking Limitations

- InTouch Access Anywhere does not support NLA

  InTouch Access Anywhere currently does not support Network Level Authentication (NLA). Disable NLA to ensure optimum connection performance for InTouch Access Anywhere.



System Properties

Remote Assistance

☐ Allow Remote Assistance connections to this computer

Remote Desktop

Click an option, and then specify who can connect, if needed.

○ Don't allow connections to this computer

● Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

- Network Quality

  The quality of the network will impact the client end, particularly with mobile devices. Long latencies, limited bandwidth, and poor Wi-Fi coverage of the working area will all have an impact on user experience.

  We recommend that in the menu of your application you add a heartbeat or a clock that displays time, including seconds, that helps visualize good connectivity.

- WindowMaker Not Supported with InTouch Access Anywhere

  InTouch WindowMaker is not supported in a TSE (Remote Desktop) environment. Therefore, InTouch Access Anywhere is not supported for use with InTouch WindowMaker. To prevent users from attempting to start WindowMaker from WindowViewer, do not install a license that enables WindowMaker and hide the menu bar in your InTouch applications.

Browser Limitations

- Browser Extension Conflicts

  Browser extensions and tool bars may inject JavaScript code into web pages, which can adversely impact the behavior of certain web pages. If InTouch Access Anywhere is not working properly, try disabling or uninstalling any active browser extensions or tool bars. Restart the web browser after uninstalling or disabling an extension to ensure that it is no longer active.

- HTTPS and SSL Encryption

  When the InTouch Access Anywhere page is delivered to the web browser using HTTPS, the SSL encryption setting will be checked by default. Modern browsers usually require WebSocket connections to be encrypted when launched from pages that are delivered using HTTPS.

Navigational Limitations

- Mouse Events

  When designing your applications, keep in mind that certain mouse events do not have an equivalent in a touch environment in most mobile devices, including the following:

  - While Left Key Down
  - On Right Key Down
  - While Right Key Down

    - On Right Double Click
    - On Right Up
    - Mouse Center click

    Other mouse events are triggered with a gesture you must become familiar with. For example, in many mobile devices, a mouse over event is triggered by a tap on the screen.

- Right Click on Mac

  To perform a right-click on Mac OSX system: Command+ left-click.

- Scroll Bars

  In some cases, moving a scroll bar in a touch environment may be difficult, particularly when the device has a small screen. As an alternative, try touching the empty area of a scroll bar in the direction you want to move.

- Dialog Boxes

  Dragging and dropping a dialog box can also be difficult in a touch environment with a small area. We recommend that you use a stylus to perform these operations for better precision, if possible.

- Using Software Keyboards

  InTouch provides the ability to invoke an InTouch keyboard or the Windows On Screen Keyboard from Input Animations. When designing applications to be accessed via InTouch Access Anywhere from mobile devices, keep in mind that these devices have their own software keyboards optimized for their specific form and size. In these cases, invoking the InTouch or the Windows keyboards from your application is not needed. In general, you will have a smoother experience using the software keyboard built into the device.

  Also, keep in mind that software keyboards in mobile devices in most cases do not have certain keys available in a physical keyboard, such as F1-F12, CTRL, or ALT. If you already have an application that uses Key Scripts associated with some of these keys, you can change your application to use alternate available, supported keys.

  Some key combinations may not be available through your mobile device, such as Shift+<letter>, CTRL+Shift, CTRL+ALT.