

AVEVA™
InTouch Access Anywhere Server
Administrator Manual



AVEVA

© 2020 AVEVA Group plc and its subsidiaries. All rights reserved.

No part of this documentation shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of AVEVA. No liability is assumed with respect to the use of the information contained herein.

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

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

Publication date: Thursday, November 19, 2020

Contact Information

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

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

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

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

Contents

Welcome	5
Documentation Conventions	5
Technical Support	5
Chapter 1 Overview	7
Overview Architecture	7
RDP Compression and Acceleration	8
Licensing	8
Chapter 2 Installation and Configuration.....	9
Pre-Installation Requirements	9
Important.....	9
Requirements	9
Adding WindowViewer to the RemoteApp List	10
In Windows Server 2012 / Server 2012 R2 / Server 2016 and Server 2019	10
Scaling Applications for Different Devices (Recommended)	12
Bind Service to All Network Interfaces	14
Verifying the Current Network Interface Configuration.....	14
Install Access Anywhere Server	14
Install All Components on a Single Server.....	15
Verify the Installation	15
Installation	18
Updating InTouch Access Anywhere Server.....	18
Uninstalling InTouch Access Anywhere Server.....	18
Configure InTouch Access Anywhere Server	19
Configure the Firewall for InTouch Access Anywhere	19
Configuring a Firewall Port Exception.....	19
Configuring a Firewall Program Exception	20
Using the Server Configuration Console	23
General.....	24
Performance	24
Communication	24
Acceleration	24
Security	24
Logging.....	25
Advanced (For Administrator Use Only)	25
InTouch Access Anywhere Web Component	25
Installation with InTouch Access Anywhere Server	25
Modifying the InTouch Access Anywhere Interface	25
Modifying the Name of the Connection	26
Secure Connections	26

Secured WebSocket Communication to Remote Desktops	26
Secured WebSocket Connection Using InTouch Access Anywhere Secure Gateway	28
Benefit of Using a Trusted Certificate.....	28
Configuring Mobile and Special Devices	29
Supported Browsers	29
HTTPS Mode.....	29
Forcing HTTPS Mode	30
Advanced Configuration.....	31
Modifying the InTouch Access Anywhere Interface	31
Adding Languages to the Display Languages Settings Page	31
Static Configuration of the Config.js File	31
Define Configuration Groups	34
Settings Precedence	34
SSO Form Post.....	35
Modify the SSO Path.....	38
Embedding InTouch Access Anywhere in an iframe	38
Hiding InTouch Applications from InTouch Access Anywhere.....	38
Adding Custom Application Screen Resolutions	39
Configure Gestures for Touch Devices	40
Activation Criteria.....	40
Toolbar button	40
Multi-touch Gesture Redirection Settings in the Config.js File.....	40
Conflict with Local Gesture Usage.....	41
Known Limitations	43
Networking Limitations	43
Browser Limitations.....	43
Navigational Limitations.....	43
NAD Limitations	44

Welcome

Use AVEVA InTouch Access Anywhere™ to access InTouch applications hosted on Remote Desktop 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:

- InTouch
- Enabling and configuring Remote Desktop Services (RDS) on Windows operating systems
- Firewall configuration
- Web server administration

Important terminology used in this book includes 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 Remote Desktop Server (RDS Session Host) or Windows workstation with remote access enabled.
- RDS - Remote Desktop Services, which includes the Remote Desktop Protocol (RDP).
- 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

Technical Support offers a variety of support options to answer any questions on 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:

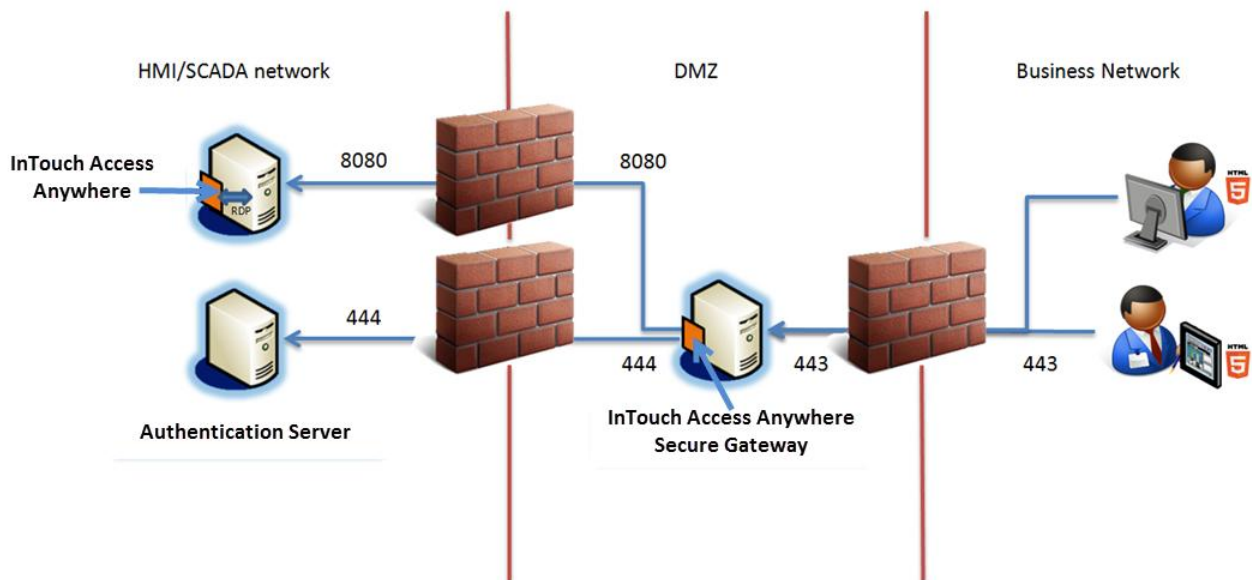
- The type and version of the operating system you are using.
- The type and version of browser you are using.
- Details of how to recreate the problem.
- The exact wording of the error messages you saw.
- Any relevant output listing from the Log Viewer or any other diagnostic applications.
- Details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

CHAPTER 1

Overview

Architecture

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



- The InTouch Access Anywhere server (WebSocket server) is installed on the same Remote Desktop Services host where InTouch WindowViewer runs applications. The server includes a collection of web resources (HTML files, CSS, JavaScript, images, etc.).
- The Authentication Server is installed on the safe side of the firewall and authenticates InTouch Access Anywhere users before granting them access to InTouch applications.
- The InTouch Access Anywhere Secure Gateway is an optional server installed separately on a computer in a DMZ to access InTouch applications protected by a firewall.

Note: You can use a VPN connection instead of InTouch Access Anywhere Secure Gateway.

This is the recommended architecture to remotely access InTouch applications running on an HMI SCADA network from an untrusted business network.

The following sequence of events occur after the user enters the URL to remotely view a running InTouch application.

1. Initiate a connection from the client device by directing the browser to the InTouch Access Anywhere 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 RDS host itself.

Note: If the optional InTouch Access Anywhere Secure Gateway is installed, an 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 RDS host itself.
4. The browser then displays the content of the remote InTouch application.

RDP Compression and Acceleration

InTouch Access Anywhere provides RDP compression and acceleration technology to improve remote client performance over a network. There are three main features of RDP technology:

- **Image compression**
Images are compressed before transmitting them to a browser for rendering. The level of compression is dependent on the selected acceleration/quality option (a default value can be configured by the administrator).
- **Packet shaping**
Packet shaping is a computer network traffic management technique that delays some or all datagrams to reduce latency and increase usable network bandwidth.
- **Whole frame rendering**
Whole frame rendering updates the display as a whole rather than in blocks, as performed by standard RDP. The benefit of whole frame rendering is especially noticeable when watching video over slow network connections. Coupled with the other optimization features, whole frame rendering results in a smoother video display on a browser.

Licensing

InTouch Access Anywhere is licensed for use only with InTouch WindowViewer running under an activated InTouch 2012 R2 TSE (RDS) or newer license.

When InTouch is launched by InTouch Access Anywhere, this RDS license will be consumed per browser session. It will be released when InTouch is closed by InTouch Access Anywhere.

Per device licenses are not supported.

CHAPTER 2

Installation and Configuration

This chapter describes how to install and configure InTouch Access Anywhere Server. It includes requirements that need to be met for InTouch Access Anywhere to be functional, prerequisites for installation, and detailed information about the installation and configuration procedures.

Pre-Installation Requirements

Important

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

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

Requirements

Before installing the InTouch Access Anywhere server, verify the following requirements have been met:

- The computer that will host the InTouch Access Anywhere server must be running a 64-bit version of the following:
 - Windows 2012 Data Center
 - Windows 2012 R2 Data Center and Standard
 - Windows 2016 Data Center and Standard
 - Windows Server 2019 LTSC Data Center - Desktop Experience, IoT - Desktop Experience, Standard - Desktop Experience

Note: Embedded operating systems are not supported by InTouch Access Anywhere Server.

- .NET Framework 4.6.2 Full Installation or later must be installed on the host computer if you are completing a stand-alone installation of InTouch Access Anywhere.

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

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

HKLM\SOFTWARE\Microsoft\.NETFramework

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

- InTouch applications must be built with version 10.6 or later to be viewed through InTouch Access Anywhere

- The InTouch Access Anywhere server must be installed on the same computer that hosts InTouch WindowViewer.
- Remote Desktop Services must be configured on the host computer.

Important: InTouch Access Anywhere leverages RDP and translates RDP to WebSockets. RDS access must be enabled on the computer hosting InTouch Access Anywhere.

- Make sure the anticipated users of InTouch Access Anywhere are members of the Remote Desktop Users group to be granted the right to log on to the Access Anywhere server remotely.
- The host computer's firewall is configured to permit inbound and outbound network traffic on port 8080.

Make sure no other application installed on the InTouch Access Anywhere server also uses port 8080.

- On host computers running Windows Server 2012, the InTouch WindowViewer executable file (view.exe) must be added to the host computer's RemoteApp list and configured to support command-line arguments.
- The corresponding TSE (RDS) Concurrent license is activated on the host computer.
- If upgrading to a newer version of InTouch Access Anywhere, first back up any custom components of the existing installation, then uninstall the existing version before installing the new version.
- InTouch Access Anywhere Server cannot be installed on computers in which the host name contains non-English characters.
- InTouch applications cannot be listed by InTouch Access Anywhere if application names or folder paths contain an ampersand (&) character.

Adding WindowViewer to the RemoteApp List

In order to make WindowViewer accessible remotely, the Windows RDS RemoteApps role should be enabled before installing the InTouch Access Anywhere server.

In Windows Server 2012 / Server 2012 R2 / Server 2016 and Server 2019

Important: This configuration requires Active Directory (2008 R2 or newer), and the server configured as follows must be joined to the AD domain.

To install the prerequisites

1. Open the **Server Manager** to the **Dashboard**.
2. In the **Manage** menu at the top right, select **Add Roles and Features**. The **Add Roles and Features Wizard** opens to the **Before You Begin** page.
3. Click **Next**. The **Installation Type** page appears.
4. Select **Role-based or feature-based installation** and click **Next**. The **Server Selection** page appears.
5. Select your server from the provided list and click **Next**. The **Server Roles** page appears.
6. Select **Remote Desktop Services** from the list.
7. Click **Next**. The **Features** page appears.
8. Expand the **Remote Server Administration Tools** feature group, and the **Role Administration Tools** group beneath it.
9. Under the **Remote Desktop Services Tools** list, select the following features:

- **Remote Desktop Gateway Tools**
 - **Remote Desktop Licensing Diagnoser Tools**
 - **Remote Desktop Licensing Tools**
10. Click **Next** . The **Add Roles and Features Wizard** appears.
 11. Click **Add Features** twice to reach the **Role Services** page under **Remote Access**.
 12. Select the **DirectAccess and VPN (RAS)** option and click **Next** twice to reach the **Role Services** page under **Remote Desktop Services**.
 13. Select the following features:
 - **Remote Desktop Connection Broker**
 - **Remote Desktop Gateway**
 - Upon selection, the **Add Roles and Features Wizard** will appear. Click **Add Features**.
 - **Remote Desktop Licensing**
 - **Remote Desktop Session Host**
 - Upon selection, the **Add Roles and Features Wizard** will appear. Click **Add Features**.
 - **Remote Desktop Web Access**
 - Upon selection, the **Add Roles and Features Wizard** will appear. Click **Add Features**.
 14. Click **Next** twice to reach the **Role Services** page under **Network Policy and Access Services**.
 15. Select the **Network Policy Server** service, and click **Next**. The **Confirmation** page appears.
 16. Click **Install**, and proceed as instructed to complete installation of the prerequisites.

Important: If and when prompted, make sure to restart the server to finish installation.

To configure and deploy the server

1. Open the **Server Manager**.
2. From the **Manage** menu, click **Add Roles and Features**. The **Add Roles and Features Wizard** opens to the **Before You Begin** page.
3. Click **Next**. The **Installation Type** page opens.
4. Select **Remote Desktop Services installation**, and click **Next**.
5. On the **Deployment Type** page, select **Quick Start**, and click **Next**.
6. On the **Deployment Scenario** page, select **Session Virtualization** (Windows 2012) or **Session-based desktop deployment** (Windows 2012 R2 and 2016), and click **Next**.
7. On the **Select server** page, if your server appears in the **Selected** list, click **Next**. If it does not:
 - a. Select the desired server's listing in the **Server Pool** list.
 - b. Click the right arrow between the lists to add your server to the **Selected** list
 - c. Click **Next**.
8. On the **Confirmation** page, select the **Restart the destination server automatically if required** option, and then click **Deploy**. Progress meters appear as the wizard proceeds through configuration steps.
9. Following configuration, the Server Manager displays the **Completion** page to indicate configuration success.

To configure Collections

1. From the Server Manager, click the **Remote Desktop Services** page, then click **Collections**. The Collection of remotely available applications created by the Quick Start Deployment Scenario appears. If you wish to remove the default Collection, continue with the next step. Otherwise, go to Step 3.
2. Right-click the **QuickSessioncollection** listing, click **Remove Collection**, and then click **Yes** to dismiss the confirmation prompt.
3. From the **TASKS** drop-down list near the top right of the Server Manager, click **Create Session Collection**. The **Create Collection** window opens to the **Before You Begin** page.
4. Click **Next** to proceed to the **Collection Name** page.
5. Enter a Name to identify this Collection in the **Name** text field. You may also enter a **Description** in the provided text field if you wish. When finished, click **Next**.
6. On the **RD Session Host** page, select your server from the **Server Pool** list, and click the right arrow to add it to the **Selected** list. When finished, click **Next**.
7. On the **User Groups** page, Domain Users are given access to the Collection by default. If you need to add other User Groups, you may click the **Add...** button and select them. When finished, click **Next**.
8. On the **User Profile Disks** page, you may configure a storage location for user settings. This tutorial will skip this step, so clear the **Enable user profile disks** check box, and click **Next** to continue.
9. On the **Confirmation** page, click **Create**. Progress indicators appear.
10. When the progress indicators advance to completion and all steps show a **Status** of *Succeeded*, click **Close**.

To publish the RemoteApp

1. From the **Remote Desktop Services** page of the Server Manager, select the Collection you just created in the **Overview** section.
2. From the **TASKS** drop-down list under the **REMOTEAPP PROGRAMS** section, click **Publish RemoteApp Programs**. The **Publish RemoteApp Programs** window appears.
3. Find the **WindowViewer** listing, and select it by checking its box.

Note: If the **WindowViewer** listing is not present in the list, click **Add Another Program...** and navigate to `view.exe` in the directory to which InTouch was installed.

4. With **WindowViewer** selected in the list, click **Next**.
5. From the **Confirmation** screen, click **Publish**. A progress indicator appears briefly.
6. The **Completion** screen appears, indicating that **WindowViewer** is now *Published*. Click **Close**.
7. Return to the Server Manager. Under the **REMOTEAPP PROGRAMS** section, right-click the **WindowViewer** entry and click **Edit Properties**. The **Properties** window for **WindowViewer** appears.
8. Click the **Parameters** entry at the left of the **Properties** window.
9. Under **Command-line Parameters**, select the **Allow any command-line parameters** option, click **OK**.

Scaling Applications for Different Devices (Recommended)

Users may view applications remotely with InTouch Access Anywhere on a variety of desktop monitors, tablets, or mobile phones. Each monitor or mobile device has a unique native screen resolution making it difficult to view an InTouch application developed at a single resolution.

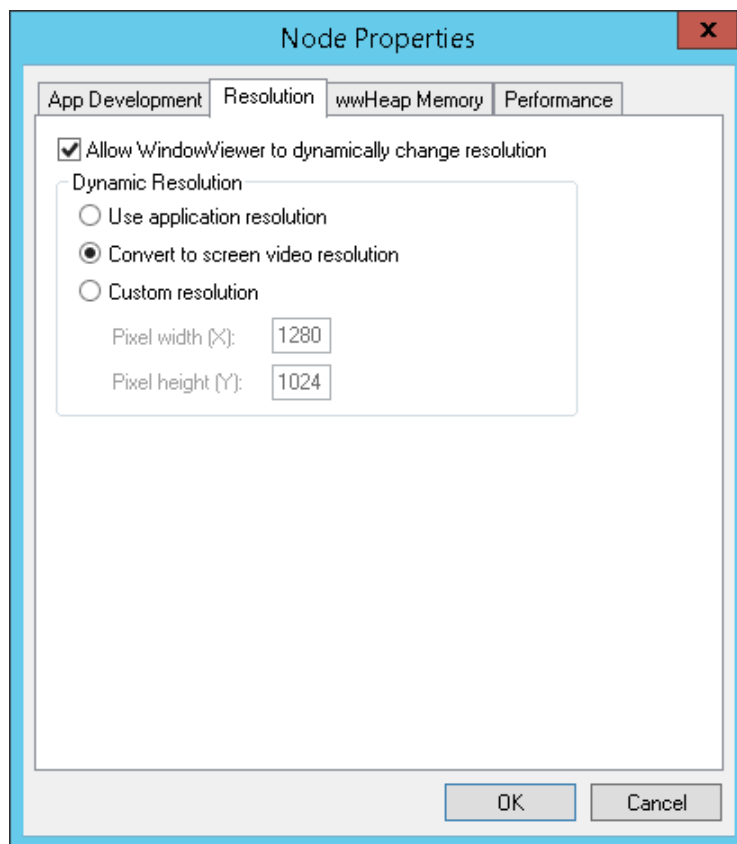
InTouch provides Dynamic Resolution Conversion (DRC) to enable InTouch distributed applications to run on different devices at their native screen resolutions. Each device can scale the application appropriately, including scaling to a custom resolution. Application scaling occurs while WindowViewer compiles the application and does not require WindowMaker.

Dynamic Resolution Conversion must be enabled for the InTouch Access Anywhere **Fit to Browser** or **Fit to Screen** display options to work correctly. See the *InTouch Access Anywhere User Guide* for details on display options and other Advanced Settings.

Important: You are strongly advised to run WindowViewer with DRC enabled and select the **Convert to screen video resolution** option.

To configure DRC for InTouch Access Anywhere applications

1. Log on to the RDS host computer as an InTouch administrator.
2. Start InTouch **Application Manager**.
3. On the **Tools** menu, click **Node Properties**. The Node Properties dialog box appears.
4. Click the **Resolution** tab.



5. Select the **Allow WindowViewer to dynamically change resolution** option to locally scale the application for different device screens.
6. In the **Dynamic Resolution** area, select **Convert to screen video resolution**.

The **Convert to screen video resolution** enables WindowViewer to run the application at the remote device's resolution. For example, if a mobile phone has an 800x600 screen and the InTouch application was developed at 1280x1024, WindowViewer dynamically scales the application to fit the phone's 800x600 resolution.

7. Click **OK** to dismiss the configuration windows.

To enable DRC for users

1. Log on to the RDS host computer as an InTouch administrator.
2. Open the win.ini file of the InTouch user who completed the previous steps (located at "Users\- 3. Add the section [InTouch] (if necessary).
- 4. Add the line ViewApplicationResolution=2 under the [InTouch] section.
- 5. Save the file.
- 6. Copy this file to the AppData folder corresponding to each user who will use InTouch Access Anywhere with DRC enabled.

Bind Service to All Network Interfaces

In a virtual network environment, InTouch Access Anywhere Server should 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 to the target group of users.

Verifying the Current Network Interface Configuration

As a quick test of your current network configuration, run PowerShell 3.0 and enter the following command:

```
RESOLVE-DNSNAME dnsname
```

The Resolve-DnsName cmdlet performs a query by DNS name for the computer's corresponding IP4 and IP6 addresses.

Example:

```
PS C:\Users\user1> resolve-dnsname itaaprd1
```

Name	Type	TTL	Section	IPAddress
-----	----	---	-----	-----
itaaprd1.Prodn_01.Prd.acmeware	AAAA	1200	Question	
fe80::b19c:7e4c:f07a:e7e2				
.com				
itaaprd1.Prodn_01.Prd.acmeware	A	1200	Question	10.101.01.111
.com				

Install Access Anywhere Server

A basic installation of InTouch Access Anywhere usually takes about five minutes. Make sure that all installation prerequisites have been met before starting the installation procedure. The following procedure explains the basic steps to install the InTouch Access Anywhere server on a computer running a supported version of Windows Server.

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

Before placing InTouch Access Anywhere into a secure, production environment, you may want to do some internal testing. *Install All Components on a Single Server* on page 15 describes an alternative installation method to place the InTouch Access Anywhere server, the Secure Gateway, and the Authentication server on a single server computer.

To install InTouch Access Anywhere server

1. Log on to the computer hosting the InTouch Access Anywhere server as an administrator.

2. Locate the Setup.exe file on your InTouch Access Anywhere installation media.
3. Double-click on Setup.exe to start the InTouch Access Anywhere Server installer.
The installation wizard shows a list of all InTouch Access Anywhere components that can be selected to be installed.
4. Select **InTouch Access Anywhere Server**, and click **Next**.
5. Click **Next** on the dialog box that shows InTouch Access Anywhere server will be installed.
6. Select the check box that acknowledges you have read and accepted the terms of the license agreement and select **Agree**.
7. Click **Install** to begin installing InTouch Access Anywhere server.
A horizontal bar shows the progress of the installation.
8. Click **Finish** to complete the installation.
9. Configure (or disable) the Windows Firewall for use with InTouch Access Anywhere. For details, see *Configuring a Firewall Program Exception* on page 20.

Install All Components on a Single Server

All InTouch Access Anywhere server components can be installed on a single computer running a supported version of Windows server. The Secure Gateway, the Authentication server, and the InTouch Access Anywhere server can be installed simultaneously.

Note: Make sure that WindowViewer is installed on the server before starting the procedure to install all InTouch Access Anywhere components.

To install all InTouch Access Anywhere Components on a single server

1. Log on to the computer hosting the InTouch Access Anywhere server as an administrator.
2. Locate the Setup.exe file on your InTouch Access Anywhere installation media.
3. Double-click on Setup.exe to start the installation.
The installation wizard shows a list of all InTouch Access Anywhere components that can be selected to be installed.
4. Select all listed **InTouch Access Anywhere** (InTouch Access Anywhere Server, InTouch Access Anywhere Secure Gateway and InTouch Access Anywhere Authentication Server) components and click **Next**.
5. Click **Next** on the dialog box that shows all components have been selected to be installed.
6. Select the check box that acknowledges you have read and accepted the terms of the license agreement and select **Agree**.
7. Click **Install** to begin installing InTouch Access Anywhere server.
A horizontal bar shows the progress of the installation.
8. Click **Finish** to complete the installation.

Verify the Installation

Configure (or disable) the Windows Firewall for use with InTouch Access Anywhere. For details, see *Configuring a Firewall Program Exception* on page 20.

To verify your InTouch Access Anywhere Server installation

1. Before using InTouch Access Anywhere to connect to your Remote Desktop server, log on using a standard Remote Desktop Client, select an application from InTouch Application Manager, and launch it in WindowViewer. Every user must connect to the Remote Desktop Server with a Remote Desktop Client for the first time. All subsequent connections by the user to the server can be made via InTouch Access Anywhere.

This configures the initial setup and enables InTouch Access Anywhere clients to determine the list of available InTouch applications.

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

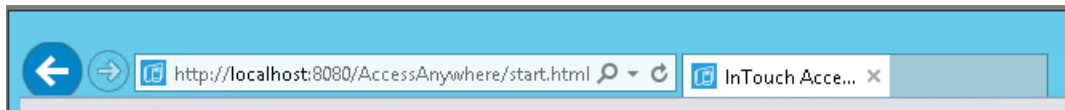
2. Open an HTML5-compliant browser and enter the URL of the InTouch Access Anywhere Server:

`http://machinename:8080/` or `http://IPaddress: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, but will prompt you to continue without a secured certificate.



3. After the InTouch Access Anywhere Server web page appears, enter user credentials and select the InTouch application available from the host computer from the drop-down list.

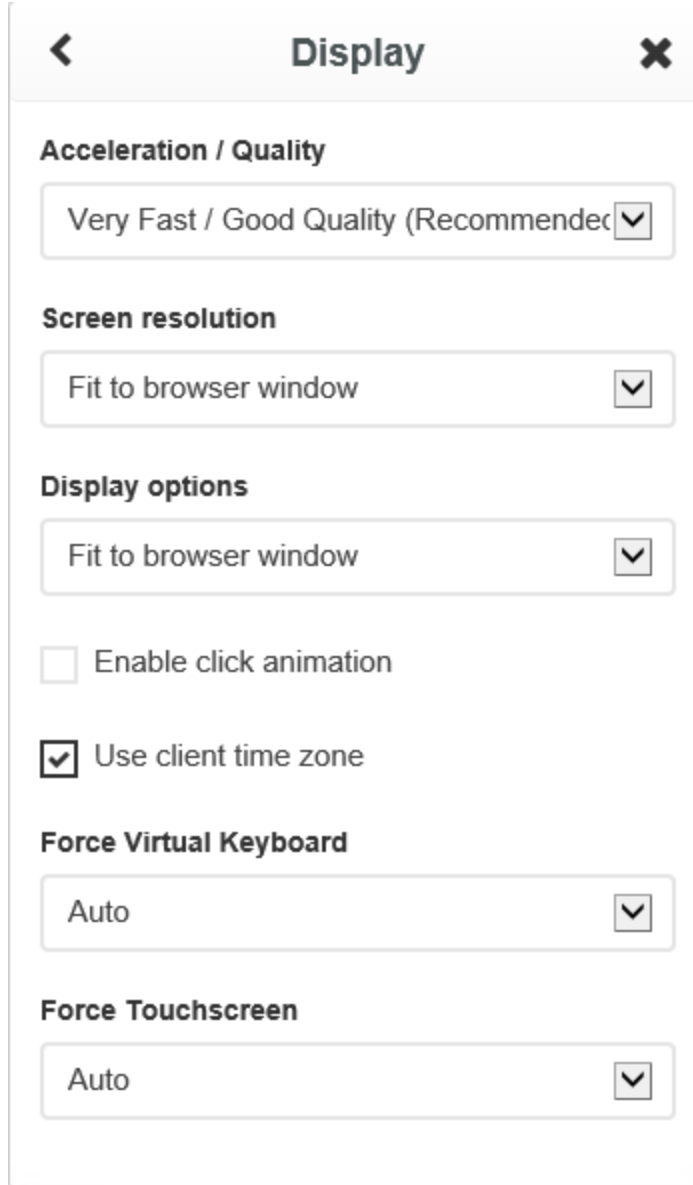
A screenshot of the InTouch Access Anywhere web interface. At the top, it says 'InTouch Access Anywhere' with a settings icon (three vertical dots) to its right. Below this are three input fields: 'User name' with a person icon, 'Password' with a lock icon, and 'Demo Application 1024 X 768' with a dropdown arrow. At the bottom right is a dark grey button labeled 'Connect'.

4. Click the  Settings icon.

Each of the listed **Settings** pages contain different options. You can either continue with the populated default settings or make selections from the available options.

Note: See the *InTouch Access Anywhere User Guide* for detailed descriptions of the options on each **Settings** page.

5. Use the **Display** settings page to select your desired display options and screen resolution.



The screenshot shows a mobile-style settings page titled "Display". At the top left is a back arrow and at the top right is a close "X" icon. The settings are organized into sections:

- Acceleration / Quality:** A dropdown menu showing "Very Fast / Good Quality (Recommended)".
- Screen resolution:** A dropdown menu showing "Fit to browser window".
- Display options:** A dropdown menu showing "Fit to browser window".
- Enable click animation:** An unchecked checkbox.
- Use client time zone:** A checked checkbox.
- Force Virtual Keyboard:** A dropdown menu showing "Auto".
- Force Touchscreen:** A dropdown menu showing "Auto".

6. Click the back arrow twice to return to the login screen, and click **Connect**.

The connection dialog appears momentarily while the web browser connects to the RDS host where the InTouch Access Anywhere Server is installed.

InTouch WindowViewer is launched at the remote node and shows the selected InTouch application.

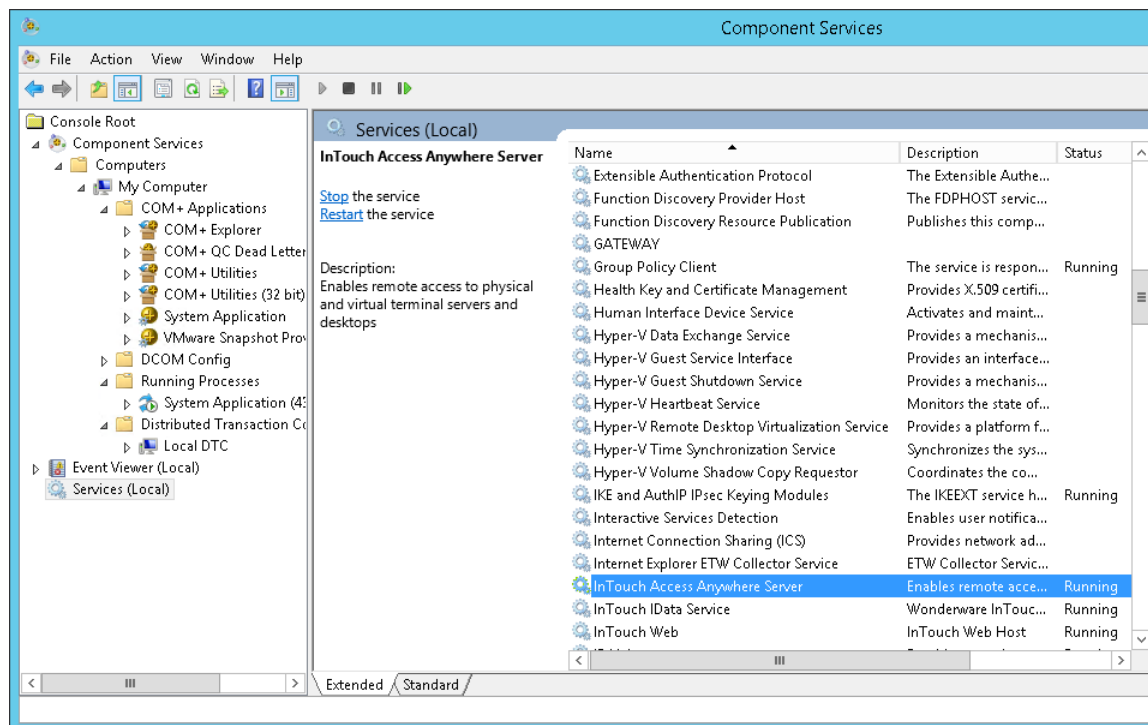
Note: After connecting with InTouch Access Anywhere, closing WindowViewer will log you off and end the session. Closing the browser will leave WindowViewer running; it only disconnects you from the session.

Installation

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

An additional service called `serviceInstaller` is installed to monitor changes in InTouch applications available on the node and update the InTouch Access Anywhere `Start.html` file accordingly. This service updates the **InTouch Applications** drop-down list that appears on the initial InTouch Access Anywhere Server log on page.

Note: The InTouch Access Anywhere service runs under a local domain user account and cannot communicate with applications or folders on remote computers, which are typical of a NAD environment. As a result, NAD applications do not appear in the list of InTouch applications. For more information, see *NAD Limitations* on page 44.



The InTouch Access Anywhere 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 cannot connect to that host. Make sure to configure firewalls and proxies between the end point devices and the server-side component to enable communication using port 8080, or use the InTouch Access Anywhere Secure Gateway.

Updating InTouch Access Anywhere Server

In order to update an InTouch Access Anywhere installation, you must back up any customizations and uninstall InTouch Access Anywhere before installing the latest version. You cannot update InTouch Access Anywhere by installing a new version on a computer currently running a previous version.

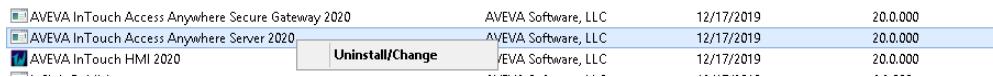
Uninstalling InTouch Access Anywhere Server

InTouch Access Anywhere can be uninstalled by launching `setup.exe` from the installation media and selecting to **Remove** the InTouch Access Anywhere Server component.

You can also uninstall the InTouch Access Anywhere Server from the Windows **Control Panel**.

To uninstall InTouch Access Anywhere Server

1. Open the **Control Panel**.
2. Select **Programs and Features**.
Navigate to the InTouch Access Anywhere Server from the list of programs and features.
3. Right click the InTouch Access Anywhere Server.



4. Select **Uninstall/Change**.
The **Modify, Repair or Remove Installation Wizard** will appear.
5. Select **Remove**, and then click **Next**.
The InTouch Access Anywhere Server will be uninstalled.

Configure InTouch Access Anywhere Server

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

The remote client running on a browser connects to the InTouch Access Anywhere Server service using WebSockets directly or through the Secure Gateway.

Configure the Firewall for InTouch Access Anywhere

The InTouch Access Anywhere Server installation attempts to create exceptions within the Windows Firewall to allow the necessary network connections.

If you experience problems connecting to InTouch Access Anywhere after installation, ensure that the InTouch Access Anywhere Server is configured to allow connections through port 8080, and that its executable is allowed to communicate by configuring the Windows Firewall as follows.

Configuring a Firewall Port Exception

By default, a client (browser) connects to an 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 port 8080.

You can open a port through the firewall either through the command line, or through the Windows firewall configuration. The command line option is presented for advanced users as a quicker way to configure the firewall versus using the GUI.

Using the Command Prompt

To configure the firewall through the command line, first open the Windows **Command Prompt** and run as an Administrator. Then, type the following command:

```
netsh.exe advfirewall firewall add rule name="<Description>" dir=in
action=allow protocol=TCP localport=<PortNumber>
```

Where:

- <Description> = the description used to describe this firewall rule
- <PortNumber> = the TCP port to open

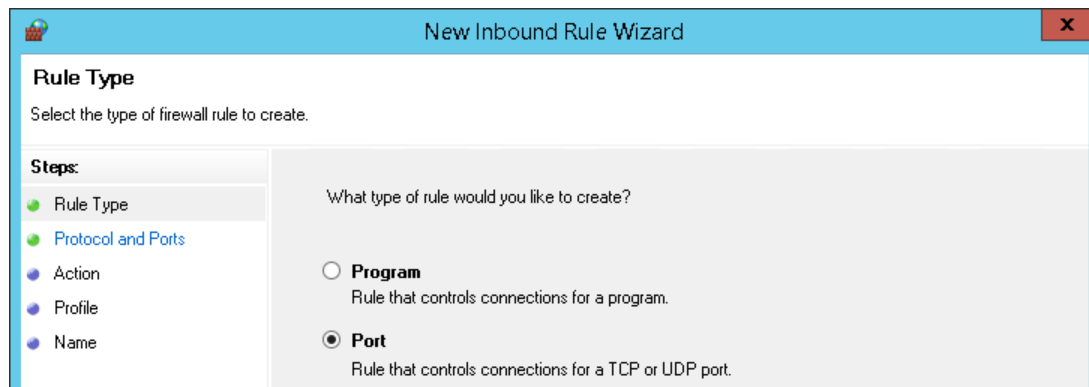
For example:

```
netsh.exe advfirewall firewall add rule name="Open Port 8080 for InTouch Access Anywhere" dir=in action=allow protocol=TCP localport=8080
```

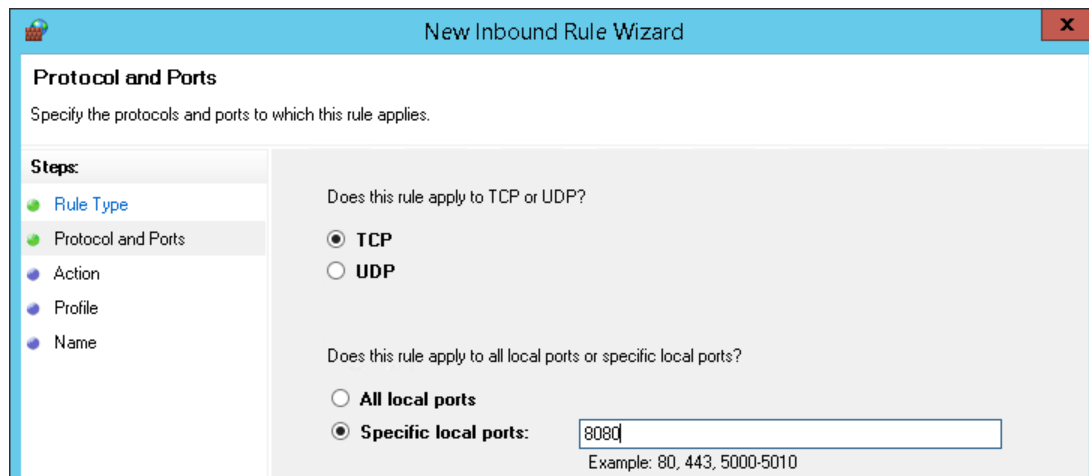
Using the Windows GUI

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. Open the Windows **Control Panel** and then **Windows Firewall**.
2. Select **Advanced Settings** and select **Inbound Rules**.
3. Click **New Rule**.



4. Select **Port** and click **Next**.
5. Enter the specific port: 8080.



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**.

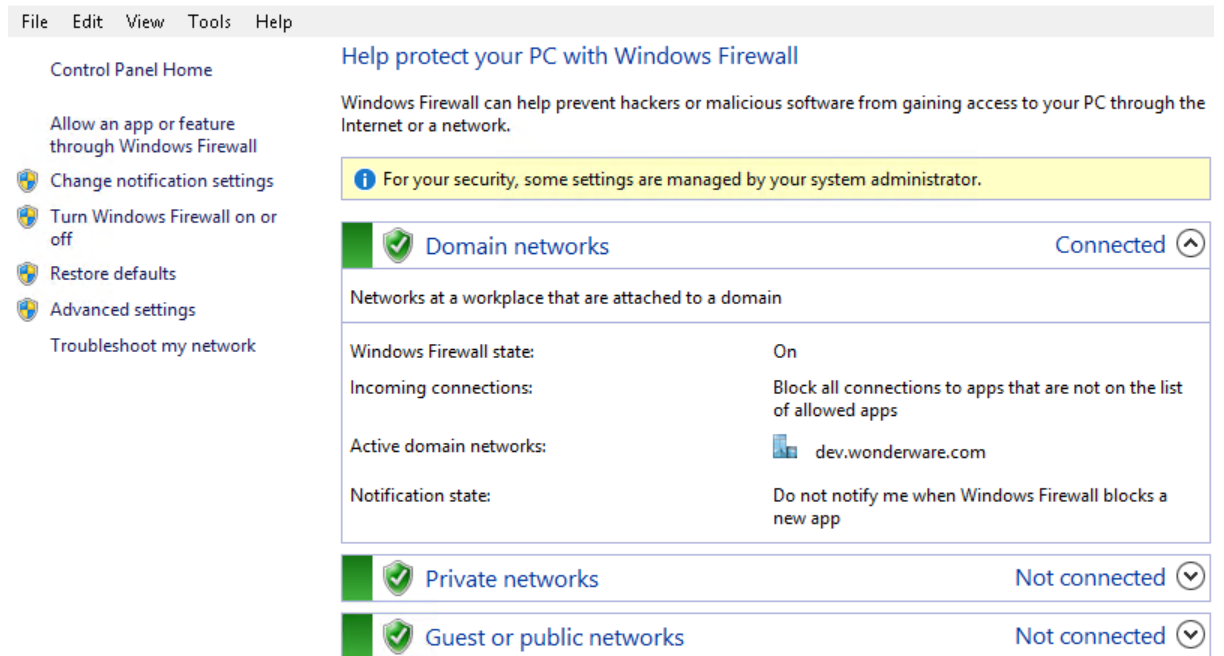
Configuring a Firewall Program Exception

In addition to adding an exception for connections on Port 8080, the InTouch Access Anywhere Server program must be added to the list of programs able to communicate with the network.

To configure a firewall program exception

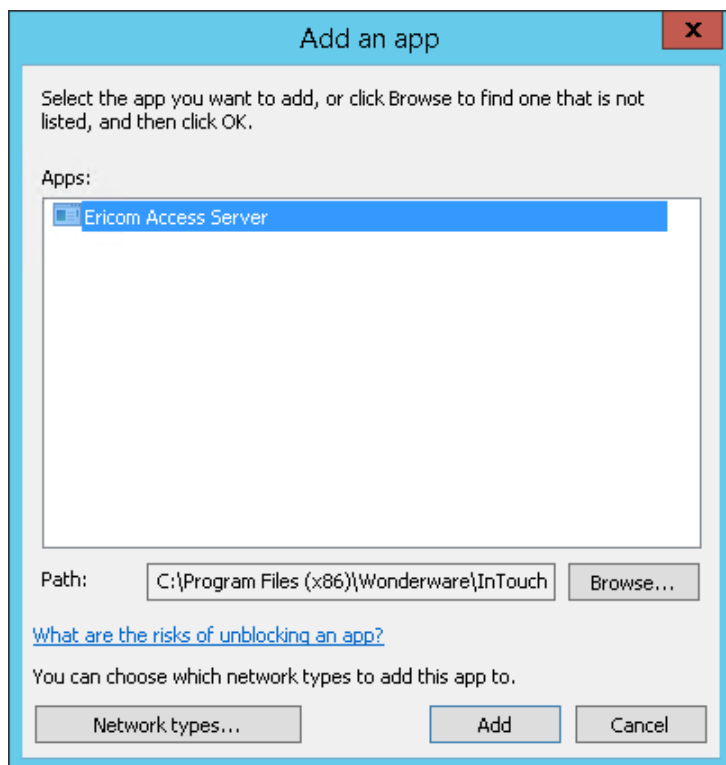
1. Log on to the computer hosting InTouch Access Anywhere server as a Windows administrator.

- Open the Windows Control Panel, and select Windows Firewall. The **Windows Firewall** window appears.



- Click **Allow an app or feature through Windows Firewall**.
- Click **Change Settings**.
- Click **Allow another app..** to show the **Add an app** dialog box.
- Click **Browse**.
- Navigate to the InTouch Access Anywhere installation folder and double-click `AccessServer64.exe`.
 C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server

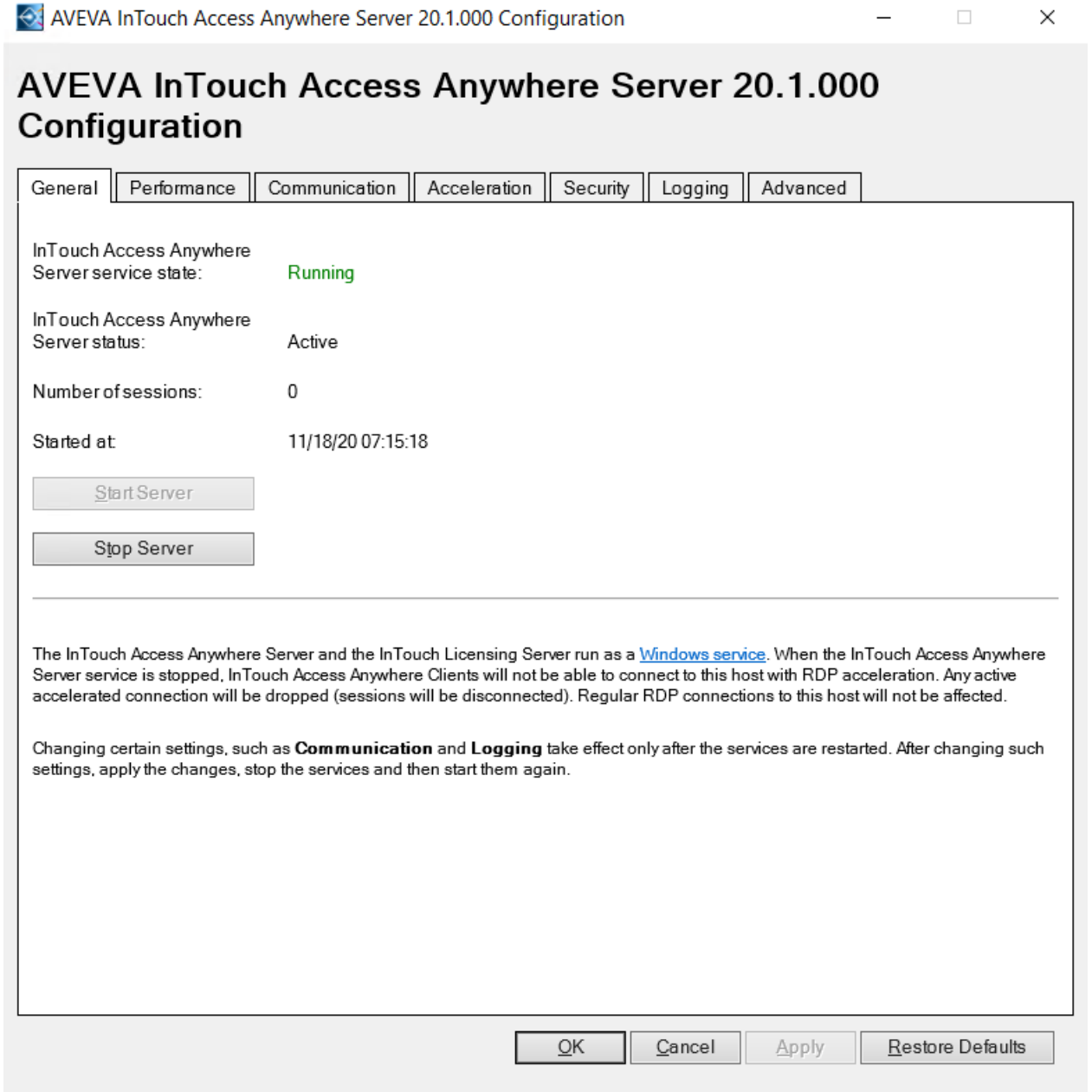
The program appears in the **Add an app** dialog box.



8. Click **Add**, and then click **OK**.

Using the Server Configuration Console

The Server Configuration console shows a series of tabs that enable an administrator to configure various settings of the server service.



You can launch the InTouch Access Anywhere Server Configuration tool from the **Start** Menu Program Group or on the **Apps** view.

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 configuration tabs of the InTouch Access Anywhere Server.

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 computer.

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

Performance

The **Performance** tab displays current performance statistics related to InTouch Access Anywhere connections.

Communication

The **Communication** page provides options to change the InTouch Access Anywhere Server port and the address of the host computer running RDS.

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 computer with multiple network cards, change the RDP host address. Change this address from localhost to the IP or DNS address of the network card that has RDP access to the system.

Changes to either setting require a service restart. The **General** tab provides buttons to start or stop the service. You can also start or stop the service using the Windows Service Manager.

Note: If you change the port number, ensure that you make the corresponding changes to the `config.js` file's "wSPORT" setting. For more information, see *Static Configuration of the Config.js File* on page 31

Acceleration

The **Acceleration** tab provides options to change the Acceleration or Quality level and disable dynamic compression.

When the **Override client acceleration/quality settings** check box is selected, all sessions use the configured setting, and all client settings are ignored. When selecting or clearing this setting, the service must be restarted for the change to become effective. 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 graphic elements within an application screen and compresses them during runtime. The most compression occurs when image quality is set to Low. The best quality images occur 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 dynamic compression, clear the **Use dynamic compression** box.

Security

This **Security** page provides options to configure the InTouch Access Anywhere Server security settings.

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.

To use a custom or trusted certificate, enter the thumbprint ID in the **Certificate Thumbprint** text box and click **Apply**. The certificate's properties will then appear.

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

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.

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 opens the Windows Registry Editor.

InTouch Access Anywhere Web Component

The web component contains the resources used by a web browser to display an interface for the user to connect to an InTouch application. These resources include HTML pages, JavaScripts, CSS files, and graphic images. Review *Advanced Configuration* on page 31 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 with InTouch Access Anywhere Server. The web components are located in the InTouch Access Anywhere Server folder, which by default is:

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

Note: Your installation may be located elsewhere depending on selections made during the installation process.

Modifying the InTouch Access Anywhere Interface

The InTouch Access Anywhere Server start page includes a group of images. All standard images can be edited and replaced with custom images. Keep the replacement images as close to the same dimensions as the original images. A default image is available as the logo.

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

```
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.
\images\Background-neuronal.jpg	Background image for the InTouch Access Anywhere Server landing page.

Note: Unless instructed by our Support group, customizations performed on the InTouch Access Anywhere page not herein described are not supported.

Modifying the Name of the Connection

The InTouch Access Anywhere connection name uses the RDS host node name by default. The connection name can be modified to a custom string.

To change the connection name:

1. Open the config.js file and add the name setting if it does not exist.
2. Set the name value to the desired string enclosed in quotation marks.

```

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

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

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

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

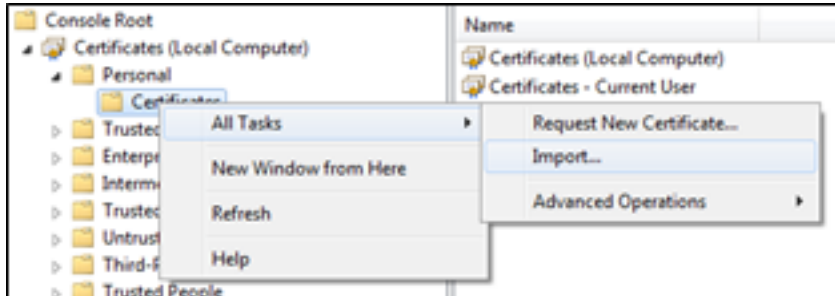
The InTouch Access Anywhere Server installation includes a self-signed certificate for secure SSL connections. Some browsers, such as Google Chrome, allow self-signed certificates for SSL-encrypted WebSocket connections. Opera browsers will notify the user that the server certificate is not signed and prompt the user to continue. Chrome OS, 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

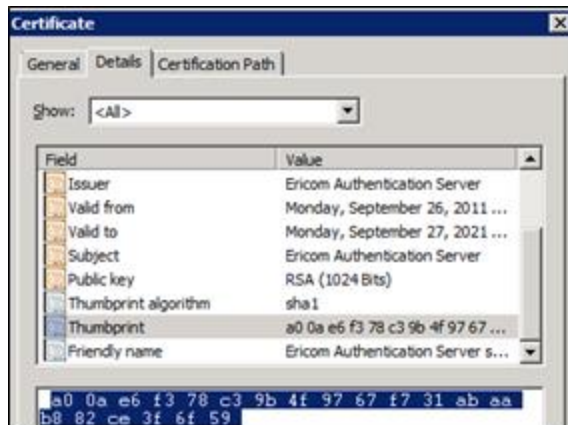
1. Show the Windows Command Prompt running as an Administrator.
2. Type certmgr.msc to show the Certificate Manager.
3. Import the trusted certificate to the Computer (Personal\Certificates) store.



4. Mark the certificate as exportable during the import.



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



6. Copy the thumbprint (Ctrl+c).
7. Stop the InTouch Access Anywhere Server service.
8. Using the Command Prompt (cmd.exe), go to the folder that contains AccessServer64.exe.
9. Run: AccessServer64.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"
```

10. After importing the thumbprint, a notification appears confirming the BIN certificate has been successfully created.
11. 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 a 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. Refer to *InTouch Access Anywhere Secure Gateway Administrator Manual* for instructions to install and configure certificates for use with InTouch Access Anywhere.

Benefit of Using a Trusted Certificate

Certain browsers permit HTTPS or SSL connections 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

This chapter provides information on supported browsers, and information regarding specific behavior of mobile devices, and special devices like tablets.

Supported Browsers

Browsers Tested with InTouch Access Anywhere

The following Web browsers have been formally tested and verified to work with InTouch Access Anywhere.

- Microsoft Internet Explorer 11
- Microsoft Edge
- Firefox version 47
- Safari version 8
- Chrome version 51
- Opera version 38

Functionally Compatible Browsers

This list includes HTML5 browsers that should be compatible with InTouch Access Anywhere, but have not been tested.

- Microsoft Internet Explorer 10 if connected through Secure Gateway
- Firefox versions 38 and later
- Safari versions 5 and later
- Chrome versions 12 and later
- Opera versions 11 and later

Refer to the InTouch Access Anywhere Readme for more information regarding tested and supported browsers.

Older versions of Firefox and Opera require WebSocket support to be manually enabled in the browser configuration.

Multiple InTouch Access Anywhere sessions can be opened in different tabs within the web browser, or in different browser windows. When a session is not in use (its tab or window is not displayed) it will reduce its CPU and memory utilization.

Note: Each InTouch Access Anywhere session consumes an RDP session and an InTouch TSE license.

HTTPS Mode

For environments where WebSockets support is not available, InTouch Access Anywhere can work in HTTPS mode to transmit data by HTTPS only. HTTPS mode is used only if WebSockets support is not available. WebSockets will be used when available as it will provide better performance. InTouch Access Anywhere Secure Gateway requires HTTPS mode when using an Internet Explorer web page browser or any SSL VPNs that only proxy HTTPS traffic.

Note: HTTPS mode requires a browser that supports the HTML 5 Canvas. Older browsers, such as Microsoft Internet Explorer 8 (or earlier), do not support the HTML 5 Canvas.

To enable HTTPS mode, 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).

To enable InTouch Access Anywhere for HTTPS support

1. Install the InTouch Access Anywhere Server on the desired RDS host.
2. Install the Secure Gateway on a separate computer 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 of the target InTouch Access Anywhere Server in the start.html page.
5. After connecting by HTTPS mode, a '-' character appears as a prefix of the address in the browser tab.

Forcing HTTPS Mode

InTouch Access Anywhere Server connections may be forced to use HTTPS mode for all connections. To enable HTTPS-only mode, configure this in config.js file:
onlyHTTPS: true

Note: Forcing HTTPS will speed up the connection process in environments where Websocket is never available. This is because InTouch Access Anywhere Server does not have to attempt the connection using Websocket and wait for the attempt to fail.

CHAPTER 4

Advanced Configuration

Modifying the InTouch Access Anywhere Interface

Some images can be modified in order to customize the appearance of the interface. The following graphics, which are stored in the "resources" sub-folder of the InTouch Access Anywhere Web Server installation (by default, "C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\resources"), are most commonly modified:

Note: Back up the **resources** folder before making any modifications. You can undo your changes by copying the backup to its original location.

File	Description
ericom.jpg	Logo image displayed at top left of InTouch Access Anywhere interface

Note: An experienced web developer can customize more graphics, though these modifications are not supported by technical support.

Adding Languages to the Display Languages Settings Page

Using the Login Settings > Language and Audio page, you can change the Display Language the login page is presented in.

To add or modify the list of languages appearing in the Display Language setting:

1. Navigate to C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\resources\lang
2. To create a new language option, duplicate an existing language file and rename with the name "dictionary.XYZ.txt"; where XYZ is the language code for the new language.
3. Use the format of the existing language file and provide the relevant translated strings for the UI elements.
4. Edit the dictionary.list.txt file present in the same path with the entry "XYZ" at the bottom of the list.
5. Save the file.

Launch a browser and navigate to the InTouch Access Anywhere home page. Navigate to the Languages & Audio settings page. The new language will be available in the Display Language drop down list.

Note: Clear the browser cache and history, if the drop down list is not updated with the new language option.

Static Configuration of the Config.js File

An administrator can modify configuration settings of InTouch Access Anywhere by editing its 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.

The config.js file is located in the following folder path:

c:\Program Files (86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere

Important: Always create a backup before making any changes to the config.js file.

Most configuration settings in the config.js file have the following format:

name: value,

A 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 to assign a value to a setting. JavaScript rules apply in this file and certain characters need to be escaped (for example, backslash).

After the settings are configured, save the file and restart the server.

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

address	Address of InTouch Access Anywhere Server. This is always blank for the standard configuration.
audiomode	0 enables audio redirection (default). 1 plays audio on remote computer. 2 disables audio redirection.
blaze_acceleration	True determines if RDP acceleration is used.
blaze_image_quality	Sets the quality level using a numeric. For example: 40 (fair quality), 75, 95 (best).
dialogTimeoutMinutes	Time out period, in minutes, after which an inactive InTouch Access Anywhere session is automatically closed and logged off. The time out period is relevant only for dialogs that have a log off button.
disableToolbar	True (default); set to False to disable the toolbar, which contains shortcut icons and file functions, that appears within an InTouch Access Anywhere session window.
domain	The name of the domain against which the user name and password are authenticated to grant access to the Remote Desktop session.
encryption	False determines if encryption is enabled from the client to the InTouch Access Anywhere server.
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.
fulladdress	Address of RDP host. This is always blank for the standard configuration.
gateway_address	Defines the address and port of the Secure Gateway. For example: secure.acme.com:4343
gwport	The default gateway port that will be used if it is not explicitly specified in the address field.

hidden	<p>A comma or space-separated list of field names as they appear in config.js. For example, "username,password,domain". The listed fields are hidden to prevent the user from modifying them.</p> <p>To hide a button, such as the Advanced button, prefix the button text with the word <code>show</code>. For example, "showAdvanced, showAbout" hides both the Advanced and About buttons.</p> <p>All hidden variables will ignore previously saved settings.</p>
leaveMessage	The message shown to the user after navigating away from an active session.
minDesktopWidth	Sets the minimum desktop width (in pixels) that InTouch Access Anywhere will display. The default is 800, which may not display as expected or desired on devices with a display width below 800 pixels.
minDesktopHeight	Sets the minimum desktop height (in pixels) that InTouch Access Anywhere will display. The default is 600, which may not display as expected or desired on devices with a display height below 600 pixels.
minSendInterval	Specifies the minimum duration between mouse position messages sent from the client when the mouse button is pressed. Units are in milliseconds.
name	Defines a custom string for the connection name. By default, the RDP host address is used.
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.
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.
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.
reconnectOnDropped	True (default) automatically reconnects a session after recovering from a network outage. Set to False to disable this behavior.
resolution	<p>Sets the resolution size of the InTouch Access Anywhere screen. The value set must be a valid option under the InTouch Access Anywhere screen resolution setting. For example: "1024,768".</p> <p>For Full Screen, use: screen.</p>
sessionTimeoutMinutes	Time out period, in minutes, after which an inactive session is disconnected. The time out period resets automatically whenever the user clicks on the keyboard or a mouse button. The default value is 0, which disables this feature.
settings (URL parameter only)	Name of the Configuration Group to be used.
settingsURL	URL of the connection settings file.

use_gateway	False (default), set to true to use a Secure Gateway for remote access.
wsport	<p>The default WebSocket port that will be used by the client. The value specified in the file (8080 by default) is used for both encrypted and unencrypted WebSocket communication. The user can override this value by explicitly specifying another port address in the client user interface (UI).</p> <p>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.</p>

WARNING! Do not attempt to modify config.js settings not listed here unless directed by Technical Support.

Define Configuration Groups

All users share configuration settings specified in the config.js configuration file. Special settings can override global settings for certain groups of users. Multiple configuration groups are defined in the configuration file.

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

```
var defaults = { / this already exists in the file
    ...
    "Marketing": { // bold text are new additions
printing:true,
clipboard:true
    },
};
```

Note: The quotation marks surrounding Marketing must be identical. If necessary, 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 is 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 an 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 used by InTouch Access Anywhere 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

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

SSO Form Post

Single Sign On (SSO) gives users the ability to view an application running in an InTouch Access Anywhere session with a single authentication. When using a third-party authentication entity (such as an SSL VPN) that supports Form Post, users can sign on to an InTouch Access Anywhere session by entering their authentication credentials only once.

The following figure shows a sample SSO form that users can complete from their mobile devices or computers to remotely connect to an Access Anywhere server and view the running InTouch application.

Note: To use Form POST with Access Anywhere versions prior to 17.2, the Secure Gateway is required.

1 — Username: User1

2 — Password: abc123

3 — Auto Start: true

4 — Run Application: true

5 — Program and Application: "C:\\PROGRA~2\\WONDER~1\\InTouch\\View.Exe" "c:\\programdata\\intouchdemos\\demoapp1_1024\\FitScreen"

6 — Working Folder: "C:\\PROGRA~2\\WONDER~1\\InTouch"

7 — Resolution: 1024,768

8 — Log On

The following table describes the information placed in each field of the sample form shown above.

1	Field to enter the user's username
2	Field to enter the user's password.
3	Boolean value when set to True starts the RDP session and WindowViewer when the connection is made to the InTouch Access Anywhere server. True is the default.
4	Boolean value when set to True runs the specified InTouch application immediately in WindowViewer when the connection is made to the InTouch Access Anywhere server. True is the default.

5	Folder path to the InTouch WindowViewer executable (view.exe), the folder path to the InTouch application, and the window size option of the application.
6	Working folder of the InTouch application to store transient run time data.
7	Horizontal and vertical pixel resolution of the InTouch application window.
8	Login button to submit the POST data to the remote server running the InTouch application.

To pass desired values to Access Anywhere, POST the variables to the path “/AccessAnywhere/sso”. Use the EAN_ Cookie prefix to define the parameters that will be passed using a POST form.

The following figure shows the underlying HTML code for the sample POST form shown above.

```

<html>
<body>
  <!-- Insert Access Anywhere server name or IP address as 'action' value if executing from a remote computer -->
  <form method="Post" action="https://10.101.01.101:8080/AccessAnywhere/sso" >
    <!-- Prompt for user name and password -->
    1 Username:<input type="text" name="EAN_username" value="User1" placeholder="UserName" /><br />
    2 Password:<input type="password" name="EAN_password" value="abc123" placeholder="Password" /><br />
    <!-- Automatically start program = make connection and start RDP session -->
    3 Auto Start:<input type="text" name="EAN_autostart" value="true" placeholder="true" /><br />
    4 Run Application:<input type="text" name="EAN_remoteapplicationmode" value="true" placeholder="true" /><br />
    <!-- Need to specify application path and information for WindowViewer -->
    <!-- Hard coded to default path and demo application -->
    <!-- Program and Application:<input type="text" name="EAN_alternate_shell" size="128" value=""C:\PROGRA~2\
    WONDER~1\InTouch\View.Exe" "C:\ProgramData\intouchdemos\demoapp1_1024" placeholder=""C:\PROGRA~2\WONDER~1\InTouch\
    View.Exe" "C:\ProgramData\intouchdemos\demoapp1_1024" /><br /> -->
    5 Program and Application:<input type="text" name="EAN_alternate_shell" size="128" value=""C:\PROGRA~2\WONDER~1\
    InTouch\View.Exe""c:\programdata\intouchdemos\demoapp1_1024\FitScreen" placeholder=""C:\PROGRA~2\WONDER~1\InTouch\
    View.Exe""c:\programdata\intouchdemos\demoapp1_1024\FitScreen" /><br />
    6 Working Folder:<input type="text" name="EAN_shell_working_directory" size="128" value=""C:\PROGRA~2\WONDER~1\InTouch"
    " placeholder=""C:\PROGRA~2\WONDER~1\InTouch"" /><br />
    7 Resolution:<input type="text" name="EAN_resolution" size="24" value="1024,768" placeholder="1024,768" /><br />
    8 <input type="submit" name="submit" value="Log On" onclick="submitForm()" />
    </form>
  </body>
</html>

```

An EAN_ prefix is appended to the names of all parameters passed in the SSO POST form, which are listed in the config.js file.

1	Field to enter the user name specified as: Username:<input type="text" name="EAN_username" value="User1" placeholder="UserName"
2	Field to enter the user's password specified as: Password:<input type="password" name="EAN_password" value="abc123" placeholder="Password"

3	<p>Boolean value to start WindowViewer when the connection is made to the InTouch Access Anywhere server. True is the default. Specified as:</p> <p>Auto Start:<input type="text" name="EAN_autostart" value="true" placeholder="true"</p>
4	<p>Boolean value to run the specified InTouch application immediately in WindowViewer when the connection is made to the InTouch Access Anywhere server.</p> <p>Run Application:<input type="text" name="EAN_remoteapplicationmode" value="true" placeholder="true"</p>
5	<p>Folder path to the InTouch WindowViewer executable (view.exe), the folder path to the InTouch application, the name of the InTouch application, and the window size option of the application.</p> <p>"Program and Application:<input type="text" name="EAN_alternate_shell" size="128" value="'C:\PROGRA~2\WONDER~1\InTouch\View.Exe"'c:\programdata\intouchdemos\demoappl_1024"/FitScreen'</p>
6	<p>Working folder of the InTouch application to store transient run time data.</p> <p>Working Folder:<input type="text" name="EAN_shell_working_directory" size="128" value="'C:\PROGRA~2\WONDER~1\InTouch"' placeholder="'C:\PROGRA~2\WONDER~1\InTouch"'</p>
7	<p>Default horizontal and vertical pixel resolution of Web browser window showing the running InTouch application..</p> <p>Resolution:<input type="text" name="EAN_resolution" size="24" value="1024,768" placeholder="1024,768"</p>
8	<p>Login button to submit the POST data to the server running the InTouch application.</p> <p><input type="submit" name="submit" value="Log On" onclick="submitForm()" /></p>
9	<p>URL and port of the InTouch Access Anywhere server running the InTouch application</p> <p>https://10.010.01.123:8080/</p> <p>This field can be hidden when the user views the form with a Web browser.</p>
10	<p>The default SSO URL, which is the Access Anywhere server's IP address or domain name, port, and SSO path.</p> <p>https://<Access_Anywhere_server>:8080/AccessAnywhere/SSO</p> <p>The default SSO path is placed in the Access Anywhere server's registry at HKLM\Software\Ericom Software\Access Server\SERVER Side\SSO Path</p> <p>You can modify the SSO path by editing the Windows registry and assigning another value to the SSO Path registry entry.</p>

Include the following fields in the form at a minimum:

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

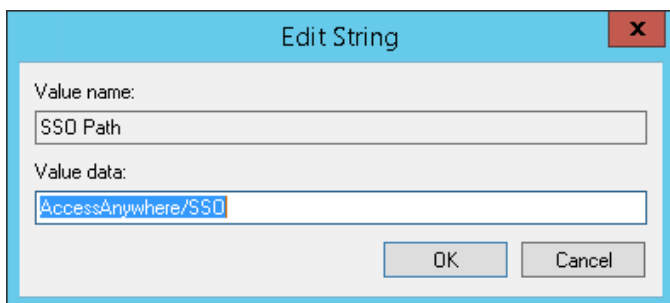
If the target is a relative URL, it will replace the "/sso" portion in the path. *Modify the SSO Path* on page 38 explains how to modify the SSO path in the Windows registry of the Access Anywhere server.

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

Modify the SSO Path

The default SSO path “/AccessAnywhere/sso” located in the Windows registry can be modified. To change this path, perform the following:

1. Open the Windows registry of the computer hosting the Access Anywhere server using regedit.
2. Navigate to HKLM\Software\Ericom Software\Access Server\SERVER Side.
3. Select the **SSO Path** value.
4. Right-click and select **Modify**.



5. Change the SSO path by entering the desired value in **Value data** field in the form: “mypath1/mypath2”
6. Update the SSO URL entry in your POST form.
https://<host>:<port>/mypath1/mypath2

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 an 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.

Hiding InTouch Applications from InTouch Access Anywhere

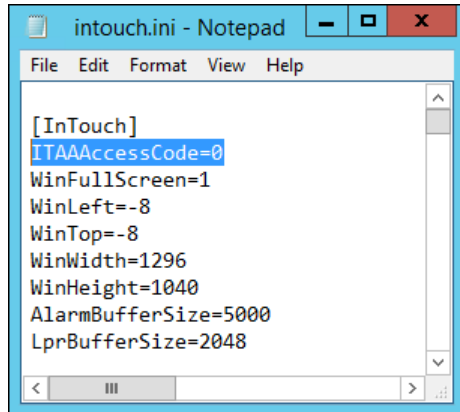
By default, all available InTouch applications are accessible by InTouch Access Anywhere.

You can hide an InTouch application from the list of applications provided by the InTouch Access Anywhere Server start page.

To hide an InTouch application

1. Browse to the location of the InTouch application in Windows Explorer.
2. Open the **intouch.ini** file in a text editor, such as Notepad.
3. Find or create the entry `ITAAAccessCode` under the `[InTouch]` section:

To hide the application, set `ITAAAccessCode=0` as shown below.



To display the application, set `ITAAAccessCode=1`. This setting is unnecessary to display the application unless it exists *and* is set to 0.

4. Save the file under its original filename.

Adding Custom Application Screen Resolutions

The Access Anywhere server can be customized to show custom application screen resolutions on the drop-down list of the **Screen resolution** option.

To add custom application screen resolutions

1. Edit the file available at: `C:\Program Files (x86)\Wonderware\InTouch Access Anywhere Server\WebServer\AccessAnywhere\AppList.Xslt`

```
<select id="resolution">
  <option value="browser"
    selected="selected">STR_FIT_TO_BROWSER_WINDOW</option>
  <option value="screen">STR_FIT_TO_SCREEN_FULL_SCREEN</option>
  <option value="640,480">STR_640_X_480</option>
  ...
  <option value="1920,1200">STR_1920_X_1200</option>
</select>
```

2. Make any changes to the options.
3. Save the file. The updated list will appear in the Screen Resolution option.

Configure Gestures for Touch Devices

InTouch Access Anywhere automatically detects if a portable device is touch capable and automatically uses the built-in virtual keyboard for text input and gesture support for display navigation. InTouch Access Anywhere supports Windows multi-touch gesture redirection. All multi-touch gestures are redirected natively into the Windows session for use by an application running inside an Access Anywhere session.

Multi-touch gesture redirection feature is enabled using the Access Anywhere Toolbar button and by config.js settings.

Activation Criteria

Access Anywhere multi-touch gesture redirection is enabled and activated based on the following criteria:

Multi-touch gesture redirection functionality is enabled if all of the following are true:

- Touch is supported by the remote RDP host
- Touch is supported by the user's computer or mobile device
- Touch redirection is enabled by setting rdpTouchEnabled to True in the config.js file

Multi-touch gesture redirection can be activated if all of the following are true:

- Touch feature is enabled
- Toggle MultiTouch icon is set to active on the Access Anywhere toolbar
- Touch is not suspended by the RDP host

Toolbar button

Users enable and disable the Windows multi-touch gesture redirection feature by toggling the Toggle MultiTouch icon in the Access Anywhere toolbar, which is enabled by default.

Multi-Touch Enabled

Multi-Touch Disabled



Multi-touch Gesture Redirection Settings in the Config.js File

The Config.js file is located in the folder path of the computer hosting the InTouch Access Anywhere server:

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

Config.js Settings	Description
rdpTouchEnabled	True (default) - enable remote touch. On the Server: enable the feature, create RDP dynamic virtual channel, and send RDP client touch events. On the Client – enable the feature, process the incoming server touch messages.
rdpTouchActive	False (default) – Sets the default activation state (ignored when not enabled.) On the Client this is the initial state of the toolbar button. If active, send touch events.

rdpTouchAction	0 (default) - Action to be taken if multi-touch redirection is enabled, but is not supported by the server or client device. Action codes and their assigned values: 0 - no action 1 - display an error message 2 - display an error message and disconnect from the session 3 - ask for user confirmation to continue without touch
----------------	--

Conflict with Local Gesture Usage

When multi-touch redirection is enabled, all gestures are redirected to the remote session. However, the user may need to use gestures locally on the device to pan and zoom around the session. When local gesture functionality is required, disable multi-touch redirection temporarily, and re-enable it when it is needed again.

CHAPTER 5

Known Limitations

This chapter describes known behaviors and limitations of InTouch Access Anywhere when viewing an InTouch application on a portable device. Refer to the *InTouch Access Anywhere ReadMe* for a more detailed list of current known issues in InTouch Access Anywhere.

Networking Limitations

- Network quality

Network quality will impact the performance of InTouch Access Anywhere running on mobile devices. Long latencies, limited bandwidth, and poor Wi-Fi coverage of the working area will impact 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.

- InTouch Access Anywhere does not support WindowMaker

InTouch WindowMaker is not supported in a Remote Desktop environment. Therefore, InTouch Access Anywhere does not support InTouch WindowMaker. To prevent users from attempting to start WindowMaker from WindowViewer, do not install a license that enables WindowMaker and hide the Fast Switch 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, disable or uninstall any active browser extensions or tool bars. Restart the web browser after uninstalling or disabling an extension, and clear the local browser cache, 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.

- Zooming in Browsers

Using the CTRL+ and CTRL- hot keys to zoom an application view in or out only works with Internet Explorer 10.

Navigational Limitations

- Mouse Events

When designing your applications, keep in mind that certain mouse events do not have an equivalent behavior on a touch mobile device, 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
- Pushbutton>Discrete Value>Direct

Other mouse events are triggered with a gesture you must learn. 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.

- Left Click on iPad

A single tap does not consistently toggle the state of a push button. Tap and hold to toggle a push button.

- Scroll Bars

In some cases, moving a scroll bar in a touch environment can 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 on a touch device with a small screen. 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 by 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, users have a better experience using a device software keyboard.

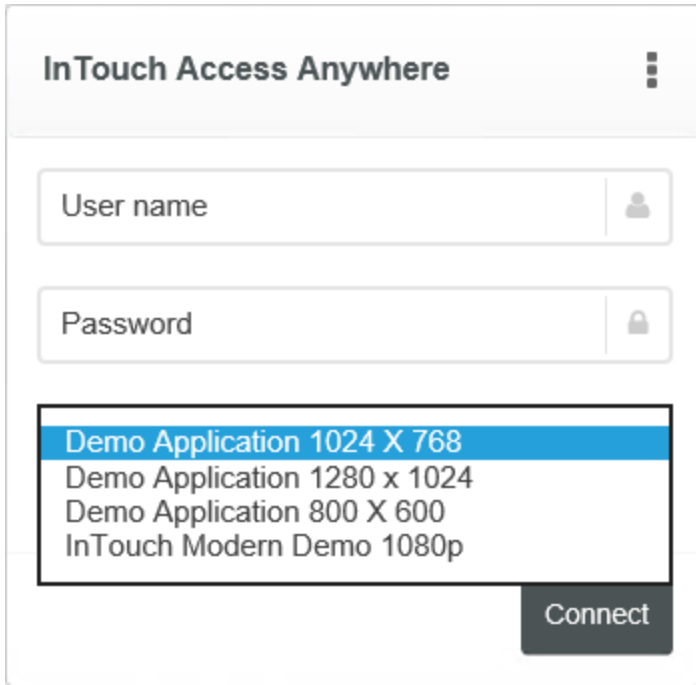
Also, keep in mind that software keyboards in mobile devices in most cases do not have certain keys available in a physical keyboard, such as F1-F12, CTRL, or ALT. If you already have an application that uses Key Scripts associated with some of these keys, modify your application to use alternate available,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

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

NAD Limitations

Distributed InTouch applications typically have a central development computer, central data storage, and client workstations that run distributed applications. You use InTouch Network Application Development (NAD) to build and maintain distributed applications. NAD enables client stations to maintain a copy of a single application without restricting the development of that application. Client stations are automatically notified when the application changes.

NAD applications do not appear on the list of applications shown on the Start.html page when the user logs on to the InTouch Access Anywhere server.



The InTouch Access Anywhere service populates the Start.html file drop-down list of available InTouch applications. This service runs under a local system account by default and cannot communicate with applications or folders on remote computers, which are typical of a NAD environment. This is the reason why NAD applications do not appear in the list of InTouch applications.

If you open Application Manager and see InTouch applications whose folders are not located on the computer's local hard drives, then those applications will also not appear on the drop down list of the Start.html page.

A workaround is to set the InTouch Access Anywhere service to run under a specific domain user account that has sufficient privileges on the Access Anywhere server and can also access the application directory on the NAD master computer.