



UNIFACE ANYWHERE

Administrator Guide

6.0

2019.10.30

COPYRIGHT AND TRADEMARK NOTICE

Copyright © 1997-2019 Uniface B.V.. All Rights Reserved.

This document, as well as the software described in it, is a proprietary product of Uniface, protected by the copyright laws of the United States and international copyright treaties. Any reproduction of this publication in whole or in part is strictly prohibited without the written consent of Uniface. Except as otherwise expressly provided, Uniface grants no express or implied right under any Uniface patents, copyrights, trademarks or other intellectual property rights. Information in this document is subject to change without notice.

Uniface, the Uniface logo, and Uniface Anywhere are trademarks or registered trademarks of Uniface B.V. in the US and other countries. Microsoft, Windows, Windows NT, Internet Explorer, and Remote Desktop Services are trademarks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trademark of Linus Torvalds. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. iPhone, iPad, iPod, Mac, and OS X are registered trademarks of Apple Inc.

© 1999-2019 Uniface B.V.. All rights reserved. Uniface is a trademark of Uniface B.V..

Portions copyright © 1998-2017 The OpenSSL Project. All rights reserved. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org). Portions copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved. This product includes software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Portions of this software are licensed from United Mindworks LLC.

All other brand and product names are trademarks of their respective companies or organizations.

CONTACT INFORMATION

Uniface B.V.

Hoogoorddreef 60, 1101 BE Amsterdam

The Netherlands

Phone: +31 20 311 62 22

Fax: +31 20 311 62 00

www.uniface.com

www.uniface.info

Please direct questions about Uniface to www.uniface.info or uniface.technical.support@uniface.com .

CONTENTS

CHAPTER I - Introduction	1
<i>Introducing Uniface Anywhere</i>	1
<i>Uniface Anywhere Features</i>	1
<i>System Requirements</i>	6
Uniface Anywhere Host	6
Uniface Anywhere Client	7
CHAPTER II - Configuring the Host	8
<i>Upgrading Uniface Anywhere</i>	8
<i>Installing the Uniface Anywhere Host</i>	9
<i>Running the 30-Day Trial Version</i>	10
Activating Uniface Anywhere using an on-premises license	11
<i>Installing the Web Files on a System other than the Host</i>	11
<i>Hosting Web files from a Directory other than the Default Directory using IIS Web Server</i>	12
<i>Running Uniface Anywhere through Apache HTTP Server</i>	13
<i>Configuring Uniface Anywhere to use a Central License Server</i>	14
Opening the License Manager Port in a Firewall	16
<i>Redundant License Servers</i>	16
Three-Server Redundancy	16
License-File List Redundancy	17
<i>License Servers in a Relay Server Environment</i>	19
<i>License Servers in Cloud Environments</i>	20
<i>Automatic Client Keyboard Support</i>	21
<i>Themes</i>	21
CHAPTER III - Administering User Accounts	22
<i>Administering User Accounts</i>	22

<i>Setting Up User Profiles</i>	23
Setting File Permissions	23
<i>Setting up a Network Printer</i>	24
CHAPTER IV - Uniface Anywhere Admin Console	25
<i>Uniface Anywhere Admin Console</i>	25
<i>Managing Applications</i>	26
Installing Applications	26
Publishing Applications	27
Sharing a Link to a Published Application	28
Running the Application outside the Browser	28
Assigning Application Launch Parameters to Users or Groups	32
<i>Managing Sessions and Processes</i>	33
Terminating a Session	33
Ending a Process	34
Shadowing a Session	34
<i>Managing Uniface Anywhere Licenses</i>	36
<i>Security Options</i>	38
Selecting SSL Transport	38
Modifying the Host Port Setting	39
Encrypting Sessions	41
Notifying Users of a Secure Connection	41
<i>Obtaining a Trusted Server Certificate</i>	43
Using an Intermediary SSL Certificate with Uniface Anywhere	44
Using an Intermediary SSL Certificate on iOS and Android	45
Standard Authentication	45
Integrated Windows Authentication	46
Password Caching on the Host	47
Password Caching on the Client	48
<i>Password Change</i>	50
Changing Passwords at Next Logon	50
Prompting Users to Change Passwords Before Expiration	51
Prompting Users to Change Passwords After Expiration	52
Password Change and Integrated Windows Authentication	52
<i>Session Reconnect</i>	53
Setting the Session Termination Option	53
Disconnecting a Session	54
<i>Shared Account</i>	56
<i>Client Time Zone</i>	57
<i>Monitoring Host Activity</i>	58
Viewing Session Information	58
Viewing Process Information	59
Refreshing the Admin Console	59

Setting the Refresh Rate	59
The Status Bar	60
Setting the Broadcast Interval	60
<i>Session Startup Options</i>	61
Applying Group Policy	61
Displaying Progress Messages	61
Setting Resource Limits	65
Specifying the Maximum Number of Sessions	65
Specifying the Minimum Physical and Virtual Memory	65
<i>Session Shutdown Options</i>	66
Specifying the Session Limit	66
Specifying the Idle Limit	66
Specifying the Warning Period	67
Specifying the Grace Period	68
<i>Windows Compatibility Assurance</i>	68
<i>Uniface Anywhere Updates</i>	71
Installing a Uniface Anywhere Update	71
Reviewing Pending and Installed Updates	73
<i>Managing Uniface Anywhere Hosts from Client Machines</i>	73
<i>Keyboard Shortcuts for the Admin Console</i>	75
CHAPTER V - Running Uniface Anywhere	76
<i>Uniface Anywhere App</i>	76
<i>Uniface Anywhere Web App</i>	78
Running the Uniface Anywhere Web App	78
Accessing the Host or Relay Server Directly from the Internet	81
<i>Mac OS X App</i>	82
<i>Uniface Anywhere Startup Parameters</i>	83
<i>Modifying the Logon HTML Page</i>	85
<i>Web Files</i>	86
Resizing the Client Window	87
<i>Uninstalling Uniface Anywhere</i>	87
<i>Automatic Client Updates</i>	87
CHAPTER VI – Mobile App Toolbar Editor	90
<i>Mobile App Toolbar Editor</i>	90
<i>Creating Custom Toolbars</i>	91
<i>Log Files</i>	97
CHAPTER VII - Advanced Topics	98

<i>Load Balancing</i>	98
Independent Hosts	99
Relay Servers	99
Dependent Hosts	100
License Server Configuration	101
Administering Relay Servers and Dependent Hosts on Different Networks	102
Host Selection	103
Relay Server in a DMZ	103
Relay Server Failure Recovery	104
<i>Uniface Anywhere Host Performance Counters</i>	107
<i>Configuration Requirements for Delegation Support</i>	108
<i>Client Printing</i>	112
<i>Designating Access to Printer Drivers</i>	112
<i>Printer Configuration</i>	115
<i>Printers Applet</i>	116
Adding and Removing Printers	116
Setting the Default Printer	117
Editing Printer Settings	117
Printing a Test Page	117
Changing a Printer's Driver	118
Resetting Printer Settings	118
Mapping Printer Drivers	119
Exporting Printer Settings to a File	121
Creating a Default Printer Setting File for a Mapped Printer	121
Client Printer Naming Customization	123
Adjusting the Printable Area	124
<i>Client Clipboard</i>	126
<i>Client Sound</i>	126
<i>Client Serial and Parallel Ports</i>	126
<i>Client File Access</i>	127
Remapping Client Drives	128
Hiding Client Drives	129
Hiding Host Drives	130
<i>Mapped Drives</i>	130
<i>Multi-Monitor Support</i>	130
<i>Specifying the Maximum Color Depth for Uniface Anywhere Sessions</i>	131
<i>Disabling Image Compression</i>	132
<i>Modifying the fontContrast Property</i>	132
<i>Obtaining the Name of the Client Computer</i>	132
<i>Application Script Support</i>	133

<i>Advanced Session Process Configuration</i>	134
Running the Windows desktop in the background of Uniface Anywhere sessions	138
<i>Proxy Tunneling</i>	139
Proxy Tunneling via the HTTP CONNECT Method	139
<i>Support for Internet Protocol Version 6</i>	140
<i>Smart Card Support</i>	142
<i>Performance Auto-Tuning</i>	142
How Performance Auto-Tuning Works	143
<i>Silent Installation</i>	144
<i>Log Files</i>	145
Selecting a New Location for the Log Files	145
Setting the Output Level	146
Maintaining Log Files	146
Client Log Files	147
Connection Monitoring	148
<i>Support Request Wizard</i>	148
<i>High Resolution Client Devices</i>	148
APPENDIX	150
<i>Licensing</i>	150
<i>Obtaining a License File</i>	151
<i>License Change Request</i>	151
<i>RapidX Protocol (RXP)</i>	152
<i>Creating Your Own Certificate Authority</i>	153
Importing the Trusted Server Certificate on a Dependent Host	153
Creating a CA Key and Certificate	154
Creating and Signing Server Keys	156
Generating a CSR Using IIS Certificate Wizard	158
<i>Disabling Automatic Client Keyboard</i>	158
<i>Configuring Support for Client Keyboards and/or IMEs</i>	159
<i>Installing Additional Keyboards and IMEs</i>	159
Client Keyboard Mapping Files	162
Keyboard/IME Identifiers Used by Uniface Anywhere	162
Configuring Client Keyboard Options	163
Specifying Layout Text Substitutions	164
Setting the Fallback Layout Text	164
Configuring Multiple Input Locales	164
<i>Third-Party Components</i>	166
<i>Known Limitations</i>	167

Introducing Uniface Anywhere

Uniface Anywhere is the simple and secure application virtualization solution that extends the reach of existing Windows applications to corporate networks or the web. With Uniface Anywhere, authorized employees, business partners, and customers can securely access applications from anywhere, regardless of connection, location, client platform, or operating system.

Uniface Anywhere Features

- **Network, Remote Dial-up, and Web Accessibility.** Uniface Anywhere provides access to 32-bit and 64-bit Windows applications from Uniface Anywhere Hosts via the network, remote dial-up, or through Web access.
- **Cross-platform Compatibility.** Uniface Anywhere provides access to any Windows application from virtually any client platform. Applications can be run from desktop computers such as Mac, Windows, and Linux, and from iOS and Android mobile devices. Windows-based applications deployed through Uniface Anywhere look, feel, and function as if they were running on a Windows operating system, regardless of the client platform.
- **Client File Access.** Uniface Anywhere supports seamless integration of client drives, including hard disk and mapped network drives. This allows users to access files stored on the client computer and to save files locally.
- **Host Monitoring.** Uniface Anywhere provides real-time monitoring of individual Uniface Anywhere Hosts, control of individual clients and processes, and logout and shutdown for individual users.

- **Session Shadowing.** The session shadowing feature allows multiple users to view and control a single session and its applications. This feature allows help desk personnel and system administrators to help troubleshoot and debug user problems. Session shadowing may also be used for live collaboration.
- **Load Balancing.** Load balancing distributes user sessions across multiple Uniface Anywhere Hosts. When load balancing is enabled, users can reconnect to a disconnected session running on any one of the load-balanced hosts.
- **Session Reconnect.** With session reconnect enabled, Uniface Anywhere maintains client sessions on the server without a client connection. If a user deliberately disconnects from the server, or if the client's connection is lost due to network problems, the user's session and applications remain running on the server for the length of time specified by the administrator. If a client's connection to a host is broken, the client will automatically attempt to reconnect to the host.
- **Performance Counters.** Performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a server. Uniface Anywhere Host performance counters allow administrators to monitor server activity from any machine with network access to a Uniface Anywhere Host.
- **Proxy Tunneling.** Proxy tunneling allows users to connect to Uniface Anywhere Hosts on the internet via proxy servers.
- **Group Policy Support.** Using Microsoft's Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.
- **SSL Security.** Uniface Anywhere provides support for Secure Socket Layer (SSL) as a method for communication between Uniface Anywhere clients and servers.
- **Time Zone Redirection.** This option allows Uniface Anywhere sessions to run in the time zone of the client computer, regardless of the time zone that is selected on the Uniface Anywhere Host.
- **Backward Compatible Client and Host.** This allows a client to connect to a Uniface Anywhere Host when the major and minor versions of the client and server match but the revision (service pack) or build numbers do not.
- **Automatic Client Updates.** Administrators can configure Uniface Anywhere to automatically update Windows clients when users connect to a Uniface Anywhere Host that is running a newer version.
- **Client Printing.** Users can print to client-accessible printers from applications running on Uniface Anywhere hosts. Uniface Anywhere's Universal Printer Driver supports nearly all printers automatically. For advanced, printer-specific features, administrators can configure Uniface Anywhere hosts to use native printer drivers.
- **Dynamic Display Resize.** Uniface Anywhere automatically adjusts the size of the session's desktop when the user reconnects to the session from a different device or changes the resolution of the client device.

- **High Resolution Display Support.** Uniface Anywhere supports high resolution displays. When the Uniface Anywhere client is run on Windows, Uniface Anywhere automatically uses the client computer's DPI (Dots Per Inch) setting. When the client is run on operating systems other than Windows, Uniface Anywhere uses the DPI setting that is specified for the user under the Control Panel's Display applet on the host.
- **Client Sound.** On Windows 7 and later, the Uniface Anywhere Host streams audio output from applications running in Uniface Anywhere sessions to Windows clients.
- **Client Serial and Parallel Ports.** Uniface Anywhere allows applications running on the host to access client machines' serial and parallel ports. This feature is supported on Windows clients only.
- **Mobile App Toolbar Editor.** Administrators can create custom toolbar buttons and menus that appear at the bottom of the Uniface Anywhere Mobile App when a Windows application is accessed from a mobile device. Custom toolbars greatly improve the usability of Windows applications when they are accessed from mobile devices such as iPads, iPhones, and Android tablets.
- **Uniface Anywhere Web App.** Developed with JavaScript and HTML5, the Uniface Anywhere Web App is a zero-install client that allows users to run Windows applications from popular web browsers on Windows, Mac, and Linux computers. The Web App supports copy and paste between local and remote applications, client-side password caching, and printing to local printers via Uniface Anywhere's Preview PDF printer.
- **Uniface Anywhere App:** Combining the functionality of Uniface Anywhere clients and browser add-ons into a single native application that can be run both from a computer's desktop and from a computer's web browsers. Users can install and activate the native app from the web app to overcome browser restrictions and access Uniface Anywhere's full functionality. For example, when the Uniface Anywhere App is installed, users running Uniface Anywhere from a web browser can still access local drives, print directly to local printers, access smart cards, and run applications outside their browser's windows.
- **Mac OS X App:** Uniface Anywhere's new Mac OS X App has been completely re-written to use modern Mac OS X APIs. It provides simplified installation, sound support, multi-monitor support, and Mac OS X Gatekeeper support, which helps protect against malware and misbehaving apps downloaded from the internet.
- **Mobile Sense:** With Uniface Anywhere's Mobile Sense technology, Windows applications behave more like mobile apps. For example, the application window that has the focus is automatically sized to fit the screen of the user's device, and the keyboard automatically opens when the Windows application is able to receive text input.
- **Support for Windows Server 2019.** Uniface Anywhere supports Windows Server 2019 (Standard and Datacenter) as a Uniface Anywhere Host.

- **Windows Compatibility Assurance:** Windows Compatibility Assurance gives administrators the option to automatically defer installation of Windows Updates until Uniface has verified that the updates are compatible with Uniface Anywhere. To support this, Uniface continuously monitors Microsoft's Windows Update service for new updates. When Microsoft releases one or more Windows Updates, Uniface Anywhere suspends installation of all Windows Updates on affected Uniface Anywhere hosts until Uniface has verified that the newly-released Windows Updates are compatible with Uniface Anywhere. If an update is incompatible, Uniface Anywhere prevents installation of all Windows Updates on the affected hosts until Uniface Anywhere has automatically downloaded and installed an update that is compatible with all Windows Update releases. Through this process, Windows Compatibility Assurance minimizes the risk of incompatibilities and relieves administrators of the burdens of managing Windows Updates on Uniface Anywhere hosts.

- **Licensing Summary:** A new tab in the Admin Console lists the Uniface Anywhere licenses that are available to a host and displays each license's Product Code, number of seats, maintenance expiration date, and status. In addition, Uniface Anywhere notifies administrators when license expiration dates are approaching or have been exceeded.

System Requirements

Uniface Anywhere Host

The Uniface Anywhere Host* requires one of the following 64-bit Windows operating systems:

Windows Server 2019

- Standard
- Datacenter

Windows Server 2016

- Standard
- Datacenter

Windows Server 2012 R2

- Standard
- Datacenter

Windows Server 2008 R2

- Standard
- Enterprise

Windows 10

- Professional
- Enterprise

Windows 8.1

- Professional
- Enterprise

Windows 7

- Professional
- Ultimate
- Enterprise

**Uniface recommends Windows Server for multi-user environments.*

- The Uniface Anywhere Host is supported on computers that have the latest Windows Updates installed.
- Where applicable, these platforms are supported with or without the Security Rollup Package.
- Administrators must have administrative rights on the host to perform the installation, and the host must have TCP/IP as a network protocol.
- Uniface Anywhere listens on Uniface's registered port 491 for TCP packets. Configure your external firewall and any software firewall on the host to allow TCP port 491.
- Uniface Anywhere supports VMware ESXi and Hyper-V.
- Uniface Anywhere does not support Windows 10 and Windows Server 2016 systems that have Device Guard enabled.

- The color depth of the client and host must be greater than 256 — 16 million or greater is recommended.
- The Memory and CPU requirements of a Uniface Anywhere Host are determined by the applications that are published and the number of users accessing the system. In general, a Uniface Anywhere Host can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)
- Uniface Anywhere supports a maximum round-trip latency of 500 milliseconds.
- Uniface Anywhere requires a minimum 28.8 kbps modem speed.
- Uniface Anywhere requires 16 kbps per user network bandwidth.

Uniface Anywhere Client

Users can connect to a Uniface Anywhere Host from any computer that supports a Uniface Anywhere client.

Uniface Anywhere supports the following client platforms:

- Windows 10 Professional and Enterprise (32-bit/64-bit), Windows 8.1 Professional and Enterprise (32-bit/64-bit), Windows 7 Professional, Ultimate, and Enterprise (32-bit/64-bit). Uniface Anywhere is supported on computers with the latest Windows Updates installed.
- Mac OS X 10.10 and later
- Red Hat Enterprise Linux and 6 and 7 (64-bit), CentOS 6 and 7 (64-bit), SUSE Linux Enterprise Desktop 12 (64-bit), Ubuntu 16.04 and 18.04 LTS (64-bit)
- iOS 9.0 or later
- Android 5.0 or later on ARM processors

Uniface Anywhere supports the following browsers:

- Internet Explorer 11 (32-bit)
- Mozilla Firefox 52 and later (standard and ESR, 32-bit and 64-bit)
- Apple Safari 9 or later on Mac OS X
- Google Chrome with Windows 7, Windows 8.1, Windows 10, and Chromebook
- Microsoft Edge

Upgrading Uniface Anywhere

Before upgrading to version 6, **you must upgrade the Uniface Anywhere license(s)** by submitting a **License Change Request** by email to license.management@uniface.com. The version 6 host installer *will not upgrade* a computer that does not have a version 6 Uniface Anywhere license.

After submitting the License Change Request form, a version 6 Uniface Anywhere license will be sent via email. Place the new license file in the directory where the existing version 5 license file is stored. (The default license folder for Uniface Anywhere version 5 is C:\Program Files\Uniface\Uniface Anywhere\Programs.)

Remove all version 5 licenses from the Programs directory. Then restart the **Uniface Anywhere License Manager**.

To restart the License Manager

1. Click Control Panel | Administrative Tools | Services.
2. Select **Uniface Anywhere License Manager** from the list of services.
3. Right-click and select **Restart**.

Note: Restarting the License Manager will not affect existing sessions running on the Uniface Anywhere Host.

After restarting the License Manager, run the version 6 Uniface Anywhere host installer by double-clicking **ua-host.exe**.

When upgrading to version 6, you will be prompted to restart the computer two times. The host installer will resume automatically after restarting. As part of the installation process, existing versions of Uniface Anywhere are removed, but Registry settings and files are saved. These files can be found in the **Program Files\Uniface\Uniface Anywhere.backup** folder and in the Registry at `HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere.backup`. The installer also moves the new license file(s) from the Programs directory to the Licensing directory.

Note: Customers will be unable to upgrade their version 5 license to version 6 if their Support contract has expired. To renew, contact your Uniface Anywhere Sales representative.

Installing the Uniface Anywhere Host

Uniface Anywhere is delivered as a self-extracting executable and can be installed by double-clicking **ua-host.exe**. When running the host setup program, you must be logged in to an account that is a member of the computer's Administrator's group.

By default, the Uniface Anywhere Host setup installs all of the core **Host** components, **Web** components (including all the files necessary to configure the host for browser logons) and **Licensing** components. You can customize the installation by clicking the **Customize** button and unchecking the components you do not wish to install. Otherwise, click the **Install** button.

To activate Uniface Anywhere, **copy your Uniface Anywhere license file(s) to the default license folder**, C:\Program Files\Uniface\Uniface Anywhere\Licensing. To configure Uniface Anywhere to use a license server, see **Configuring Uniface Anywhere to use a Central License Server**.

If you opt to copy your license file(s) at a later time, you must restart the Uniface Anywhere License Manager, then the Uniface Anywhere Application Publishing Service after copying the file(s).

To restart the Uniface Anywhere License Manager

1. Click Control Panel | Administrative Tools | Services.
2. Select **Uniface Anywhere License Manger** from the list of services.
3. Right-click and select **Restart**.

To restart the Uniface Anywhere Application Publishing Service

1. Click Control Panel | Administrative Tools | Services.
2. Select Uniface Anywhere Application Publishing Service from the list of services.
3. Right-click and select **Restart**.

After installing the host and restarting the computer, select a web browser to open Uniface Anywhere's **Interactive Quick Start Guide**. This guide provides instructions for publishing applications through the Admin Console, and sharing links to the applications. The **Interactive Quick Start** can be opened at any time by appending **?help=ac** to the Uniface Anywhere logon page. For example, **http://hostname/UAnywhere/?help=ac**

Minimum permissions for the license file(s) (in C:\Program Files\Uniface\Uniface Anywhere\Licensing*.lic) are:

Administrators: Full Control; **Users:** Read & Execute; **SYSTEM:** Full Control

Note:

If the following error message appears in a Log file, it is possible that the permissions are incorrect for the license file:

```
FlexLM code #-1; FlexLM text: Cannot find license file. The license files
(or license server system network addresses) attempted are listed below.
Use LM_LICENSE_FILE to use a different license file, or contact your
software provider for a license file.)
```

When combining two Uniface Anywhere licenses or when using two separate licenses on the same Uniface Anywhere Host, the hostnames in the license files are case-sensitive and must be identical.

If you would like to set startup preferences for the Uniface Anywhere Host, choose Uniface Anywhere Application Publishing Service from the list, and click the **Startup** button. Select the options you want to apply to the Uniface Anywhere Host.

Running the 30-Day Trial Version

Uniface Anywhere's 30-day trial version can be requested from Uniface License Management.

Activating Uniface Anywhere using an on-premises license

For computers without direct access to the internet, or if a cloud trial license cannot be established, Uniface will generate an on-premises, Flexera-based trial license, which will be sent via email.

To activate Uniface Anywhere using an on-premises license

1. Determine the computer's **Host Name** and **Host ID** (Physical Address).
 - a. Open the Command Prompt window by clicking Start | (All) Programs | Accessories | Command Prompt.
 - b. Type **ipconfig /all** and press the **Enter** key.
 - c. Locate the computer's **Host Name** and **Physical Address**.
2. Email to license.management@uniface.com with the computer's Host Name, Host ID (Physical Address), and number of seats.
3. When you receive the license file from Uniface:
 - a. Copy the .lic file into c:\Program Files\Uniface\Uniface Anywhere\Licensing directory.
 - b. Start the **Uniface Anywhere License Manager Service**.
 - c. Restart the **Uniface Anywhere Application Publishing Service**.

Installing the Web Files on a System other than the Host

You can install the Uniface Anywhere web files on a system other than the Uniface Anywhere Host.

To install the Web files on a system other than the Uniface Anywhere Host

1. Run the Host installer on the desired web server, selecting to install the web files.
2. Edit the logon.html page on the web server and add the following statements, inserting the address of the Uniface Anywhere Host in place of hostname.

```
if (host.length == 0)
{
    host="hostname";
}
```

Hosting Web files from a Directory other than the Default Directory using IIS Web Server

You can host the Uniface Anywhere web files from a directory other than the default UAnywhere directory, using Microsoft IIS Web Server.

To host web files from a directory other than the default directory

1. Create a directory in `c:\inetpub\wwwroot\` on the web server and call it what you would like your users to see. For example, create a folder: `C:\inetpub\wwwroot\Web`.
2. Copy the contents of `c:\Program files\Uniface\Uniface Anywhere\Web` directory from a Uniface Anywhere Host to the new directory.
3. Open IIS Manager and go to Sites | Default Web Site. Right-click **Default Web Sites** and click **Add Virtual Directory**.
4. Provide the same **Alias** as the directory created in Step 1, and point the **Physical Path** to the directory where you copied the files in Step 2. For example, `c:\inetpub\wwwroot\Web`.
5. Click the new virtual directory; then double-click on **MIME Types**.
6. Click **Add**. In the **File name extension** box, type `.mem`. In the **MIME Type** box, type `application/octet-stream`. Then click **OK**.
7. To verify that the IIS settings are correct, open a browser and type the URL to connect to your Uniface Anywhere host, for example: **`http://hostname/web/logon.html`**. (*hostname* is name of your Uniface Anywhere Host. *web* is the name of the virtual directory you created in ISS.)

Running Uniface Anywhere through Apache HTTP Server

When the Apache HTTP Server 2.4 web service is installed on the Uniface Anywhere Host, users can connect from a client machine using a web browser.

If IIS is installed, the **World Wide Web Publishing** service must be stopped and disabled before downloading Apache. From **Services**, right-click **World Wide Web Publishing** service and select **Properties**. From the **Properties** dialog, select **Disabled** from the **Startup type** drop-down menu and click the **Stop** button. Click **OK**.

1. Go to <http://www.apachelounge.com/download/> and download the latest version. The version tested by Uniface was **httpd-2.4.29-Win64-VC15.zip**.
2. Download and install **C++ Redistributable Visual Studio 2017**. The version tested by Uniface can be downloaded from the following link: https://aka.ms/vs/15/release/VC_redist.x64.exe
3. Extract **httpd-2.4.29-Win64-VC15.zip** onto the Uniface Anywhere Host in C:\Apache24 directory.
4. Click Start | All Programs | Accessories | Command Prompt. Right-click Command Prompt and Run as administrator.
5. In the **Command Prompt** window, type the following:

```
cd C:\Apache24\bin
httpd -k install
httpd -k start
```

You may need to open port 80 in the firewall if it is not already open. If SSL is running, verify that port 443 is open.
6. Open c:\Apache24\bin and run **ApacheMonitor.exe**. From the system tray, open the Apache Monitor and verify that the service has started.
7. Open c:\Apache24\htdocs and create a directory called UAnywhere.
8. Copy the contents of c:\Program files\Uniface\Uniface Anywhere\Web into c:\Apache24\htdocs\UAnywhere directory.
9. Open a browser on the Uniface Anywhere Host and go to **http://localhost/UAnywhere/logon.html** to start a session.

Uniface Anywhere's version number includes the software's *major version*, *minor version*, *service pack version*, and *build number*. For example, in version **6.1.2.37894**, **6** is the major version, **1** is the minor version, **2** is the service pack version, and **37897** is the build number.

The *major version* number is increased when Uniface releases a Major Upgrade to Uniface Anywhere. Major Upgrades generally include significant new or altered functionality and features, user interface changes, or architectural changes. The *minor version* number is increased when Uniface releases a Minor Upgrade to Uniface Anywhere. Minor Upgrades generally include minor feature additions or alterations, as well as bug fixes and security improvements. The *service pack version* number is increased when Uniface releases a Service Pack to Uniface Anywhere. Service Packs generally include bug fixes, and may include support for new platforms and minor enhancements. The *build number* is increased in all Uniface Anywhere releases. A release in which only the build number is increased is a Patch. Patches generally include fixes for security issues, compatibility issues, and product defects. For example, a Patch may include changes that enable Uniface Anywhere to run on the latest releases of Microsoft Windows.

Configuring Uniface Anywhere to use a Central License Server

By default, the Uniface Anywhere License Manager service is installed together with the Uniface Anywhere Host, and the Uniface Anywhere Host is configured to use the Uniface Anywhere License Manager that is on the same computer as the Uniface Anywhere Host. Alternatively, one or more Uniface Anywhere Hosts can be configured to use a central Uniface Anywhere License Manager that is running on a different computer. You can configure a Uniface Anywhere Host to use a Uniface Anywhere License Manager on a different computer using either of the following methods.

We recommend stopping the Uniface Anywhere License Manager on the Uniface Anywhere Host before getting started. The License Manager should be disabled on all secondary servers of the Central License Server.

To stop the Uniface Anywhere License Manager

1. Click Control Panel | Administrative Tools | Services.
2. Select **Uniface Anywhere License Manager** from the list of services.
3. Click the **Stop** button.

After stopping the Uniface Anywhere License Manager on the Uniface Anywhere Host, you can proceed with one of the following methods for configuring a central license server. In the examples below, *LicenseServer1* is the name of the license server.

On the Uniface Anywhere Host, place port@host (e.g., 27000@LicenseServer1) in the LM_LICENSE_FILE environment variable instead of the path to the license file. FLEXnet Publisher's LMTOOLS.EXE reports that the license file on LicenseServer1 is being read correctly.

—or—

On the Uniface Anywhere Host, place USE_SERVER directly after the SERVER line in the license file on the Uniface Anywhere Host. This is essentially the same as the preceding method but the change to the environment variable is not required.

For example, the permanent license file (e.g., license.lic) on Uniface Anywhere Host would appear as follows:

```
SERVER LicenseServer1 00d0b74f4023
USE_SERVER
```

Opening the License Manager Port in a Firewall

If there is a firewall between Uniface Anywhere Hosts and the license server, the ports for FLEXnet (27000, by default) and for the license manager (BLM) need to be open in the firewall. For the license manager, add

```
port=<port#>
```

to the license on the license server for a specific port. (Unless you manually assign a specific port number, an ephemeral port number is used.)

EXAMPLE:

```
SERVER caspian 000476BA8F74 27000
DAEMON BLM port=5678
INCREMENT session blm 6.0 31-dec-2019 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 6.0 31-dec-2019 uncounted D1D222D031C4
HOSTID=ANY
```

Redundant License Servers

If you wish to use redundant servers, select stable systems as server machines. Do not pick systems that are frequently rebooted or shut down. Redundant license server machines can be any supported Uniface Anywhere Host machines. These servers must have excellent communications on a reliable network and need to be located in the same subnet. Avoid configuring redundant servers with slow communications or dial-up links.

Uniface Anywhere supports two methods of redundancy:

- Via a set of three redundant license servers
- Via a license-file list in the LM_LICENSE_FILE environment variable

Note:

The License Manager service should be disabled on secondary servers of Central License Servers and Three-Server Redundant License Servers.

Three-Server Redundancy

With three-server redundancy, if any two of the three license servers are up and running, a “quorum” of servers is established, and the system is functional and serves its total complement of licenses.

Three-server redundancy is designed to provide hardware failover protection only and does not provide load-balancing. This is because with three-server redundancy, only one of the three servers is "**master**" and capable of issuing licenses.

Following is an example of a three-server redundant license file that Uniface supplies after registering online. You must provide the hostnames of the three Uniface Anywhere Hosts as well as the hostids (Ethernet addresses, in most cases) for each. The port of the license server (e.g., 27000) must also be appended to each server line, if it is not already listed.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
DAEMON blm
INCREMENT session blm 6.0 31-dec-2019 5 99E82D1B9A64 HOSTID=ANY
INCREMENT any_app blm 6.0 31-dec-2019 uncounted D1D222D031C4 \
HOSTID=ANY
```

The three-server license file needs to be copied to each of the three license servers.

Lastly, you must point the Uniface Anywhere Host to the license server. This can be done in two different ways, either by copying the license to each Uniface Anywhere Host and editing it to use `USE_SERVER` (see example below), or by adding each server to the environment variable.

```
SERVER wilson 000476BA8EE9 27000
SERVER piper 00115B73383E 27000
SERVER caspian 000476BA8F74 27000
USE_SERVER
```

With the second option, add each server to the environment variable, using commas to separate the servers. For example, `LM_LICENSE_FILE = 27000@wilson;27000@piper;27000@caspian`. Restart the **Uniface Anywhere Application Publishing Service** and the **Uniface Anywhere License Manager** on the "master" server first (wilson, in the example above), then on the secondary and tertiary servers.

We recommend running Flexera's **Imtools** application to check the status of the redundant license servers once all three servers are up and running. Launch `Imtools.exe` and select the **Server Status** tab. Click on **Perform Status Enquiry** and verify that your servers are "UP."

You can obtain `Imtools` from the Licensing directory (`\Uniface Anywhere\Licensing`) or from the Start menu. The `Imtools` application is included for diagnostic purposes. Any questions on its functionality should be directed to Flexera.

License-File List Redundancy

As an alternative to three-server redundancy, license-file list redundancy is available when there is limited system administration available to monitor license servers, when load-balancing is required for applications located far apart (e.g., Chicago and Tokyo), or when two or more license servers are required.

With license-file redundancy, each one of a group of license servers serves a subset of the total licenses. As such, this method does not provide true redundancy in the way three-server redundancy does.

Set the **LM_LICENSE_FILE** environment variable to a list of license files, where each license file points to one of the license servers. Uniface Anywhere attempts a license checkout from each server in the list, in order, until it succeeds or gets to the end of the list.

The following example illustrates how license-file list redundancy works. If ten licenses are desired, you will need to request two Product Codes with a count of five for each. The actual licenses will be generated from the Product Codes. Unlike with three-server redundancy, the server machines can be physically distant. The license servers on both servers need to be running.

The sample license files will look like:

License 1 for chicago:

```
SERVER chicago 00508BFE7FFE 27000
DAEMON blm
INCREMENT session blm 6.0 permanent 5 DF9C8F5ADF34 HOSTID=ANY \
    user_info="Joe User joeu@mycompany.com" ISSUER="Uniface \
    Corporation" ISSUED=17-feb-2019 NOTICE="Copyright (C) \
    1996-2019 Uniface B.V.. All Rights Reserved" ck=142 \
    SN=12865-AA
INCREMENT any_app blm 6.0 permanent 5 1DF84A360E8F HOSTID=ANY \
    user_info=" Joe User joeu@mycompany.com " ISSUER="Uniface \
    Corporation" ISSUED=17-feb-2019 NOTICE="Copyright (C) \
    1996-2019 Uniface B.V.. All Rights Reserved" ck=84 \
    SN=12865-AA
```

License 2 for tokyo:

```
SERVER tokyo 00508BF77F7E 27000
DAEMON blm
INCREMENT session blm 6.0 permanent 5 16BE40E1D98D HOSTID=ANY \
    user_info="Joe User joeu@mycompany.com" ISSUER="Uniface \
    Corporation" ISSUED=17-feb-2019 NOTICE="Copyright (C) \
    1996-2019 Uniface B.V.. All Rights Reserved" ck=142 \
    SN=12865-AA
INCREMENT any_app blm 6.0 permanent 5 6DB6F3E402DF HOSTID=ANY \
    user_info=" Joe User joeu@mycompany.com " ISSUER="Uniface \
    Corporation" ISSUED=17-feb-2019 NOTICE="Copyright (C) \
    1996-2019 Uniface B.V.. All Rights Reserved" ck=84 \
    SN=12865-AA
```

The administrator of the chicago server should set **LM_LICENSE_FILE** to: 27000@chicago;27000@tokyo where 27000 represents the port that the license servers in Chicago and Tokyo are running. This will direct the license engine to first attempt license

checkouts from **chicago**. If unsuccessful, it will attempt to checkout from **tokyo**.

The administrator of the tokyo server should set **LM_LICENSE_FILE** to: 27000@tokyo;27000@chicago. This will direct the license engine to first attempt license checkouts from **tokyo**. If unsuccessful, it will attempt to checkout from **chicago**.

To change or set the **LM_LICENSE_FILE** variable

1. To view or change the current Environment Variables, right-click **My Computer** and select **Properties**.
2. Select the **Advanced** tab and click **Environment Variables** below.
3. Under **System variables**, select **LM_LICENSE_FILE** and click **Edit**.
4. Change the **Variable value** from **C:\Program Files\Uniface\Uniface Anywhere\Licensing** to reflect the new redundant servers. Separate the license server names with a semicolon (;). Uniface Anywhere will attempt the first server in the list. If that fails for any reason, the second server is tried.
5. Restart the Uniface Anywhere Application Publishing Service.

As with three-server redundancy, we recommend running **lmttools** to verify the status of the redundant license servers once all servers are up and running.

License Servers in a Relay Server Environment

By default, licenses are checked out and managed from dependent hosts. Licenses can be managed from a relay server by setting the value of the **ManageLicensesFrom** property to **Relay** in the **HostProperties.xml** file. This change must be made on the relay server as well as the dependent hosts.

To checkout licenses from the relay server

1. Stop the **Uniface Anywhere Application Publishing Service**.
2. Locate the file **HostProperties.xml** in the **C:\ProgramData\Uniface\Uniface Anywhere** directory.
3. Open **HostProperties.xml** in WordPad and locate the **ManageLicensesFrom** property.
4. Set the **ManageLicensesFrom** property to **Relay**.
5. Save the file.
6. Restart the **Uniface Anywhere Application Publishing Service**.

The default value for the **ManageLicensesFrom** property is **Host**. If this property is changed to **Relay** on an independent host or if it is set to an invalid value, licenses will revert to being managed from the host.

License Servers in Cloud Environments

Uniface Anywhere license files are bound to the MAC address of the computer on which the Uniface Anywhere License Manager service is running. In cloud environments, such as Amazon Web Services (AWS), the MAC address of a virtual computer can change. If the MAC address of a computer running the Uniface Anywhere License Manager service changes, the service will no longer be able to check out licenses and Uniface Anywhere sessions will fail to start. To prevent this, virtual computers running the Uniface Anywhere License Manager service must be configured to have a fixed MAC address. In AWS environments, this may be done by creating an **Elastic Network Interface (ENI)** with a fixed **Elastic IP address (EIP)** and a fixed MAC address, and attaching the ENI to the virtual computer (the EC2 Instance) that is running the Uniface Anywhere License Manager service.

To create an EIP and ENI in AWS and attach it to an EC2 Instance

1. Create an Elastic IP (EIP)

From the EC2 console's navigation pane, go to NETWORK & SECURITY | Elastic IPs, and select **Allocate new address**.

For more information, consult the AWS EIP documentation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html>

2. Create an Elastic Network Interface (ENI)

- 2.1 From the EC2 console's navigation pane, select **Network Interfaces**.
- 2.2 Click **Create Network Interface**.
- 2.3 Enter a **Description**, and choose a subnet from the appropriate Availability Zone.
- 2.4 Leave the Private IP as auto assign.
- 2.5 Choose the Security Groups that include your firewall rules.

3. Assign the Elastic IP (EIP) to the Elastic Network Interface (ENI)

- 3.1 After creating the EIP and ENI, go to Network Interface | Actions | Manage IP Addresses.
- 3.2 Assign the EIP you created in Step 1 to the ENI.

For more information, consult the AWS ENI documentation:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html>

Note:

In order to assign an ENI to an Instance, the subnet of the ENI must be in the same Availability Zone as the AWS Instance running the Uniface Anywhere License Manager service.

You can use the subnet in the Availability Zone or create a custom subnet in the Availability Zone via Amazon Virtual Private Cloud (VPC).

4. Attach the ENI to the Instance running the Uniface Anywhere License Manager service

- 4.1 From the EC Instances, select the Instance that is running the Uniface Anywhere License Manager service and go to Actions | Networking | Attach Network Interface.
- 4.2 Choose the ENI created in Step 2. If it is not available, it may be attached to another AWS instance or it may have been created in a different Availability Zone than the Instance.

Automatic Client Keyboard Support

The automatic client keyboard feature lets administrators configure Uniface Anywhere Hosts to automatically work with any client keyboard. Users can switch between keyboards on the fly using the local keyboard switching features of their client device, and the Input Method Editor (IME) of the client. It is not necessary to install keyboard layouts on the Uniface Anywhere Host or keyboard mapping files on Uniface Anywhere clients.

Automatic client keyboard is enabled by default. Instructions for disabling automatic client keyboard and enabling legacy methods for handling client keyboards are described in the *Appendix*.

Themes

On Windows 7 and later, Uniface Anywhere displays applications using the Windows 7 Theme. On Windows Server 2008 R2, Themes are not enabled by default in Windows.

To enable Themes on Windows Server 2008 R2

1. Install **Desktop Experience**. (<http://technet.microsoft.com/en-us/library/cc742809.aspx>)
2. After the host has been rebooted, start the Themes service.
3. Enable Group Policy in the Admin Console:
 - a. From the Admin Console, click Tools | Host Options
 - b. Click the **Session Startup** tab
 - c. Enable **Apply Group Policy**
4. Enable Themes for all users via Group Policy:
 - a. Run mmc.
 - b. Click **File | Add/Remove Snap-in...**
 - c. Select **Group Policy Object**.
 - d. Click **Add**.
 - e. Click **Finish**.
 - f. Click **OK**.
 - g. Navigate to User Configuration\policies\Administrative Templates\Control Panel\Personalization.
 - h. Double-click **Force a specific visual style file or force Windows Classic**.
 - i. Click **Enabled**.
 - j. Under **Path to Visual Style**, type the path:
%windir%\resources\Themes\Aero\ aero.msstyles

Administering User Accounts

To access applications on a Uniface Anywhere Host, clients must sign in to the host machine. When users start a Uniface Anywhere client, they are prompted for their user name, password, and the name of the host they wish to access. This information is optionally encrypted and passed to the Application Publishing Service running on the Uniface Anywhere Host. The Application Publishing Service then performs the logon operation using standard multi-user features of Windows.

When a user signs in to a host and a domain is not specified, the Uniface Anywhere Host first attempts to authenticate the account on the local machine, followed by the machine's domain, and lastly the trusted domains. Users can override this default behavior and specify a domain by typing the domain name followed by a backslash (\) and their network user name in the **User name** box of the **Sign In** dialog. For example, NORTH\johng.

When a local user name on the Uniface Anywhere Host is the same user name as a domain account, each with a different password, Uniface Anywhere treats them as two separate accounts. Consider, for example, the following scenario:

- A local account on the Uniface Anywhere Host **johng** with a password of **local**
- A domain account **johng** with a password of **domain**

When typing user name, **johng** with the password **local** in the **Sign In** dialog, the account will authenticate on the local Uniface Anywhere Host. When typing **johng** with the password **domain** in the **Sign In** dialog, Uniface Anywhere does not attempt to authenticate on the domain, but fails with an invalid user name or password. You must specify the domain name in the User name field in the **Sign In** dialog. For example, NORTH\johng.

After a user signs in, Uniface Anywhere relies on the host's operating system to provide the security necessary to run applications safely in a multi-user environment. Applications run in the security context of the client user to ensure private sessions. Access to all machines and network resources is governed by the operating system and the rights that have been granted to individual user's sessions.

Users must be able to log on interactively (locally) on the Uniface Anywhere Host. Assign local logon rights to users in Local Security Policy, Domain Security Policy, and Domain Controller Security Policy.

This chapter contains basic information regarding the administration of user accounts on the Uniface Anywhere Host. For more detailed information, please consult Windows Help, accessible from the Start menu.

Setting Up User Profiles

Most Windows applications store user specific settings and files under the user's Windows profile. By default, Windows creates a local profile for each user that logs on to a system. A local profile is specific to a given computer and will not work well if you are running multiple Uniface Anywhere Hosts. If you are running a multi-host environment, you should set up roaming user profiles. A roaming profile is stored centrally and can be accessed from any networked computer for which that profile is valid. When a user with a roaming profile logs on to any networked computer, the desktop will appear exactly as the user left it the last time he or she logged off. For multi-host environments, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

Note: A profile is only valid on the platform for which it was created. For example, a Windows 7 profile can only be used on a Windows 7 computer.

Setting File Permissions

As the system administrator, you may need to restrict user access to certain files and resources. Keep in mind that there are multiple users accessing the host. Particularly in a load-balanced server environment, we recommend write-protecting system and application folders so that users are unable to save files on a local Uniface Anywhere Host. Otherwise, the next time a user logs on to Uniface Anywhere and is routed to a different server, the files and folders will be inaccessible.

You must use Windows Explorer to set the permissions for files on the server. By setting file permissions, you can restrict user access to applications, printers, and folders.

Tip: While in Windows Explorer, choose the **Help** button or press **F1** for more information on setting file permissions.

Setting up a Network Printer

As the administrator, you can set up network printers for use by Uniface Anywhere clients. You must first create a port on the Uniface Anywhere Host that connects directly to the host and then install the printer locally. This provides direct access to the printer.

To add a port to the Uniface Anywhere Host

1. Click Start | Settings | Printers.
2. Double-click **Add Printer**.
3. Select local printer, then click **Next**.
4. Click Create a new port and select Standard TCP/IP Port as the type. Click Next.
5. Type the printer's IP address, as prompted by the printer wizard.
6. Select the printer manufacturer on the left and the printer model on the right, or click **Have Disk**.
7. Follow the directions provided by the wizard to install the proper printer driver.

Uniface Anywhere Admin Console

The Admin Console allows you to administer, monitor, and control client access to the Uniface Anywhere Host. The Admin Console displays a list of the users signed in to a Uniface Anywhere Host, along with the applications users are running. Through the Admin Console, you can perform a variety of administrative tasks, such as adding and removing applications, terminating user sessions, and ending processes running on the host.

To access the Admin Console

Double-click the **Uniface Anywhere Admin Console** icon on the desktop.

–or–

1. Click the **Start** button on the Windows taskbar.
2. Click Uniface Uniface Anywhere | Admin Console.

1.

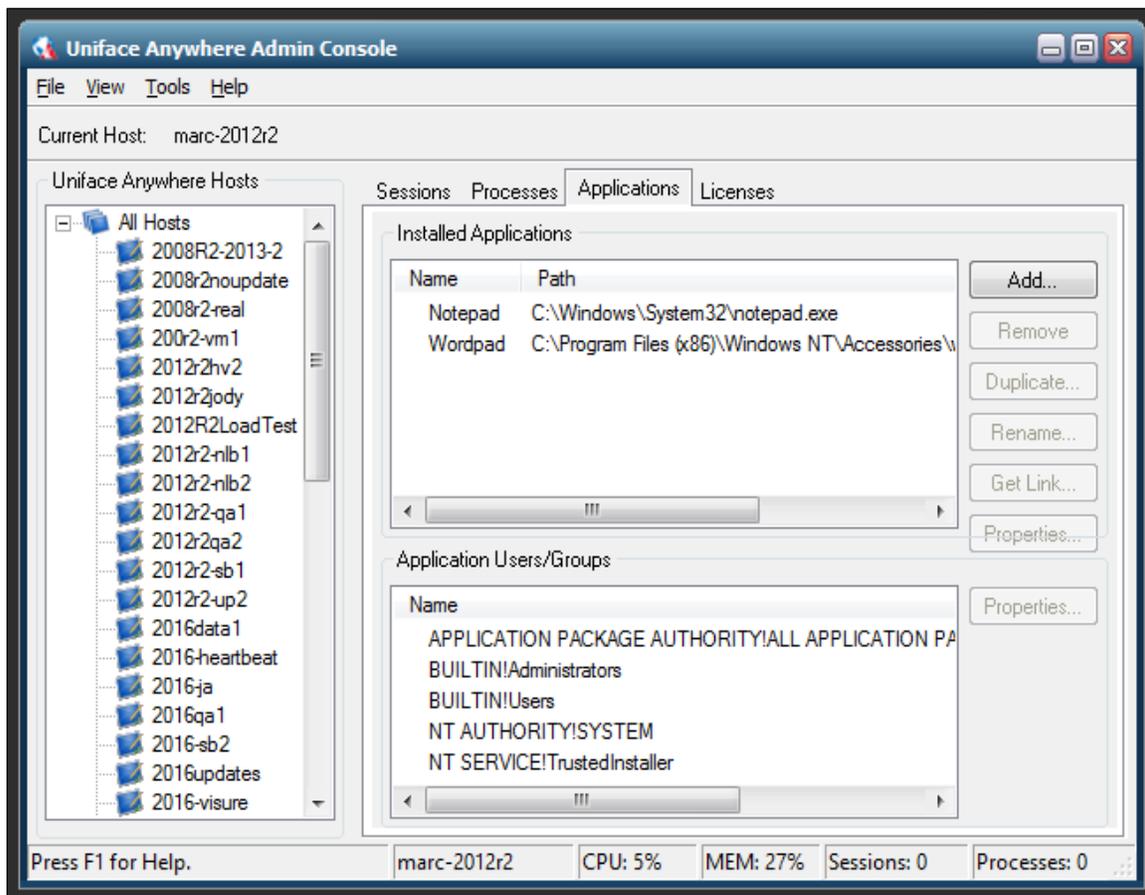
The left panel of the Admin Console lists the hosts on the network running the Application Publishing Service. By default, the Admin Console displays information for the host running on your machine. To connect to other hosts and view information about them, click the host name from the list of Uniface Anywhere Hosts.

If a host's icon has a red x, the administrator does not have administrative rights on the host. If the host's icon has a red x and is grayed out, the host is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that host from the Admin Console.



Click the **All Hosts** icon in the left panel of the Admin Console to view a list of all active sessions on the network. This allows you to view active Uniface Anywhere sessions without connecting to individual hosts. This is also helpful for locating a particular session's host.

You must belong to the Administrators group on each Uniface Anywhere Host in order to access that host from the Admin Console. Without administrative rights on a host, you will be unable to add applications and terminate processes, etc.



Managing Applications

The Admin Console allows you to publish and share applications.

Installing Applications

When installing applications to be run through Uniface Anywhere, please consult the vendor's documentation for instructions on proper multi-user installation. You will likely need to install the application under an administrative account, but installation requirements will vary depending on the application. Installation should also adhere to Microsoft's guidelines for multi-user deployment.

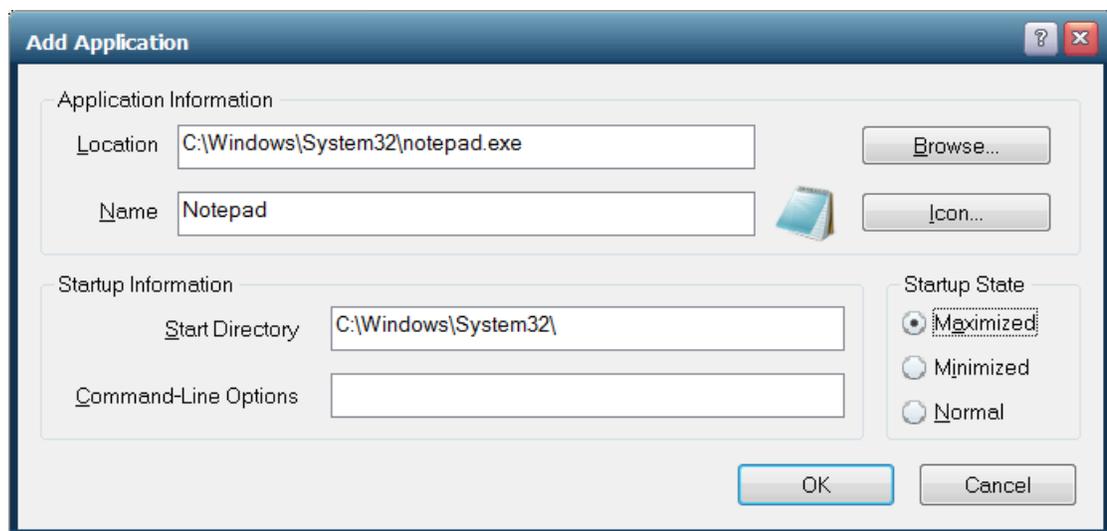
Note: Please note that deploying applications via Uniface Anywhere does not entitle your enterprise to unlimited access rights. You must still abide by the vendor's licensing agreement with regard to the number of applications that can be run concurrently.

Publishing Applications

Applications are published in the Admin Console. When you publish an application, you can specify the application's startup state, as well as startup parameters that control how the application opens. When running the *Interactive Quick Start Guide*, follow the prompts to publish an application.

To publish an application

1. Select the desired host from the list of **All Hosts**.
2. Click the **Applications** tab.
3. Click the **Add** button.
4. Click the **Browse** button next to the **Location** box to locate and select the application's executable file.
5. Click **OK**.



By default, the browse dialog opens to the **PROGRAMDATA\Microsoft\Windows\Start Menu\Programs** directory. After publishing the first application, the dialog then opens to the directory of the last published application.

Changing the Application Name

If you browsed for the application's .exe file, the file name will automatically be entered in the **Name** box. (This application name is displayed to users in the Program Window.) You can keep the default display name or you can type a new one. The application name cannot consist entirely of spaces and it cannot contain a backslash (\). This field cannot be left blank.

Changing the Application Icon

Click the **Icon** button if you would like to select an icon other than the application's default icon.

Changing the Startup State

In the Startup State section, select whether the application starts *Maximized*, *Minimized*, or in *Normal* mode. The default startup state is Normal.

Changing the Start Directory

2. If you browsed for the application's executable file, the pathname of the directory will automatically be displayed in the **Start Directory** box. Otherwise, type the full pathname of the directory in which you want the application to start.

Specifying Command-Line Options

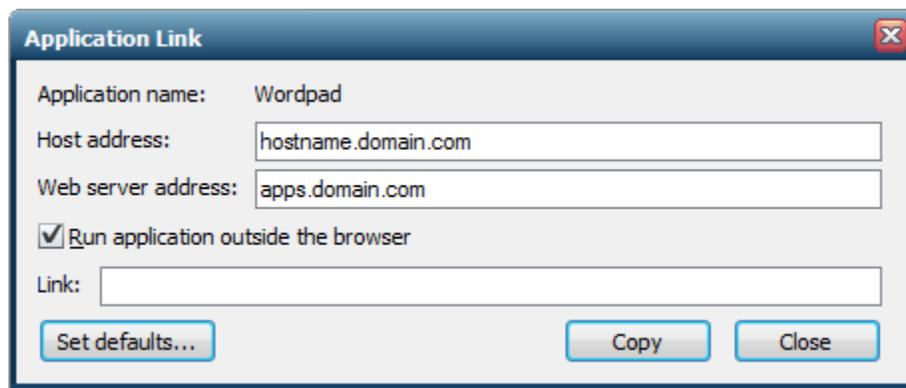
In the **Command-Line Options** box, you can specify launch parameters for the application. Because these parameters are specific to each application, please refer to the application's documentation for information about specific launch parameters.

Sharing a Link to a Published Application

The Admin Console's **Get Link** button allows you to copy a link to the selected application and share it with users for quick access to the application.

To share an application link

1. From the list of **Installed Applications**, select the application you would like to share.
2. Click the **Get Link** button to the right of the list of Installed Applications.
3. From the **Application Link** dialog, click the **Copy** button to copy the link to the clipboard.
4. Paste the link into an email or instant message and share with users.



Note: If the Admin Console is running in tutorial mode, the following message is displayed when clicking the **Copy** button: *Click **Copy** to copy this link to the clipboard. You can then paste it into an email or instant message and share it with users.*

Running the Application outside the Browser

When the user clicks the link to the published application and signs in to the Uniface Anywhere Host, the application opens and runs outside the web browser. To disable this default setting, uncheck **Run application outside the browser**. This will add the parameter **&embed=true** to the URL. When the user clicks the link with this parameter added, the application will run inside the user's web browser.

Editing the Host Address

The **Host address** specifies the address that the Uniface Anywhere App or Web App will use to connect to the host computer. By default, this is the fully qualified domain name of the computer on which the Uniface Anywhere Host is installed. In cases where clients connect to hosts via a relay server or load-balancer, set the **Host address** to the fully qualified domain name of the relay server or load-balancer.

To edit the Host address

1. In the **Application Link** dialog, type the fully qualified domain name of the host in the **Host address** box. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

Editing the Web Server Address

The **Web server address** specifies the address of the web server that is used to serve the Uniface Anywhere Web App and the Uniface Anywhere App and their supporting files to users' browsers. The default web server address is the same as the host address. If you plan to use your own web server, install the Uniface Anywhere Web component on the web server and change the **Web server address** to the address of your web server. For example, if your web server is installed on the same computer as the Uniface Anywhere host, set the **Web server address** and the **Host address** to the same address, the address of the computer on which the Uniface Anywhere host and the web server are running.

To edit the Web Server address

1. In the **Application Link** dialog, type the address of your web server in the **Web Server address** box. The application link will update automatically.
2. Click the **Copy** button to copy the URL and share with users.

Note:

If users will access the host from both internal and public networks, the host and web server must be accessible from both the internal and public networks via the addresses specified in the **Host address** and **Web server address** fields. To accomplish this, internal DNS entries must map the **Host address** and **Web server address** to the internal IP addresses of the computers, and public DNS entries must map the **Host address** and **Web server address** to the public IP addresses of these computers.

Setting Default Link Properties

You can set the default application link properties to those specified in the **Application Link** dialog, to include the Host address, Web server address, and whether the application is run inside or outside the browser. These default link properties will be applied when new applications are published.

To set the default link properties

1. From the **Application Link** dialog, click the **Set defaults** button.
2. Click **Yes** to confirm.

Duplicating an Application

Duplicating an application makes an exact copy of the selected registered application. This is useful if you want to make the same application available to different users or groups but with variations. For instance, you may want to register one version of an application with command-line options to bypass the **Sign In** dialog, and another version without command-line options that requires clients to sign in. When duplicating an application, you are required to select a new display name.

To duplicate an application

1. From the list of **Installed Applications**, select the application you would like to duplicate.
2. Click **Tools | Applications | Duplicate**.
–or–
Click the **Duplicate** button to the right of the list of Installed Applications.

Renaming an Application

The display name that you assign to an application will appear to the end user in the Program Window. You can change an application's display name at any time.

To rename an application's display name

1. From the list of Installed Applications, select the application you would like to rename.
2. Click **Tools | Applications | Rename**.
–or–
Click the **Rename** button to the right of the list of Installed Applications.
3. Type a name in the **New** box in the **Rename Application** dialog.

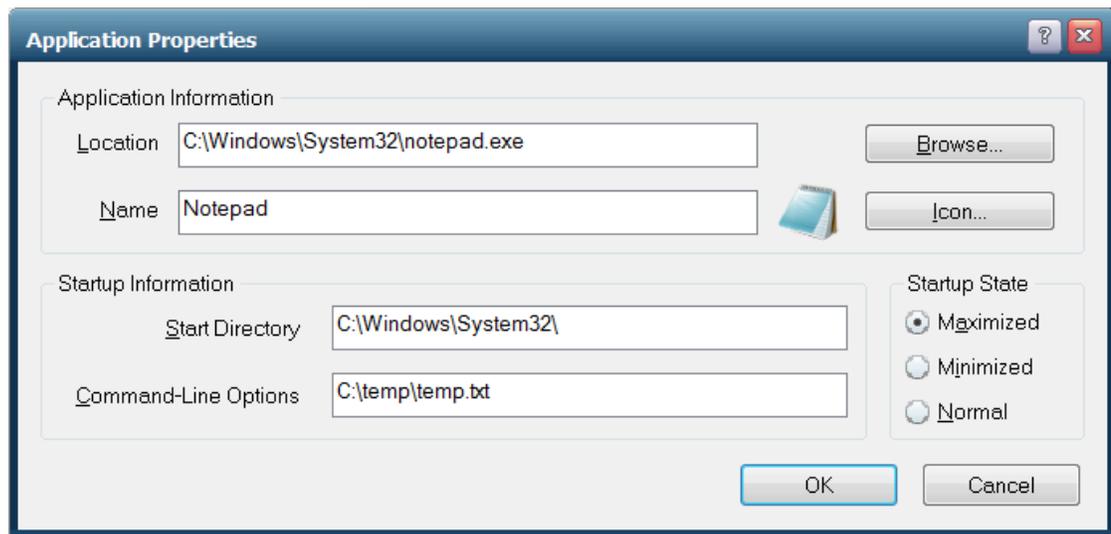
Editing an Application's Properties

Once an application has been published, you can edit the application's properties at any time. For example, you can edit the application's startup state, the location of its executable file, or the folder from which you want the application to start.

To edit an application's properties

1. Click the **Applications** tab.
2. Select an application from the list of Installed Applications.
3. Click the **Properties** button.
4. Do any of the following:
 - In the **Location** box, type a new pathname.
 - In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
 - In the **Command-Line Options** box, type any startup parameters for the application.
 - In the **Display Name** box, type a new display name for the application.
 - In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.

- Click the **Icon** button to browse for a new application icon.



Removing Applications

Uniface Anywhere-deployed applications are removed through the Admin Console. Removing an application from the Admin Console does not uninstall it from the host; it only prevents Uniface Anywhere clients from accessing the application.

To remove an application

1. Click the **Applications** tab.
2. From the Installed Applications list, select the application(s) you want to remove.
3. Click the **Remove** button.

–or–

Click Tools | Applications | Remove.

If you remove an installed application from the Admin Console while a user is running the application, the user's session is not interrupted. When the user exits that application, however, the application will no longer be available, and the icon will not appear in the Program Window.

After registering an application with the Admin Console, the application's name and path will appear in the list of **Installed Applications**. You can sort items in the list in ascending or descending order by clicking the column's title. This holds true for all lists in the Admin Console.

If you want to set up applications that use ODBC data sources, you must set up the ODBC drivers as system DSNs (data source names), in order for Uniface Anywhere clients to be able to access the data sources. For more information about data sources, consult the Windows ODBC Data Source Administrator online Help.

Due to access restrictions, the Admin Console cannot verify the validity of paths specified in UNC format (e.g., \\Machine Name\Folder Name\...) or that reside on a mapped network drive. If the Location or Start Directory of a published item involves a mapped drive or is specified with a UNC path, the Admin Console will accept the specified path regardless of whether or not it is valid. If the path is invalid, or if the client user does not have rights to access the specified

executable file or folder, the published item will not appear in the Program Window. Select the item and click the **Properties** button. Try updating the item's **Location** or its **Start Directory**.

If the item has been uninstalled or moved to a new location, it will not be displayed in the Admin Console when the Application Publishing Service has been restarted.

The Admin Console is unable to display group and user settings for any item's path specified in UNC format or that resides on a mapped drive. The following message is displayed in the Admin Console's Application Users/Groups window for any application or file where this applies: "User/Group settings not available."

If an item that resides on a mapped drive but is not licensed for use with Uniface Anywhere is published in the Admin Console, the item's icon will appear in the Program Window. However, the user will be unable to open the item and will receive an error message when attempting to launch it.

Tip:

Click the right mouse button on an item in the list of Installed Applications or the list of Application Users/Groups to display shortcut menus of the most frequently used commands.

Assigning Application Launch Parameters to Users or Groups

The Admin Console allows you to assign specific parameters for how an application will run for users or groups on the network or on local machines. The parameters set for a user or group will apply each time that user or group launches the application. Application launch parameters set for an individual take precedence over parameters set for a group or for an application. When a client launches an application through Uniface Anywhere, the Program Window will first check for launch parameters assigned to the individual user. If no parameters are assigned, it will check the list of Groups the user belongs to, in the order the Program Window obtains them from the system. Otherwise, the Program Window will look for generic launch parameters assigned to the application.

Tip:

Check the user's **About Uniface Uniface Anywhere** box to verify what Group or Groups the user is assigned to and in what order the Groups are listed in the system.

File permissions for users and groups are controlled by Windows NT file system (NTFS) security settings on the host. File permission are *not* set through the Admin Console. When you select an application from the Installed Applications list, the Application Users/Groups list displays the user permissions that have been specified for that file and/or application with NTFS. You can then edit the application's properties for specific users or groups. File permissions can only be set on drives formatted with NTFS.

To assign application launch parameters for a user or group

1. Click the **Applications** tab.
2. Select an application from the list of **Installed Applications**.
3. Select a user or group from the **Application Users/Groups** list.
4. Click the **Properties** button.
5. Do any of the following:

- In the **Start Directory** box, type the full pathname of the directory in which you want the application to start.
- In the **Startup State** section, select whether the application starts maximized, minimized, or in normal mode.
- In the **Command-Line Options** box, type the command-line arguments you want to use when launching the application.

The screenshot shows a dialog box titled "Application Properties for BUILTIN!Users". It contains the following fields and options:

- User Information:** User Name: BUILTIN!Users
- Application Information:** Display Name: Wordpad
- Startup State:** Radio buttons for Maximized, Minimized, and Normal (selected).
- Startup Information:** Start Directory: C:\Program Files\Windows NT\Accessories\; Command-Line Options: (empty)

Buttons for OK and Cancel are located on the right side of the dialog.

Managing Sessions and Processes

Administrators can encrypt and shadow sessions and terminate processes and sessions through the Admin Console, as described below.

Terminating a Session

When terminating a user's session, all Uniface Anywhere-deployed applications that the user is running will be terminated, and the user will be logged off the Uniface Anywhere Host.

To terminate a session

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to terminate.
3. Click Tools | Sessions | Terminate.

Ending a Process

A process is any action taking place on a Uniface Anywhere Host that is initiated by a client. A client running an application, for example, is a process. Each running application is assigned a unique name and process ID in the Windows Task Manager. These process names and IDs are duplicated in the Admin Console. Administrators can end any process from the Admin Console.

To end a process

1. Click the **Processes** tab.
2. Select the process or processes you would like to end.
3. Click Tools | Processes | Terminate.

Note: Terminating a session or ending a process without giving users a chance to close their application can result in the loss of data.

Shadowing a Session

Session shadowing allows multiple users to view and control a single session and its applications. This allows technical support and system administrators to provide remote assistance to customers and users. Session shadowing may also be used for live collaboration.

Only administrators can connect to running Uniface Anywhere sessions, but only with permission from the session's user.

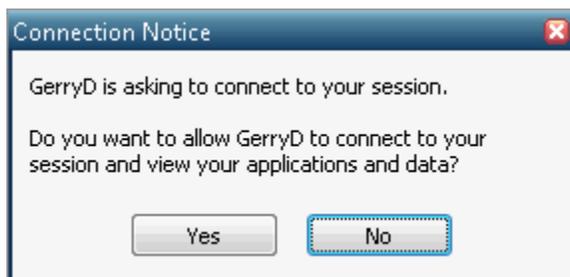
To shadow a session

1. Click the **Sessions** tab.
2. From the **Sessions Name** column, select the session(s) you would like to shadow.
3. Click Tools | Sessions | Connect.

–or–

From the **Sessions Name** column, right-click the session you would like to shadow.

After the session is selected, a message such as the following is displayed to the session's user, where GerryD is the administrator's user name:



If the user clicks **Yes** and permits access to his or her session, the connection is made immediately and the Uniface Anywhere client session opens in a new frame window.

If the user clicks **No** and denies access, the following message is displayed on the host:



Session shadowing will also be denied when the session is disconnected, when the session is about to be or is in the process of being shut down, or when the user fails to respond within one minute. Connection is also denied in the event of a Uniface Anywhere communication failure.

The **Sessions** tab of the Admin Console displays the number of clients connected to a session. 2 or higher in the **Connected Clients** column indicates that the session is being shadowed. Disconnected sessions have 0 connected clients. To disconnect from a session and end session shadowing, simply close the frame window where the session is displayed.

Note: When a Uniface Anywhere session is being shadowed, the host's cursor remains on the client until that session is closed. It does not go away even when the session is no longer being shadowed.

Managing Uniface Anywhere Licenses

The Admin Console lists all the Uniface Anywhere licenses that are available to a host and displays each license's Product Code, number of seats, expiration date, status, etc. Uniface Anywhere warns administrators when expiration dates are approaching and when licenses and Support contracts have expired.

To view licenses

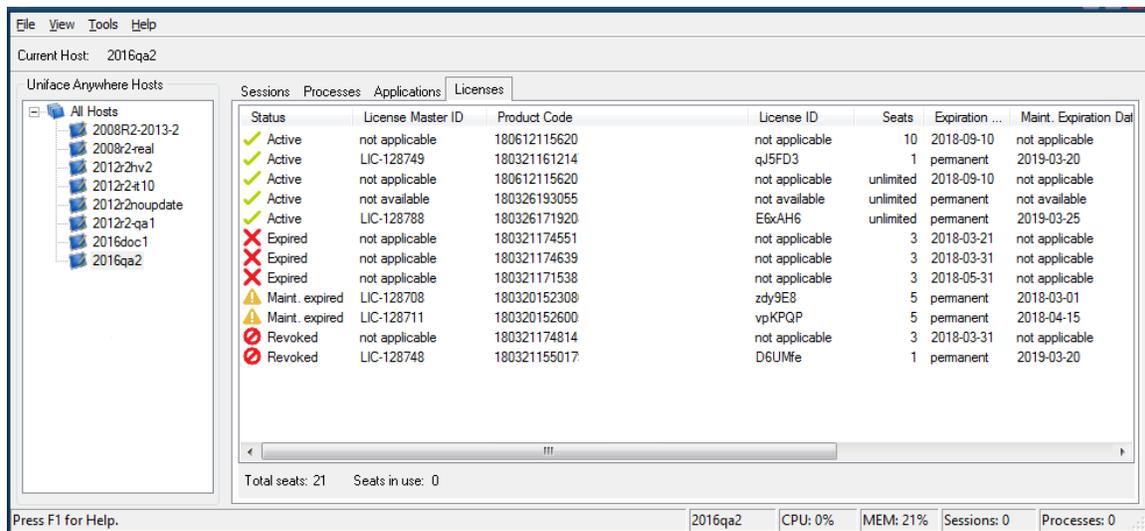
1. From the Admin Console, select the appropriate host from the list of Uniface Anywhere Hosts.
2. Click the **Licenses** tab.

For each license, the following information is displayed:

Column	Description
Status	A license status can be listed as <i>Active</i> , <i>Expired</i> , <i>Expires soon</i> , <i>Maint. Expired</i> , <i>Maint. Expires soon</i> , <i>Old version</i> , <i>Revoked</i> , and <i>Trial</i> .
License Master ID	Uniface's record of the license (e.g., LIC-122689)
Product Code:	28-digit alphanumeric code that appears in the license file, uniquely identifies the license, and is used for secure transactions (e.g., 171205182219607CJs4ndny07Auu)
License ID	Unique, encoded alphanumeric ID representing the license file (e.g., GHPc7u with license file <i>GHPc7u.lic</i>)
Seats	The number of concurrent users the license allows. If there are no restrictions, seats will be <i>unlimited</i> .
Expiration Date	The date the license expires (a trial license, in most cases). When a license does not have an expiration date, the expiration date is listed as "permanent."
Maint. Expiration Date	The date the Support contract expires.
Features	Type of license (e.g., <i>session</i> or <i>strong encryption</i>)
Version	The license's Uniface Anywhere version number (e.g., 5.0 and 6.0)
License Server	The name of the license server that the host is using

Depending on which column is selected, licenses are sorted alphanumerically in ascending order. Click the column header to sort in descending order.

At the bottom of the Licenses tab, Uniface Anywhere displays the number of **Total seats** for all the valid licenses listed for the selected computer. It also displays the number of **Seats in use**, which is the number of seats currently checked out from the licenses listed, and includes licenses that have been checked out from the selected computer and from any other Uniface Anywhere Host that is using the same license(s).



A **session license** is a license available to a Uniface Anywhere Host that authorizes one or more users to start Uniface Anywhere sessions on a host.

A **strong encryption license** is delivered in a separate license file and provides the following additional encryption algorithms: **128-bit RC4**, **168-bit 3DES**, and **256-bit AES**. The strong encryption license is a per server license, and not based on the number of concurrent users. To obtain a strong encryption license, contact your Uniface Anywhere Sales Representative or mail to license.management@uniface.com.

Customers with a valid Uniface Anywhere Support contract are able to receive technical support for issues that occur on the licensed host. When the Support contract has expired (as indicated in the **Maint. Expiration Date** column), only critical Uniface Anywhere Updates can be installed on the host. Non-critical Uniface Anywhere Updates cannot be installed, and customers are not eligible to request support. Expiration warnings begin to appear 30 days before the expiration date and appear once every 7 days. You can opt to disable expiration warnings by checking **Don't display this message again**.

If a Uniface Anywhere Update was released after the Support contract on *any* of the licenses available to a Uniface Anywhere Host have expired, you must renew the Support contract in order to install the update on the host. If an update was released after the Support contract has expired on some, but *not all* licenses, you can either remove the license(s) with the expired Support contract, or you can renew the expired Support contract(s).

Contact your Uniface Anywhere Sales Representative to renew Support contracts.

Note: If the expiration date of the Support contract for any license available to a Uniface Anywhere Host is earlier than the build date of the Uniface Anywhere Host, the **Application Publishing Service** will not run.

For trial licenses of Uniface Anywhere, the License Master ID, License ID, and the Maintenance Expiration Date will be listed as *not applicable*. The **Expiration Date** column indicates the date that the trial will stop working. When a trial license status has *expired*, users are no longer able to run Uniface Anywhere on that computer. Extend the Uniface Anywhere trial license by contacting your Uniface Anywhere Sales Representative.

If a license is listed as *Revoked*, it is invalid, and must be removed from the system, and the Application Publishing Service must be restarted. Contact your Uniface Anywhere Sales Representative for further assistance. If a license is listed as *Old version*, the version of the license is older than the license version required by the host. If it is the only license on the host, it will need to be upgraded. It does not need to be removed for other licenses to work.

Note: To refresh the list of licenses, right-click and select **Refresh** or press the **F5** button on the keyboard.

For more detailed information about Uniface Anywhere licensing, see the *Appendix*.

Security Options

Through the **Security** tab of the **Host Options** dialog, administrators can select the transport mode of communication between clients and the Uniface Anywhere Host and select the level of encryption for data transmitted between client and host. Administrators can also modify the host port setting and enable Integrated Windows authentication and password caching.

Selecting SSL Transport

Uniface Anywhere provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between Windows and Uniface Anywhere Hosts. When selecting the SSL transport, an SSL Certificate file must be specified. SSL certificates are required to secure communication between Uniface Anywhere clients and hosts.

You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. Wildcard SSL certificates are also supported. For more information, see [Obtaining a Trusted Server Certificate](#).

To select SSL Transport

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, click SSL.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

Note: When SSL Transport is selected, HTTPS must be enabled on the web server if users will be accessing the Uniface Anywhere Host via a web browser.

When a relay server is used:

- The certificate must be installed on the relay server but does not need to be installed on the dependent hosts.
- On the dependent hosts, the value in the **Relay server** field on the **General** tab of the **Host Options** dialog must match the certificate's Common Name.

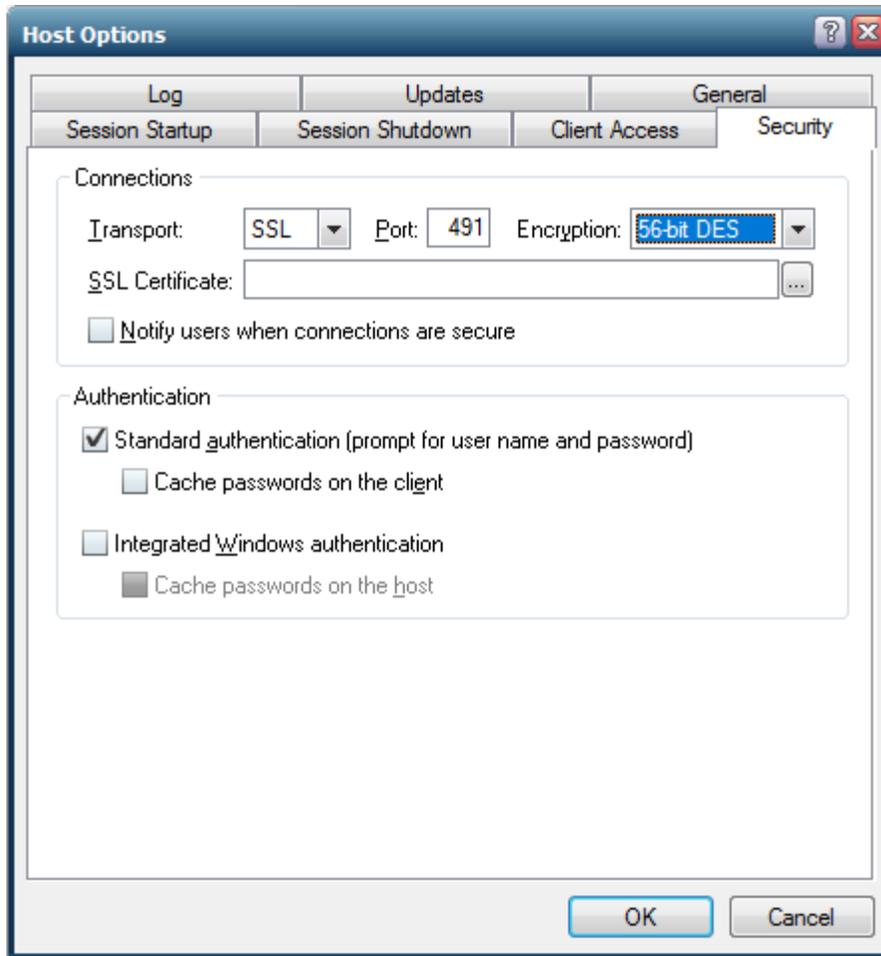
Modifying the Host Port Setting

In order for users to access Uniface Anywhere through a firewall or router, administrators are able to modify the host port setting for the Application Publishing Service. The Application Publishing Service must be running on a dedicated port. Conflicts may arise if another service is running on the same port. The default port number for both TCP and SSL is 491.

To modify the Host Port setting

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Security** tab.
4. Type a new port number in the **Port** box.
5. Click **OK**.

The port can only be set to 443 if there is no web server on the computer configured to accept HTTPS connections. (Web servers accept HTTPS connections on port 443.) If the **Note:** **Uniface Anywhere Application Publishing Service** must accept connections on port 443 (to allow connections through proxy servers, for example), the web server must be run on a different computer.



After modifying the host port setting, you will need to append the **port** parameter to the logon page. Use the port parameter followed by the new port number.

For example, **`http://hostname/UAnywhere/logon.html?port=1667`**

Users running Uniface Anywhere from a shortcut will need to append the `-hp` argument (followed by the new port number) to the shortcut.

For example, `"C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -h server1 -hp 1667`.

Users can also specify the port number in the **Connection** dialog when signing in to Uniface Anywhere. In the **Host Address** box, type the host name or IP address, followed by a colon and the port number. For example, `server1:1667`. If it's an IPv6 address, the IP address of the host must be in brackets. For example, `[fe80::29c:29ff:fe95:519a]:491`.

If the new port number is not specified by either of these methods, users will be unable to sign in to Uniface Anywhere.

Note: After changing the host port, you must restart the **Print Spooler Service** and the **Uniface Anywhere Application Publishing Service** in order for client printing to work on a port other than the default port 491.

Encrypting Sessions

For purposes of security, administrators can optionally encrypt all data transmitted between the client and the host. This includes the client's user name and password, which are supplied during logon, and any application data submitted by the client or returned by the host. When TCP transport mode is selected, Uniface Anywhere uses **56-bit DES** encryption. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits.

When SSL transport mode is selected, the following encryption algorithms are also available: **128-bit RC4**, **168-bit 3DES**, and **256-bit AES**. A special license is required to use these algorithms. To obtain this license, contact your Uniface Anywhere reseller.

To encrypt a host's sessions

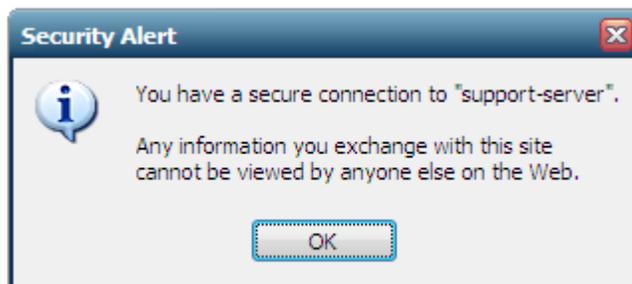
1. Click Tools | Host Options.
2. Click the **Security** tab.
3. From the **Encryption** list, select an encryption level.
4. Click **OK**.

After encryption is enabled, all succeeding Uniface Anywhere sessions will be encrypted. Sessions that are active when the feature is enabled will remain unencrypted. The next time the user signs in to the Uniface Anywhere Host, however, his or her session will be encrypted. The user must sign off the Uniface Anywhere Host, and sign back in for the session to be encrypted.

When encryption is enabled, all connections to that Uniface Anywhere Host use the selected transport and encryption algorithm, including connections from Admin Consoles, clients, and dependent hosts. When a relay server is used, Uniface Anywhere provides linked encryption. Specifically, the Application Publishing Service on the relay server decrypts the data it receives from the client and re-encrypts it before it forwards the data to the dependent host. Similarly, it decrypts the data it receives from the dependent host, and re-encrypts it before it forwards it to the client.

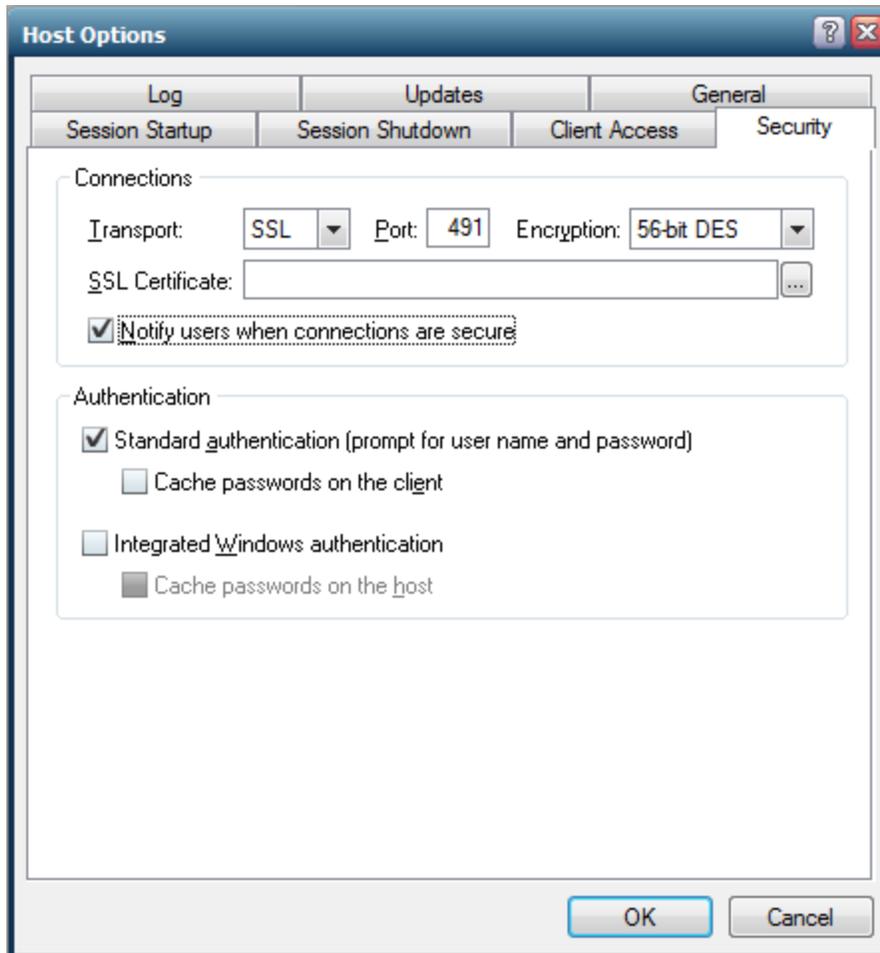
Notifying Users of a Secure Connection

When the SSL transport is selected, you can opt to notify users with a Security Alert when connections are secure.



To notify users when connections are secure

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, click SSL.
4. Type or browse to the path of the server's certificate file in the **SSL Certificate** box.
5. Click the **Notify users when connections are secure** option.
6. Click **OK**.



Obtaining a Trusted Server Certificate

To obtain a server certificate from a CA that is trusted by the client operating system, consult the documentation from the CA of your choice using the following information as a guide. The CA will require a Certificate Signing Request (CSR).

To generate a CSR

1. Download the latest version of OpenSSL from <https://www.openssl.org/source/>.
2. Install OpenSSL on the Uniface Anywhere Host.
3. Click Start | Run.
4. Type **cmd**, and press **Enter**.
5. Type the following command to generate a private key for the server:
`[OPENSSL_DIR]\bin\openssl genrsa -out server.key 2048`
where OPENSSL_DIR is the path to the directory in which OpenSSL is installed (e.g., C:\OpenSSL).
6. Type the following command:
`[OPENSSL_DIR]\bin\openssl req -sha256 -new -key server.key -out server.csr`

Running this command will prompt you for the attributes to be included in your certificate, as follows:

Country Name: US

State: your state

Locality: your city

Organization: your company name

Organizational Unit: your department

Common Name: your server's name

E-mail Address: your e-mail address

Unless you are using a wildcard SSL Certificate, the Common Name *must* match the host name of the Uniface Anywhere Host (i.e., the name that users will specify when connecting to the host). Any variation in the name will cause the client to issue a warning when connecting. The output of the above command will be a file named **server.csr**, which can be sent to your CA. Since Uniface Anywhere's SSL implementation is based on the OpenSSL toolkit, the tools used are the same as those used in other OpenSSL-based products, such as the Apache mod_ssl package. Follow instructions provided by your CA for the mod_ssl package to obtain a certificate for your server.

When your CA sends you the signed server certificate file, save it as **server.crt**. Copy this file and the **server.key** file (generated in step 5 above) to a directory on the Uniface Anywhere Host that can be accessed from the System account and accounts that belong to the Administrator group but that cannot be accessed from normal user accounts. Finally, select the signed certificate file in the Admin Console, as described below.

To select the server certificate

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, select **SSL**.
4. Type or browse to the path to the server's certificate (e.g., server.crt) file in the **SSL Certificate** box.
5. Click **OK**.

Uniface Anywhere requires that the certificate and its key be in PEM format. When requesting a certificate from a third-party CA, Uniface recommends requesting it in PEM format. If this is not possible and the certificate can only be delivered in DER format, it can be converted to PEM format using the following command:

```
openssl x509 -inform der -in MYCERT>cer -out MYCERT.pem
```

The resulting MYCERT.pem file can then be renamed to MYCERT.crt for use in Uniface Anywhere.

Using an Intermediary SSL Certificate with Uniface Anywhere

When using an intermediary SSL certificate with Uniface Anywhere, you must concatenate your existing certificate with the intermediary certificate. The following example uses the Go Daddy intermediary certificate.

1. Take the .crt and .key files that are being used on the Uniface Anywhere Host.
2. Download the Go Daddy intermediary certificate (e.g., GODaddyCA.crt). This should have come with the original certificate purchase but can also be located at the following Go Daddy site: <https://certs.godaddy.com/Repository.go>
3. Concatenate your .crt and the intermediary .crt file. (Combine them into a third file as follows: copy test_server.crt+GODaddyCA.crt server.crt.)
4. Rename the key file from step 1 to server.key so that it matches the newly created server.crt file.
5. Copy these two files onto the Uniface Anywhere Host (e.g., c:\Data).
6. Launch the Admin Console. Click Tools | Host Options. Click the **Security** tab.
7. Change the transport to SSL and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.
8. Browse to the SSL certificate server.crt in c:\data and click **OK**. You should not see an error message at this point if you have .crt and .key files with the same prefix.
9. Enable **Notify users when connections are secure** for testing purposes.
10. Click **OK**.
11. Start a Uniface Anywhere session from a different system.

Using an Intermediary SSL Certificate on iOS and Android

In order for the Uniface Anywhere App on iOS and/or Android to trust a server certificate, it must be able to trust the entire SSL certificate chain, including any intermediate certificates and all root certificates.

To make a server certificate that will provide the entire SSL certificate chain

1. Obtain all .crt files included in your certificates chain and .key files being used on the Uniface Anywhere Host.
2. Concatenate your .crt and all intermediate and root .crt files.
(Combine them into a final file as follows:
copy test_server.crt+intermediate.crt+root1.crt+root2.crt server.crt)

Note: There may be 0 or more intermediate files and 1 or more root files. If your .crt file is self-signed, you will just need to rename your .crt file to server.crt.

3. Rename the key file from step 1 to **server.key** so that it matches the newly created **server.crt** file.
4. Copy these two files onto the Uniface Anywhere Host (e.g., c:\Data).
5. Launch the Admin Console. Click Tools | Host Options. Click the **Security** tab.
6. Change the transport to **SSL** and increase the encryption level to 256-bit AES, if you have a high-encryption license. If not, leave it at 56-bit.
7. Browse to the SSL certificate **server.crt** in c:\data and click **OK**. You should not see an error message at this point if you have .crt and .key files with the same prefix.
8. Enable **Notify users when connections are secure** for testing purposes.
9. Click **OK**.
10. Start a Uniface Anywhere session from an iOS or Android device.

Standard Authentication

Standard authentication is the default method for authenticating users on a Uniface Anywhere Host. Standard authentication allows users to sign in to Uniface Anywhere via the **Sign In** dialog by typing their user name and password. Once authenticated, users are added to the host's INTERACTIVE group and given the same access rights as if they had signed in to the host at its console.

To enable Standard authentication

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. Click Standard authentication (prompt for user name and password).
4. Click **OK**.

Integrated Windows Authentication

Integrated Windows authentication allows users to connect to a Uniface Anywhere Host and start a session without having to sign in to the host and re-enter their user name and password. When Integrated Windows authentication is the only option enabled, the user's user name and password are never transmitted over the network. Instead, Uniface Anywhere simply runs the user's session in the same security context as the Uniface Anywhere Client. Users are added to the host's NETWORK group instead of its INTERACTIVE group. As a result, they may be denied access to some resources.

When users connect to a Uniface Anywhere Host using Integrated Windows authentication, they are able to access most of the same resources on the host that they would be able to access if they signed in to the host interactively. However, depending on the authentication protocols supported by the client's and host's operating systems and the network, when users access resources that reside on other computers on the network they might be required to re-enter their user name and password. If network resources are unable to request a user name and password, access might be denied.

In order to access other computers on the network, the Active Directory must be configured to allow authentication credentials to be passed to other computers. Microsoft refers to the right to pass authentication credentials to a third or more computers as "delegation." Delegation is supported on Active Directory networks with the proper settings. Please refer to your Microsoft Windows operating system documentation for instructions on properly configuring an Active Directory Domain Controller. See [Configuration Requirements for Delegation Support](#) in Chapter 6 for more information.

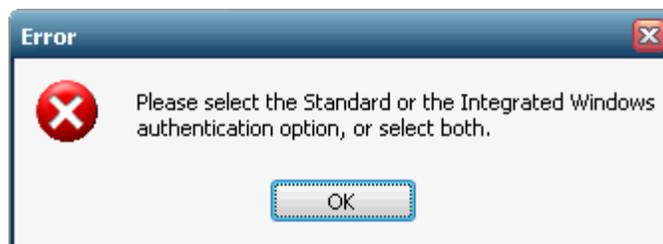
Note: The **Cache passwords on the host** option, described in the following section, can be enabled to obtain an INTERACTIVE group logon with Integrated Windows Authentication.

Integrated Windows authentication is available to users who sign in from Windows computers that are members of the same domain as the Uniface Anywhere Host and to users who sign in from Windows computers that are members of Trusted Domains of the Uniface Anywhere Host.

To enable Integrated Windows Authentication

1. Click Tools | Host Options.
2. Click the **Security** tab.
3. Enable Integrated Windows authentication.
4. Click **OK**.

Uniface Anywhere requires that either Standard authentication or Integrated Windows authentication be enabled. If neither one of these authentication methods is selected, and you click **OK** to close the dialog, the following error message is displayed:



If both Standard authentication *and* Integrated Windows authentication are enabled, the Uniface Anywhere Host will first attempt to log the user on via Integrated Windows authentication. If this fails, Uniface Anywhere will then attempt to log the user on with Standard authentication by presenting the **Sign In** dialog and requiring a user name and password.

Password Caching on the Host

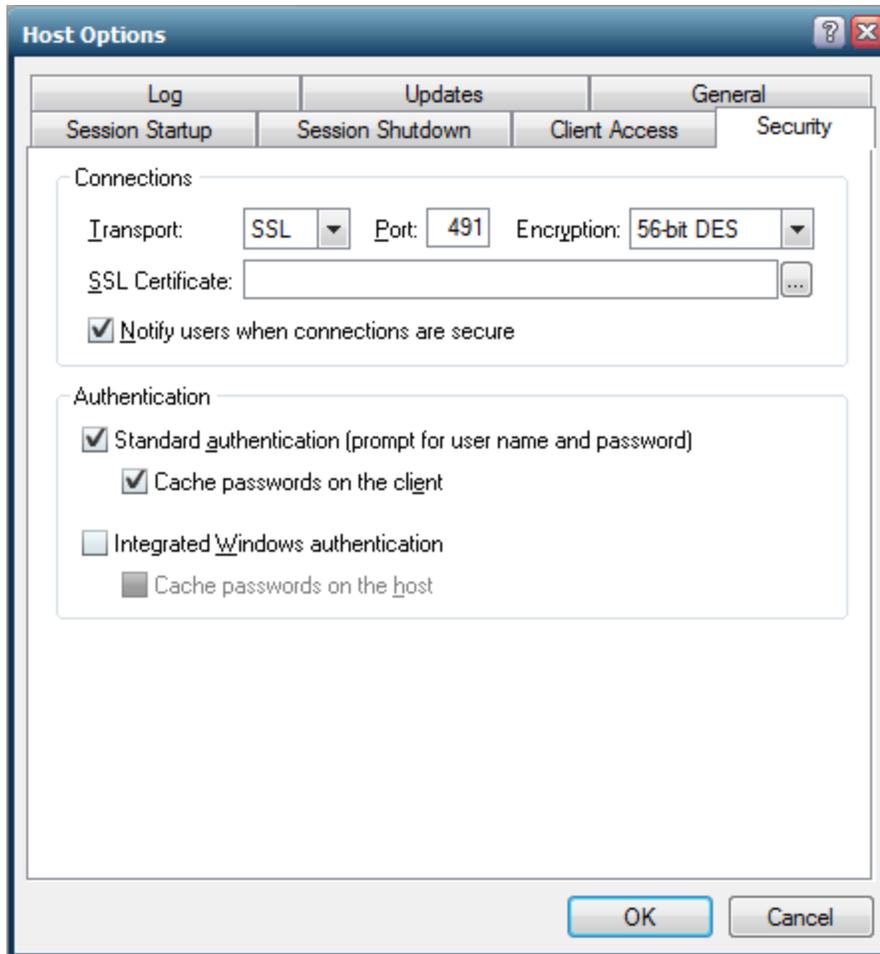
When a user signs in to a Uniface Anywhere Host with standard authentication (either with a user name and password supplied by the **Sign In** dialog, parameters, or command-line arguments), that user is added to the host's INTERACTIVE group. Alternatively, a user that signs in to a Uniface Anywhere Host using integrated Windows authentication is added to the host's NETWORK group. By default, members of the INTERACTIVE group have greater access to the host's resources than members of the NETWORK group. As a result, a user that signs in via Integrated Windows authentication may encounter "access denied" errors under a number of conditions.

Note: Areas restricted from members of the NETWORK group include DCOM (also known as OLE and COM/COM+) security limitations, file security limitations, and application specific security checking. Administrators should verify that all resources (files, services, etc.) that Integrated Windows authenticated users need to access have the proper security settings to allow that access.

To avoid these errors, administrators can enable the **Cache passwords on the host** option. Doing so allows users to sign in with full INTERACTIVE access rights without having to enter their user name and password every time they connect. Users are prompted for a password when first connecting to the host or following a password change. Passwords are encrypted and stored within their respective profiles. With subsequent connections to Uniface Anywhere, users are automatically signed in and added to the host's INTERACTIVE group. They are granted the same access rights had they signed in to the host at its console.

Uniface Anywhere encrypts passwords using an RSA algorithm with a 512-bit key that is stored on the host. The encryption key is stored in the %ALLUSERSPROFILE%\Uniface\Uniface Anywhere\ks\ks.dat file. Only members of the host's Administrators group and the SYSTEM account can read this file.

Note: In clusters of Uniface Anywhere Hosts where roaming profiles are used, the key file from one host needs to be copied to all hosts in the cluster.



Password Caching on the Client

Client-side password caching allows users who are not members of the Uniface Anywhere Host's domain to sign in to Uniface Anywhere without having to enter their user name and password every time they connect to the server. When **Cache password on the client** is enabled, the **Sign In** dialog includes a **Remember me on this computer** check box. If the user enables this, after the first manual authentication, the user's logon credentials are encrypted on the host, transmitted over the network, and stored on client computers in user-private directories.

When the user makes subsequent connections to the server, the cached password is transmitted back to the host, where it is decrypted. The **Sign In** dialog is displayed with the user name and password and with **Remember me on this computer** checked. If the user disables the **Remember me on this computer** option, the user's credentials will be deleted from the client computer.

Uniface Anywhere caches passwords on the client using an RSA algorithm with a 512-bit key that is stored on the host. The encryption key is stored in the %ALLUSERSPROFILE%\Uniface\Uniface Anywhere\ks\ks.dat file. Only members of the host's Administrators group and the SYSTEM account can read this file.

Note: In clusters of Uniface Anywhere hosts, the key file from one host needs to be copied to *all* hosts in the cluster.

To enable client-side password caching

1. From the Admin Console click Tools | Host Options.
2. Click the **Security** tab.
3. Enable Standard authentication (prompt user for user name and password).
4. Enable Cache passwords on the client.
5. Click **OK**.

On most platforms, the cached password is stored in the user's home directory in a .dat file named for the Uniface Anywhere Host. The table below provides example locations of the cached password for each Uniface Anywhere Client. In the examples, user1 is the user name, server1 is the name of the Uniface Anywhere Host, and 192.168.100.111 is the IP Address of the Uniface Anywhere Host.

Platform	Password Locations
Mac OS X	/Users/user1/.ua-client/192.168.100.111.dat
Windows	\Users\user1\AppData\Roaming\Uniface\Uniface Anywhere
Linux	/home/user1/.ua-client/192.168.100.111.dat

Client-side password caching is supported on all Uniface Anywhere clients.

Password Change

Users can change passwords when:

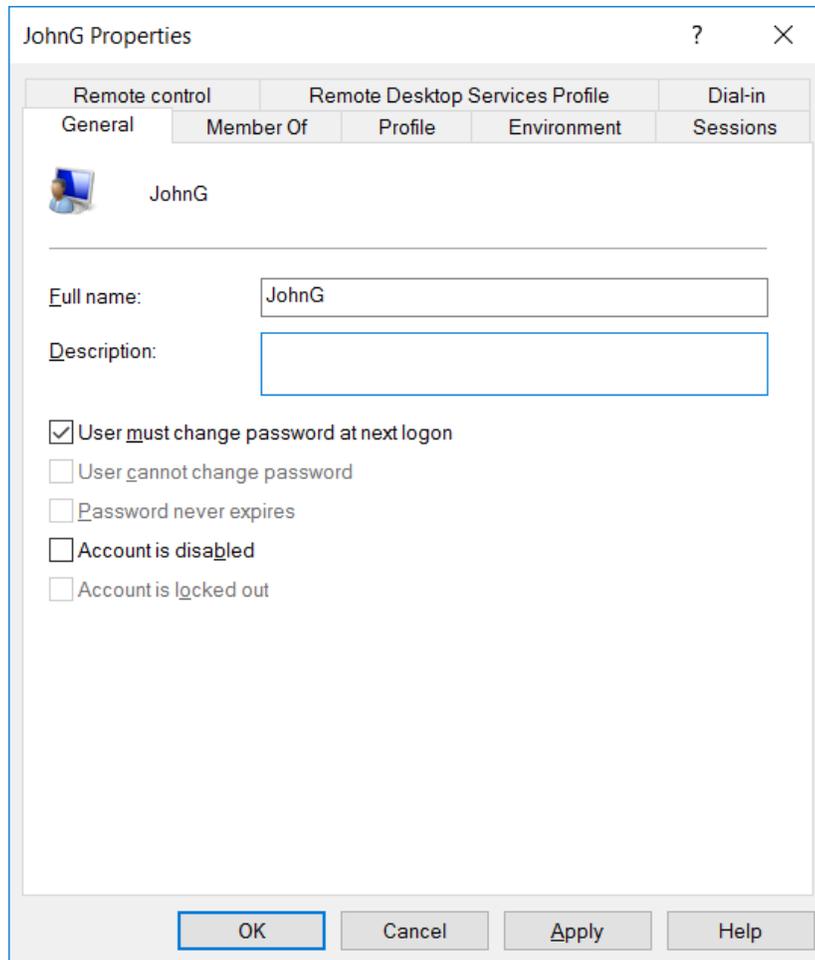
- a. The administrator requires the user to change his or her password at the next logon;
- b. The security policy is configured to prompt users to change passwords before expiration; and
- c. The user's password has expired.

Changing Passwords at Next Logon

Administrators can require a user to change his or her password by checking the **User must change password at next logon** option in the **Administrator Properties** dialog. (For Local accounts, this dialog can be accessed by clicking My Computer | Local Users and Groups | Users | *UserName* | Properties).

To sign in when the *User must change password at next logon* option is enabled for a user's account

1. Run the Uniface Anywhere client (e.g., browse to <http://hostname/UAnywhere/>).
2. Type the user name and password in the **Sign In** dialog. If the user account does not exist in the domain in which the Uniface Anywhere Host resides, include the domain name in the **User name** field as a prefix (e.g., domain\username).
3. Click **OK**.
4. Click **OK** to the following message: "You are required to change your password at first logon."
5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change password** dialog.
6. Click **OK**.



Prompting Users to Change Passwords Before Expiration

By default, users are prompted to change their passwords whenever they log on within 14 days of their password's scheduled date of expiration. Administrators can modify the change password "prompt" period by editing the **Prompt user to change password security** setting. For example, the local security setting can be viewed and changed by clicking Start | Control Panel | Administrative Tools | Local Security Policy | Local Policies | Security Option.

To sign in during the password change "prompt" period

1. Run the Uniface Anywhere client (e.g., browse to <http://hostname/UAnywhere/>).
2. Type the user name and password in the **Sign In** dialog.
3. Click **OK**.
4. The following message is displayed:
"Your password will expire in x day(s). Do you want to change your password now? Yes/No"
If the user clicks **No**, the Uniface Anywhere session will start. If **Yes**, the **Change Password** dialog is displayed.
5. Type a new password in the **New Password** and **Confirm New Password** fields.

Prompting Users to Change Passwords After Expiration

To sign in after a password has expired

1. Run the Uniface Anywhere client (e.g., browse to `http://hostname/UAnywhere/`).
2. Type the user name and password in the **Sign In** dialog. If the user account does not exist in the domain in which the Uniface Anywhere Host resides, include the domain name in the **User name** field as a prefix (e.g., `domain\username`).
3. Click **OK**.
4. Click **OK** to the following message: “Your password has expired and must be changed.”
5. Type a new password in the **New Password** and **Confirm New Password** fields of the **Change Password** dialog.
6. Click **OK**.

Password Change and Integrated Windows Authentication

When Integrated Windows Authentication is enabled, Uniface Anywhere relies on the operating system of the client to change passwords. For example, Uniface Anywhere supports the following scenario:

1. The administrator edits a user's settings and specifies that the **User must change password at next logon**.
2. Upon logging on, the user is prompted to change his or her password.
3. The user changes the password and signs in to the client computer.
4. The user starts the Uniface Anywhere client and connects to a Uniface Anywhere Host.
5. The password has already been changed, so the user is authenticated on the host without being prompted for a password, unless the **Cache passwords on the host** option is enabled. In this case, the user will be prompted to enter a new password.

If, however, the administrator specifies that the **User must change password at next logon** after the user has logged on to the client computer, and the user subsequently connects to a Uniface Anywhere Host that has Integrated Windows authentication enabled, authentication may fail. If it fails and both the **Integrated Windows authentication** and **Cache passwords on the host** option are enabled, the user will be prompted to sign in and make a password change as described above.

Note:

In the Admin Console's dialog boxes, you can easily get Help by right-clicking an item, and then clicking **What's This?** A pop-up window will appear, displaying a brief explanation of the item. You can also get Help by clicking  on the title bar of a dialog box and then selecting an item.

Session Reconnect

Session reconnect allows sessions to be maintained on a Uniface Anywhere Host without a client connection. If the client's connection to the host is lost, intentionally or unintentionally, the user's session and applications remain running on the Uniface Anywhere Host for the length of the session timeout specified in the Admin Console. Session reconnect allows users to return to their Uniface Anywhere session in the exact state they left it. Through the Program Window users can select to disconnect, rather than exit from Uniface Anywhere, and can return to their session as they left it — without having to shut down their open applications and running processes.

If the network connection is lost or if users unintentionally disconnect from Uniface Anywhere, their session state is preserved for the length of time specified in the Admin Console. After a user is authenticated through normal logon procedures, Uniface Anywhere determines if the user has an active session. If so, that session resumes and appears exactly as it did prior to disconnection. If not, a new session is started. Users are also able to disconnect from one client and reconnect to the session from another client.

When attempting to reconnect to a disconnected session, users are required to specify their logon credentials. After the host validates them, the host reconnects them to the disconnected session. If the session is hosted on a server that is part of a load-balanced configuration, the user is routed to his or her session without any indication that the session is on a load-balanced server. If Integrated Windows authentication is available, users are automatically re-authenticated and re-connected to their session.

Setting the Session Termination Option

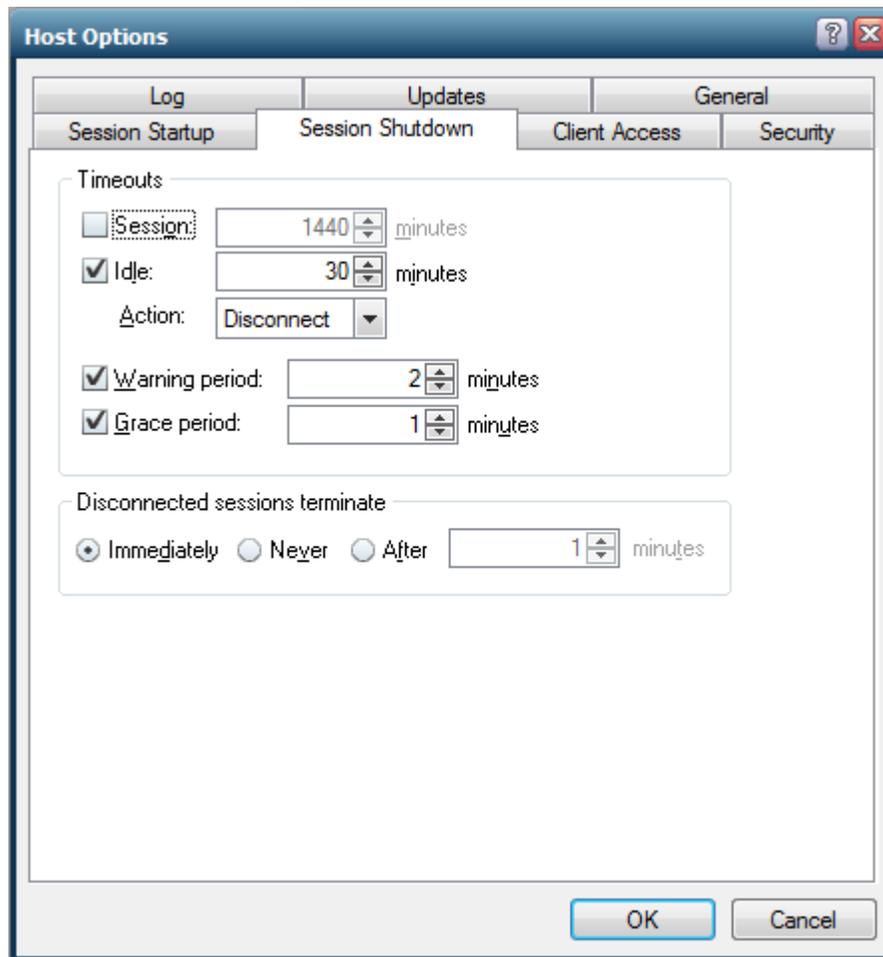
Administrators control how long client sessions and applications remain running on the Uniface Anywhere Host through the Admin Console's **Host Options** dialog.

- Select **Immediately** if you want client sessions to terminate as soon as the client disconnects.
- Select **Never** if you want sessions to terminate only when a user manually closes all applications running within a session or when an administrator manually terminates a session using the Admin Console. This is the default setting.
- Select **After __ minutes** to specify the number of minutes that a session will remain running after a client has disconnected from the session. Type the number of minutes in the edit field that a session should remain running after the client disconnects.

The **Sessions** tab of the Admin Console displays the number of clients connected to a session. Disconnected sessions have 0 connected clients.

To set the session termination option

1. From the Admin Console, click Tools | Host Options.
2. Click the Session Shutdown tab.
3. Select one of the following session termination options:
 - Immediately**
 - Never**
 - After ___ minutes.** In the edit box, type the number of minutes sessions should remain running after their clients disconnect.
4. Click **OK**.

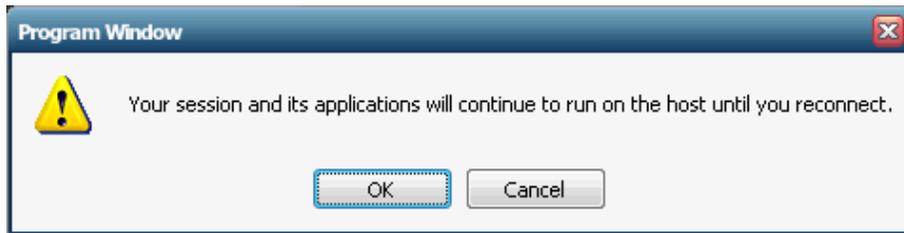
**Disconnecting a Session**

If sessions are set to never terminate or to terminate after a specified number of minutes, the Program Window's File menu includes a **Disconnect** option. If sessions are set to terminate immediately, the Disconnect option does not appear in the Program Window's File menu.

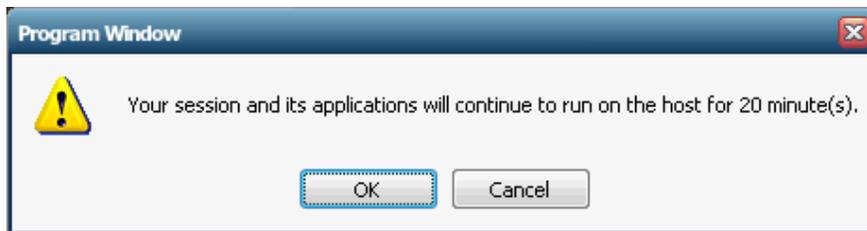
To disconnect a session

From the Program Window, click File | Disconnect.

With session termination set to **Never**, the following message is presented to the user upon disconnecting from Uniface Anywhere:



When sessions are set to terminate after a specified number of minutes (20 minutes, for example) a message such as the following is presented to the user upon disconnecting from Uniface Anywhere:



If a user attempts to disconnect from a session and already has a disconnected session, the following message appears:

*You already have a session (session_name) that is disconnected. If you disconnect the current session, that previous session will be terminated.
Do you want to continue?*

If the user clicks **Yes**, the disconnected session is terminated. If **No**, the user is returned to the running session.

Note: When a user reconnects to a session, the `-a` and `-r` command-line arguments are ignored. In addition, when the user reconnects to a session from the same client computer, the `-ac` command-line argument is ignored.

Shared Account

A shared account should be specified when multiple users are using the same account for starting a Uniface Anywhere session. Users who sign in to Uniface Anywhere with a shared account cannot disconnect and then reconnect to Uniface Anywhere. This prevents a user from reconnecting to another user's session.

When logging on to a Uniface Anywhere Host with a shared account, the **Disconnected sessions terminate** option in the Admin Console is ignored, and the behavior is determined by the **SessionTimeoutBrokenConnection** property in the **HostProperties.xml** file. (HostProperties.xml is located in C:\ProgramData\Uniface\Uniface Anywhere).

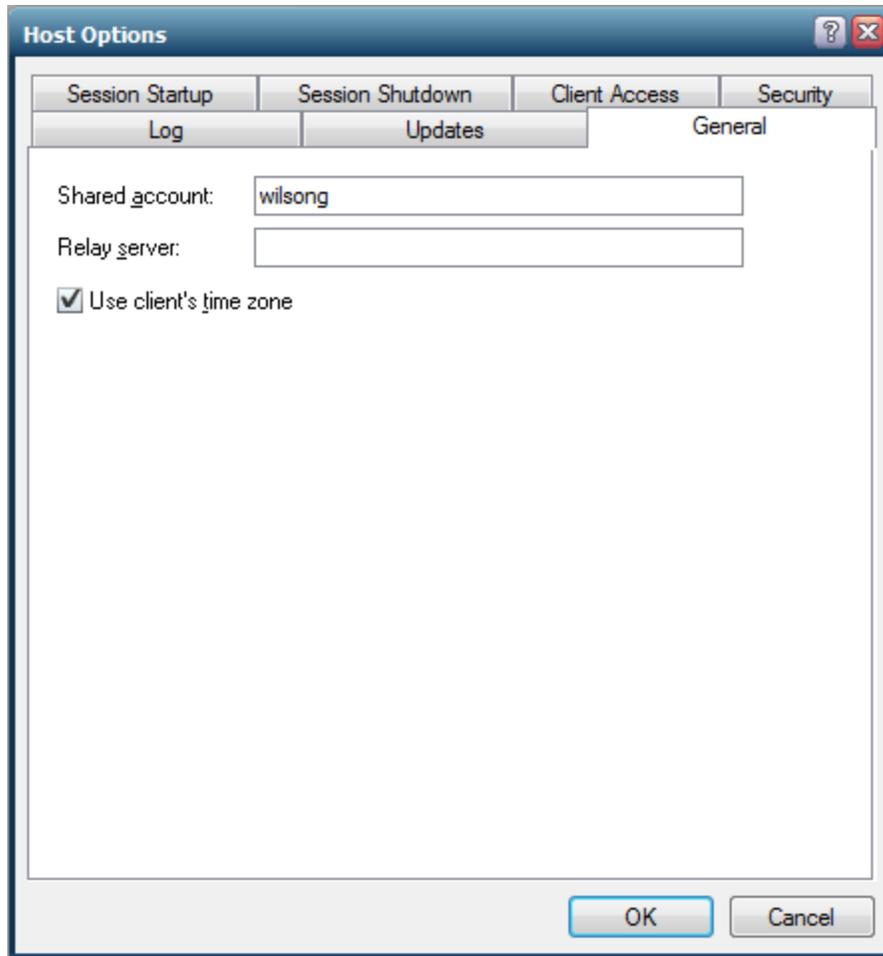
If the value of this property is set to 0, the session will terminate immediately. If the value is greater than zero, the session will be suspended and will remain running on the server for the number of minutes specified. In the latter case, only the user who started the session will be able to reconnect to the suspended session. By default, **SessionTimeoutBrokenConnection** is set to 0 minutes.

To specify a shared account

1. Click Tools | Host Options.
2. Click the **General** tab.
3. Type the user name of the shared account in the **Shared account** edit box. If multiple shared accounts are required, separate the user names of the accounts with semicolons.
4. Click **OK**.

If an administrator designates an existing user name as a shared account while that user is disconnected from his or her session, the session will remain running on the server until the termination limit has been reached. The session will then be terminated. Before specifying a shared account, verify in the Admin Console that there are no connected or disconnected sessions using that account.

Uniface Anywhere does not support the use of domain names (for example, NORTH\johng) for shared accounts.



Client Time Zone

By default, all Uniface Anywhere sessions are run in the time zone of the Uniface Anywhere Host machine. Administrators can opt to run Uniface Anywhere sessions in the time zone of the client computer by enabling the **Use client's time zone** option from the Admin Console.

To enable client time zone

1. Click Tools | Host Options.
2. Click the **General** tab.
3. Enable Use client's time zone.
4. Click **OK**.

Monitoring Host Activity

The Admin Console displays information about host activity and processes taking place on the host. Administrators can use this information to determine which applications are no longer being used and whether additional hosts are required, for example.

Viewing Session Information

The Admin Console displays the following session information:

Column	Displays the...
Session Name	Unique identifier assigned to a session.
User	Network user name of the user accessing applications on the host.
Connected Clients	Number of clients connected to a session. 0 indicates that no one is connected to the session (the client has disconnected). 1 indicates that the client is connected and the session is active. 2 or higher indicates that the session is being shadowed.
IP Address	IP address of the client computer from which the user is accessing the host. (Each computer on a network has a unique IP address.)
Startup Time	Date and time the user started the application.
Applications	Number of applications the user is accessing.

To view session information

Click the **Sessions** tab.

Note: Click the **All Hosts** icon from the left panel of the Admin Console to view a list of all active sessions on the network. This allows you to view active Uniface Anywhere sessions without connecting to individual hosts.

Viewing Process Information

A process refers to the specific application that a user is running from the host. The Admin Console displays the following process information:

Column	Displays the...
Name	Name of the application running on the host.
User	Network user name of the user accessing the application.
Startup Time	Date and time the user started the application.
Process ID	Process identification number assigned by the host's operating system. (The number for each running application matches the process identification number displayed in the Windows Task Manager.)

To view process information

Click the **Processes** tab.

Refreshing the Admin Console

You can manually update the sessions, processes, and applications information displayed in the Admin Console or you can set it to update automatically. If the Admin Console is set to update automatically, you can still update it manually at any time.

To refresh the Admin Console

Click View | Refresh.

Setting the Refresh Rate

You can set the sessions, processes, and applications tabs of the Admin Console to manually refresh or to automatically refresh at a specified frequency.

To set the refresh rate to allow only manual refresh

1. Click View | Options.
2. Click **Manual**.



To set the refresh rate to refresh automatically

1. Click View | Options.
2. Click the Refresh every x seconds option.
3. Type a value in the **seconds** box.

The Status Bar

The Status Bar is displayed at the bottom of the Admin Console window. The Status Bar provides brief descriptions of menu commands when the mouse pointer is placed over that item in the menu. The Status Bar indicates the name of the Uniface Anywhere Host currently being accessed, as well as the Mem usage and CPU utilization for that host, as calculated by the Windows Task Manager.

The last two items on the Status Bar, **Sessions** and **Procs** indicate the number of sessions and the number of processes running on the active Uniface Anywhere Host.

If **All Hosts** is selected, the **Sessions** number will reflect all the sessions running on the network, and the **Procs** number will reflect all the processes on the network.

To turn the Status Bar on or off

1. Click View | Options.
2. Select or clear the **Status Bar** check box.

Setting the Broadcast Interval

You can modify how often host information is sent to the Admin Console by modifying the Broadcast Interval value. This value represents how many milliseconds elapse between broadcasts, affecting how often a host's CPU, MEM, Sessions, and Processes status bars are updated, and how long it will take a host to appear in the list of **All Hosts**. The broadcast is sent via UDP and has a packet size of approximately 25-37 bytes.

To set the broadcast interval

1. Stop the **Application Publishing Service**.
2. Locate the **HostProperties.xml** file in the C:\ProgramData\Uniface directory.
3. Open **HostProperties.xml** in Wordpad and locate the following section:

```
</property>  
<property id="BroadcastInterval" group="Miscellaneous" type="UINT32">  
<value>300</value>  
</property>
```
4. Type the desired number of milliseconds for the value. (This value must be an integer greater than or equal to 1. Setting the value to 0 will prevent other Uniface Anywhere Hosts from being listed in the Admin Console. The default value for Broadcast Interval is 300.)
5. Start the **Application Publishing Service**.

Session Startup Options

Through the **Session Startup** tab of the Admin Console's **Host Options** dialog, administrators can enable startup options such as Group Policy, Progress Messages, and Logon Scripts. Administrators can also set various resource limits.

Applying Group Policy

Uniface Anywhere supports Microsoft's Group Policy. Using Group Policy and its extensions, administrators can manage registry-based policy, assign scripts, redirect folders, manage applications, and specify security options.

To apply Group Policy on a Uniface Anywhere Host

1. From the Admin Console, click Tools | Host Options.
2. Click Session Startup.
3. Select Apply Group Policy.
4. Click **OK**.

Note: It may take users longer to sign in to Uniface Anywhere when Group Policy is enabled.

Displaying Progress Messages

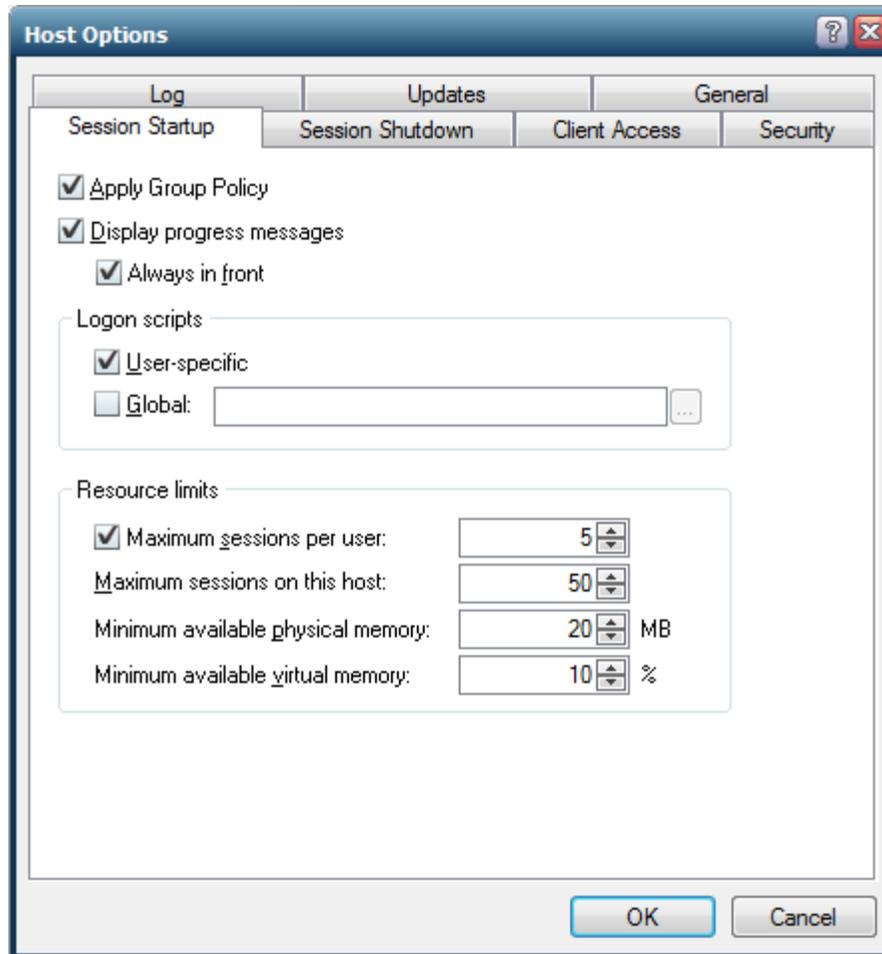
After a user is authenticated, a dialog that reports session startup progress can be displayed to users. When enabled, these messages inform users of the following:

- When their personal settings are being loaded
- When Group Policy is being applied
- When network drives are being connected
- When logon scripts are being run

To display session startup progress messages to users

1. From the Admin Console, click Tools | Host Options.
2. Click Session Startup.
3. Select Display progress messages.
4. To ensure that messages are displayed in front of all other windows, select **Always in front**.
5. Click **OK**.

Note: If a logon script has the ability to display user interface to the user, the **Always in front** option should not be enabled. Otherwise, the logon script's user interface may be partially obscured by the progress message.



Logon Scripts

Logon scripts allow administrators to configure the operating environment for Uniface Anywhere users. Scripts may perform an arbitrary set of tasks such as defining user-specific environment variables and drive letter mappings.

Uniface Anywhere supports two types of logon scripts: global scripts that execute for all users that sign in to the host, and user-specific scripts that execute for individual users. Before loading the user's profile and launching the Program Window, Uniface Anywhere's Logon Manager checks to see if a script of either (or both) type has been specified. If so, the Logon Manager runs the script(s) within the user's security context each time the user is authenticated.

User-specific logon scripts are specified using the functionality provided by the operating system. For example, the logon script for local users on a Windows Server 2016 is specified as follows:

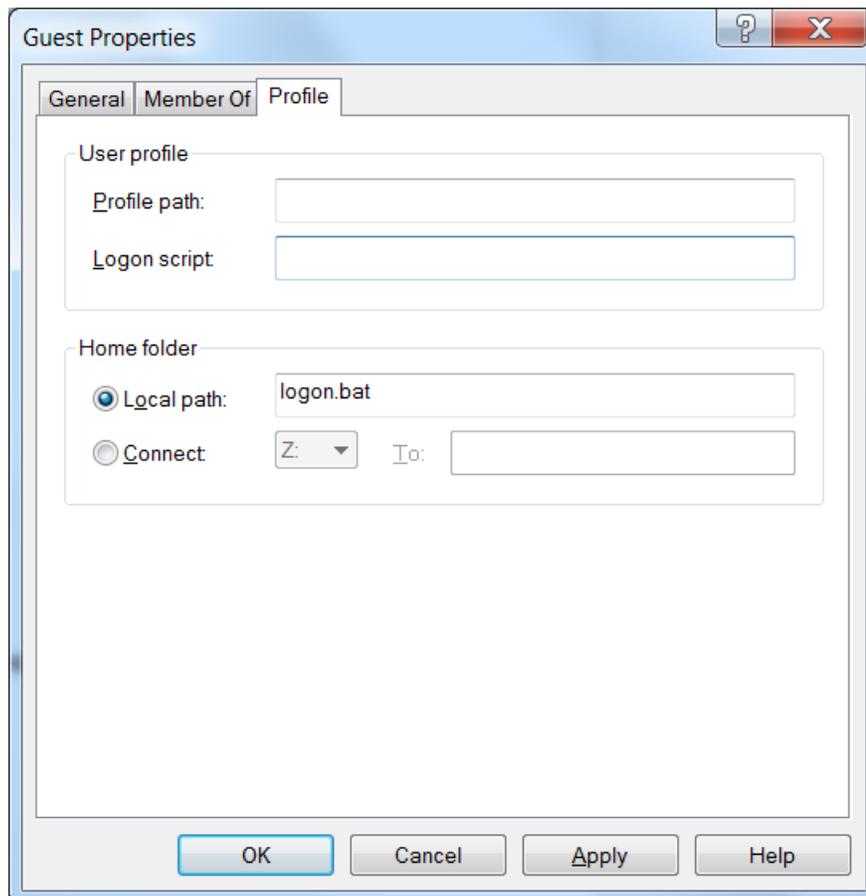
1. From the Control Panel, navigate to Administrative Tools | Computer Management | Local Users and Groups | Users.
2. Select a user and click **Properties**.
3. Click Profiles.
4. In the **Logon script** box, type the file name of the user's logon script.

If the value entered in the **Logon Script** box specifies a file name and extension only, Uniface Anywhere searches for the file in the following directories, in the following order:

1. If the user's account is a domain account:
 - a. `\\pdcname\NETLOGON`, i.e., the NETLOGON share of the primary domain controller.
 - b. `\\pdcname\SYSVOL\domainname`, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.

2. If the user's account is a local account:
 - a. `systemroot\System32\Repl\Import\Scripts`
 - b. `systemroot\sysvol\sysvol\domainname`

If the logon script is stored in a subdirectory of one of the above directories, precede the file name with the relative path of that subdirectory. For example, `Admins\JohnG.bat`.



Administrators specify global and user-specific logon scripts through the Admin Console's **Session Startup** dialog.

To run user-specific logon scripts

1. From the Admin Console, click Tools | Host Options.
2. Click Session Startup.
3. Select User-specific.
4. Click **OK**.
- 3.

To run a global logon script

1. From the Admin Console, click Tools | Host Options.
2. Click Session Startup.
3. Select **Global** and specify the path of the global script file.
4. Click **OK**.

Note: Authenticated users must have read and execute access to the logon script files.

If a logon script fails to execute, an error message is displayed. Check the location of the logon script.

If the user's account is a **domain** account:

- a. `\\pdcname\NETLOGON`, i.e., the NETLOGON share of the primary domain controller.
- b. `\\pdcname\SYSVOL\domainname`, i.e., the domain subdirectory of the primary domain controller's SYSVOL share.

If the user's account is a **local** account:

- a. `systemroot\System32\Repl\Import\Scripts`
- b. `systemroot\sysvol\sysvol\domainname`

Additional tools such as DebugView, available from <https://technet.microsoft.com/en-us/sysinternals/bb896647.aspx> can help track the cause of the problem when these errors occur. Open the DebugView executable on the host and check for any errors that point to the incorrect location of the script.

Note: Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.

Setting Resource Limits

Uniface Anywhere allows administrators to prevent users from starting new sessions when certain resource limits are exceeded on a Uniface Anywhere Host. These limits help administrators prevent hosts from becoming loaded to the point where users experience performance problems and random resource allocation failures.

To limit the number of sessions per user

1. From the Admin Console, click Tools | Host Options.
2. Click Session Startup.
3. Select **Maximum sessions per user** and enter the maximum number of sessions per user in the edit box.
4. Click **OK**.

Specifying the Maximum Number of Sessions

The maximum number of sessions that can be supported from a given host is set to 50 by default. Administrators should adjust this value to one that is appropriate for the capacity of the host.

To edit the maximum number of sessions per host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Session Startup** tab.
4. Edit the number in the **Maximum sessions on this host** box. This will set the limit for the number of sessions the host can support. For example, if the maximum number of sessions is 11, the user who initiates the twelfth session will be prevented from logging on.
5. Click **OK**.

In a relay server setting, Uniface Anywhere checks the maximum sessions setting on the relay server and its dependent hosts. The **Maximum sessions on this host** value designated on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server.

Specifying the Minimum Physical and Virtual Memory

To prevent users from logging on when the available physical memory on a host falls below a given value, enter the value in the **Minimum available physical memory** edit box.

To prevent users from logging on when the available virtual memory on a host falls below a given value, enter the value in the **Minimum available virtual memory** edit box.

Session Shutdown Options

Through the Admin Console, administrators can specify time limits for the number of minutes of client idle time and the number of minutes that sessions are allowed to run on a host. Administrators can also specify whether the user is either disconnected or logged off when the idle limit is reached, and when to display warning messages to users about to be disconnected or logged off. Administrators can also designate a grace period during the log off period to allow users to save files and close applications, etc.

Specifying the Session Limit

The session limit is the number of minutes that a session is allowed to run on a Uniface Anywhere Host.

To specify the session limit

1. From the Admin Console, click Tools | Host Options.
2. Click the Session Shutdown tab.
3. Enable **Session**.
4. In the edit box, type the number of minutes that a session is allowed to run on a host before its user is logged off.
5. Click **OK**.

The minimum amount of session time is 1 minute and the maximum is 44640 minutes (31 days). This feature is disabled by default.

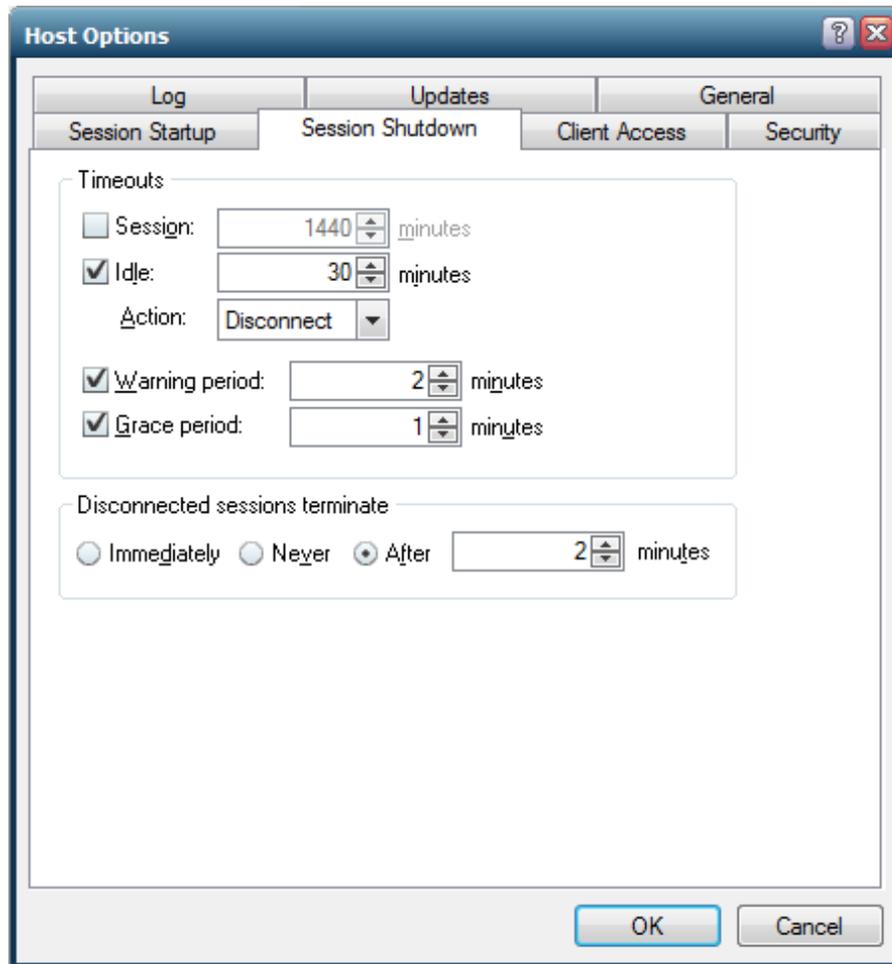
Specifying the Idle Limit

Idle time refers to the number of minutes since the last mouse or keyboard input event was received in a session. The idle limit is the number of minutes of idle time that a Uniface Anywhere Host allows.

To specify the idle limit

1. From the Admin Console, click Tools | Host Options.
2. Click the Session Shutdown tab.
3. Enable **Idle**.
4. In the edit box, type the number of minutes of idle time allowed by the host.
5. From the **Action** list, click **Disconnect** to disconnect users when the idle limit has been reached or click **Log off** to log users off when the idle limit has been reached.
6. Click **OK**.

The minimum amount of idle time is 1 minute and the maximum is 44640 minutes (31 days). The idle time is set to 30 minutes by default.



Specifying the Warning Period

The warning period refers to the number of minutes before a session limit or idle limit is reached when users are warned they are about to be disconnected or logged off. For example, if the warning period is set to 2, users will be warned 2 minutes before the session limit or the idle limit is reached. This feature is disabled by default.

To specify the warning period

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Warning period**.
4. In the edit box, type the number of minutes before a session or idle limit is reached when users are warned that they are about to be disconnected or logged off.
5. Click **OK**.

Note: The warning period must be less than the session limit and idle limit settings.

Specifying the Grace Period

The grace period refers to the number of minutes after a logoff begins during which users may save files, close applications, etc. Grace period is enabled and set to one minute by default. The minimum grace period value is one minute and the maximum value is 15.

To specify the grace period

1. From the Admin Console, click Tools | Host Options.
2. Click **Session Shutdown**.
3. Enable **Grace period**.
4. In the edit box, specify the number of minutes after a logoff begins that users are able to save files and close applications, etc.
5. Click **OK**.

Windows Compatibility Assurance

To provide multi-user remote access on all versions of Windows, Uniface Anywhere must access internal functions and data structures in Windows. When a computer running the Uniface Anywhere Host starts, Uniface Anywhere analyzes some of the operating system's binary files and automatically identifies the addresses of the operating system functions and variables that Uniface Anywhere requires.

In most cases, Uniface Anywhere is able to identify the required operating system addresses regardless of the version of Windows and the Windows Updates that are installed on the computer. In rare cases, however, Windows Updates include changes to the operating system that either prevent Uniface Anywhere from locating a required address or are incompatible with Uniface Anywhere's interface to the operating system. When this happens, Uniface Anywhere is unable to start sessions on a computer. To prevent this from occurring, Uniface Anywhere v6 provides **Windows Compatibility Assurance**.

The **Windows Compatibility Assurance** feature gives administrators the option to automatically defer installation of Windows Updates until Uniface has verified that the updates are compatible with Uniface Anywhere. To do this, Uniface continuously monitors Microsoft's Windows Update service for new updates. When Microsoft releases one or more Windows Updates, Uniface Anywhere suspends installation of all Windows Updates on affected Uniface Anywhere hosts until Uniface has verified that the newly released Windows Updates are compatible.

Note:

To ensure Uniface Anywhere Hosts do not download newly released Windows Updates during the short window of time between when Microsoft releases a new update and Uniface detects that the update has been released, Uniface Anywhere controls when Windows Updates can be installed on Uniface Anywhere Hosts. On Windows 10 and later, Uniface Anywhere delays Windows Updates by the number of days specified by the value of the **DelayWindowsUpdates** property in the HostProperties.xml file. (This is set to 1 day, by default).

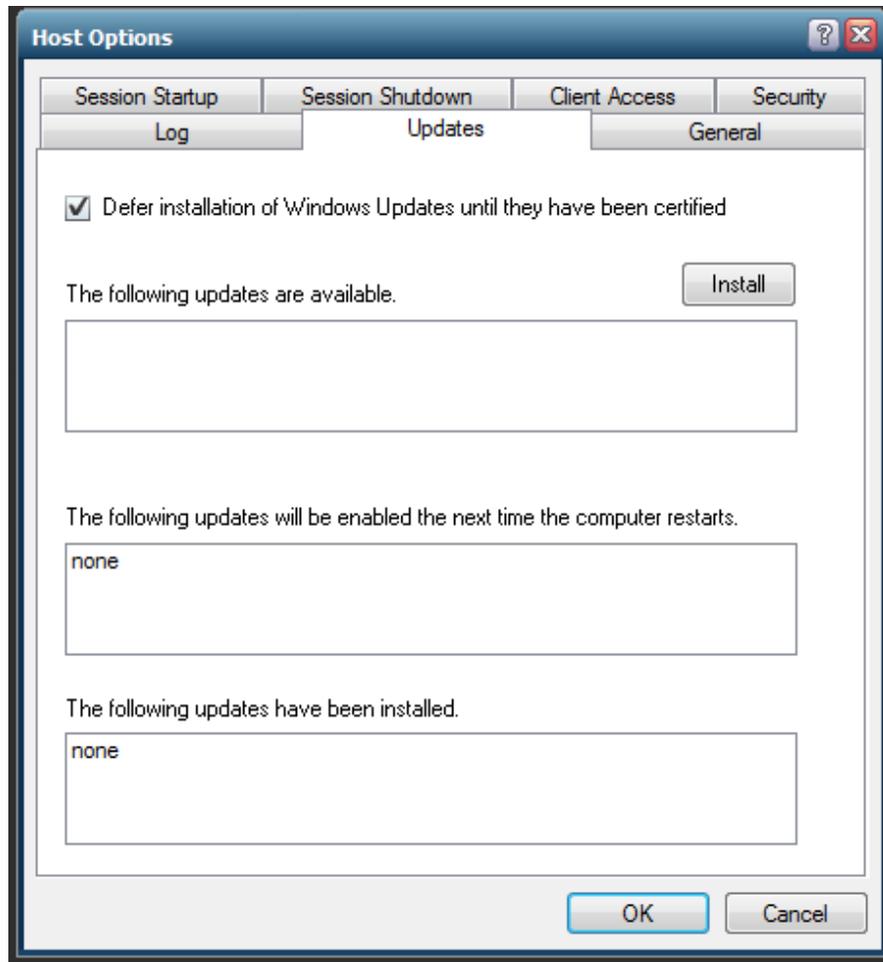
On earlier versions of Windows, Uniface Anywhere only allows Windows Updates to be installed during the time period specified by the value of the **AllowWindowsUpdates** property in the HostProperties.xml file. (The default value is 02:00-14:00 UTC, which means Windows Updates can install new updates between 6:00 p.m. and 6:00 a.m. PST.)

If an incompatibility is identified, Uniface Anywhere prevents installation of all Windows Updates on affected hosts until it has automatically downloaded and installed an update that is compatible with all Windows Update releases. Uniface Anywhere notifies the administrator when a compatibility update is downloaded and installed. After the compatibility update is successfully installed and the computer is restarted, Uniface Anywhere will resume Windows Updates.

When enabled, Windows Compatibility Assurance minimizes the risk of incompatibilities. Windows Compatibility Assurance is enabled by default, but can be disabled through the **Host Options** dialog. However, if a Windows Update is incompatible with Uniface Anywhere, and it is installed on the host, Uniface Anywhere and/or the host machine will stop working. Uniface recommends that this option is not disabled. However, if Uniface Anywhere is running on a closed network, and is unable to communicate with Uniface's Update server, this feature can be disabled to prevent warning messages from being displayed.

To disable Windows Compatibility Assurance

1. From the Admin Console, click Tools | Host Options.
2. Click the **Updates** tab.
3. Click the checkbox next to **Defer Windows Updates until they have been certified by Uniface**.



Uniface Anywhere displays messages describing an update's certification status when the Admin Console first opens and when selecting a host from the **All Hosts** list. Certification status messages display as follows:

	Message displayed:
If Windows Updates have been certified by Uniface...	<i>Uniface Anywhere is compatible with the latest Windows Updates, which were released on [date of release].</i>
If certification by Uniface is pending...	<i>Uniface is testing Windows Updates released on [date of release]. Uniface Anywhere is delaying installation of Windows Updates until Uniface certifies that these Windows updates are compatible with Uniface Anywhere.</i>
If certification by Uniface is pending, but the Windows Compatibility Assurance option is disabled...	<i>Uniface is testing Windows Updates released on [date of release] to see if they are compatible with Uniface Anywhere.</i>
If Uniface determines that Windows Updates are incompatible...	<i>Uniface Anywhere is incompatible with Windows Updates released on [date of release]. Uniface Anywhere is delaying installation of Windows Updates until a Uniface Anywhere Compatibility Update is available.</i>
If Windows Updates are incompatible but the Windows	<i>Uniface Anywhere is incompatible with Windows Updates released on [date of release]. If these Windows Updates are installed on this</i>

Compatibility Assurance option is disabled...	<i>computer, Uniface Anywhere and/or this computer will stop working.</i>
-----------------------------------------------	----------------------------------------------------------------------------------

Uniface Anywhere verifies that all the licenses the computer is using support the selected Uniface Anywhere update. If any of the licenses do *not* support the update, the Uniface Anywhere update will not be installed. For example, if the host is using a version 5 license and the selected Uniface Anywhere update is version 6, the Uniface Anywhere license(s) that this computer is using must be upgraded before the update can be installed. Contact your Uniface Anywhere Sales Representative to upgrade licenses.

Uniface Anywhere Updates

There are three types of Uniface Anywhere Updates:

- Critical
- Recommended
- Optional

Critical updates are changes that are required for Uniface Anywhere to run on the latest releases of Microsoft Windows. Critical updates do not include functionality changes. They generally only replace a few binary files on the host.

Recommended updates are changes that fix Uniface Anywhere defects and usability issues. They generally do not include user interface changes unless a user interface change is necessary to fix an important defect. Recommended updates generally replace all of Uniface Anywhere's binary files.

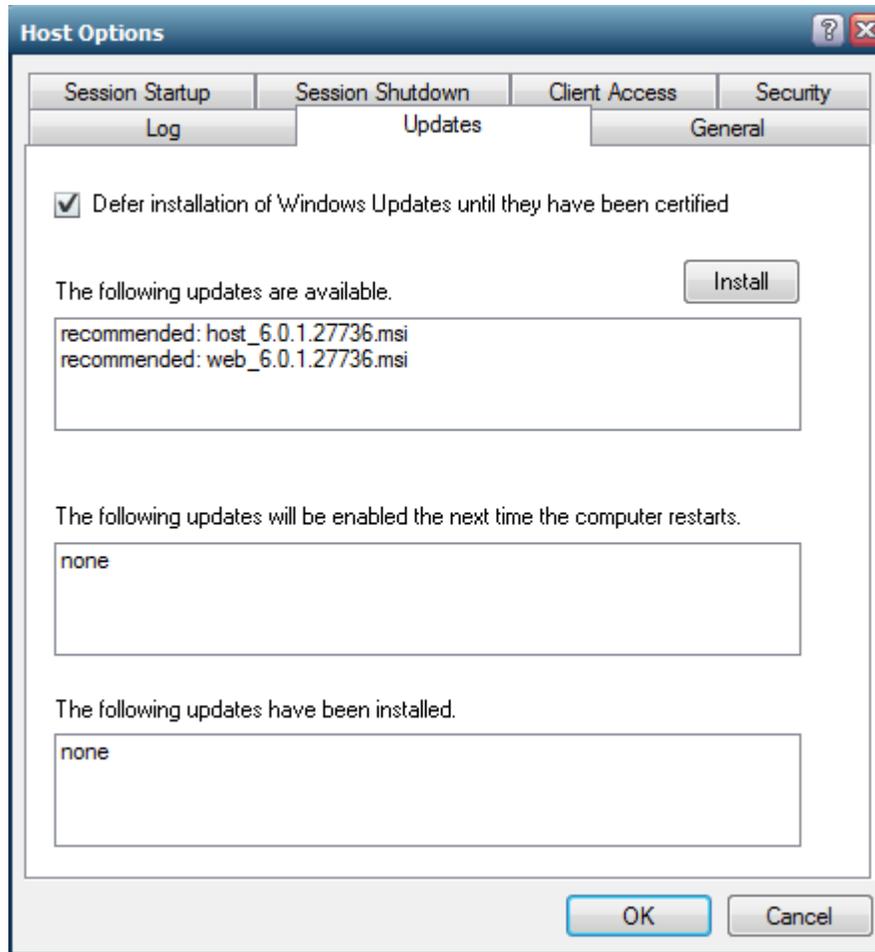
Optional updates are changes that add new features and functionality to Uniface Anywhere. Optional updates include major upgrades and minor upgrades. Optional updates generally replace all of Uniface Anywhere's binary files.

Uniface Anywhere will only automatically download and install *critical* Uniface Anywhere Updates if the Windows Compatibility Assurance option is enabled. By default, Uniface Anywhere defers installation of Windows Updates until they have been certified by Uniface.

Installing a Uniface Anywhere Update

Uniface Anywhere displays the available Uniface Anywhere updates in the **Updates** tab of the **Host Options** dialog, and allows administrators to select an update and install it.

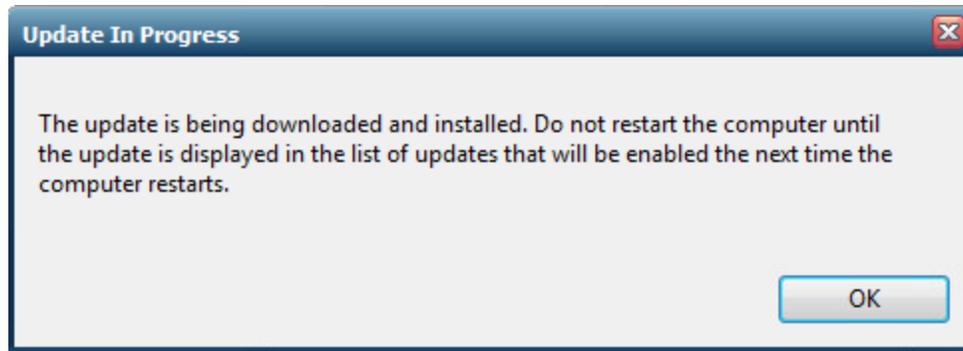
In the example below, there are two available Uniface Anywhere updates: *host_6.0.1.27736.msi* and *web_6.0.1.27736.msi*. Both are recommended updates.



To install an update

1. From the Admin Console, click Tools | Host Options.
2. Click the **Updates** tab.
3. Select one or more updates from the list of available Uniface Anywhere updates.
4. Click the **Install** button.
5. Click **Yes** to confirm.

After confirming the download, the following message is displayed:



When the update has been installed, a message confirming installation will be displayed. The installed update will be enabled the next time the computer is restarted. Uniface recommends restarting the computer at the first opportunity, when users will not be affected.

After the computer has been restarted, and the update is enabled, a message will confirm that a new version of Uniface Anywhere has been installed and enabled.

Reviewing Pending and Installed Updates

When performing update checks, the Application Publishing Service looks for updates that support:

- a. the version of Uniface Anywhere that is installed on the computer,
- b. the version of the computer's operating system, and
- c. the type of updates that are approved to be downloaded and installed on the host.

When the Application Publishing Service finds a match, it downloads the update's installer and runs it. After the update's installer has been run, the update is pending but not yet fully installed. Pending updates are installed and activated the next time the computer is restarted. Administrators can view the pending and installed updates on the Updates tab of the Admin Console's **Host Options** dialog.

To review pending and installed updates

1. From the Admin Console, click Tools | Host Options.
2. Click **Updates**.
3. **The following Uniface Anywhere updates will be enabled the next time the computer restarts** group box lists the updates that have been downloaded but are not yet fully installed.
4. **The following Uniface Anywhere updates have been installed** group box lists the updates that are installed and active on the host.
5. Click **OK**.

Managing Uniface Anywhere Hosts from Client Machines

Administrators can connect to the Admin Console from any client machine. This allows the administrator to end processes, terminate sessions, and administer applications from any machine running a Uniface Anywhere client.

To access the Admin Console from a client machine

1. Set the permissions for the Admin Console so that only Administrators can access the application.
2. In Windows Explorer, locate **AdminConsole.exe** from the Uniface Anywhere\Programs folder.
3. Right-click **AdminConsole.exe** and select **Properties**.
4. In the **Properties** dialog box, select **Security**.
5. In the **Security** dialog box, select **Permissions**.
6. In the **File Permission** dialog box, set the permissions so that only Administrators can execute the application. (For help with setting permissions in Windows Explorer, choose the Help button from the File Permission box, or press F1 while running Explorer.)
7. Add the Admin Console (AdminConsole.exe) as a registered application with the Admin Console.
8. From the client machine, log on to a Uniface Anywhere Host as an Administrator, or as a user with administrative rights on the host. This will launch the Program Window.
9. From the Program Window, launch the Admin Console by clicking the Admin Console icon. (This icon will only appear in the Program Window if the user has administrative rights on the host.) You can administer applications and user access as if running the Admin Console from the Uniface Anywhere Host.

Keyboard Shortcuts for the Admin Console

Action	Result
Applications Tab	
Double-click the application	Displays Application Properties dialog
DELETE*	Removes selected application
CTRL+A*	Displays Application Properties dialog
CTRL+S	Displays Application Properties for Users/Groups dialog
Sessions Tab	
DELETE	Terminates selected session
Processes Tab	
DELETE	Terminates the selected process
General	
CTRL+TAB	Cycles through tabs
CTRL+SHIFT+TAB	Reverse cycles through tabs
CTRL+P	Displays Options dialog
CTRL+B	Turns Status Bar on or off
ALT+F4	Exits the Admin Console
F1	Displays Help for the Admin Console
F5	Refreshes the Sessions, Processes, and Applications tabs
INSERT	Displays Add Application dialog box

*An application from the list of Installed Applications must be selected in order for these shortcuts to work.

Uniface Anywhere App

The new Uniface Anywhere App combines the functionality of Uniface Anywhere 5's native clients and browser add-ons into a single application that can be started from a computer's desktop, a mobile device, or a web browser.

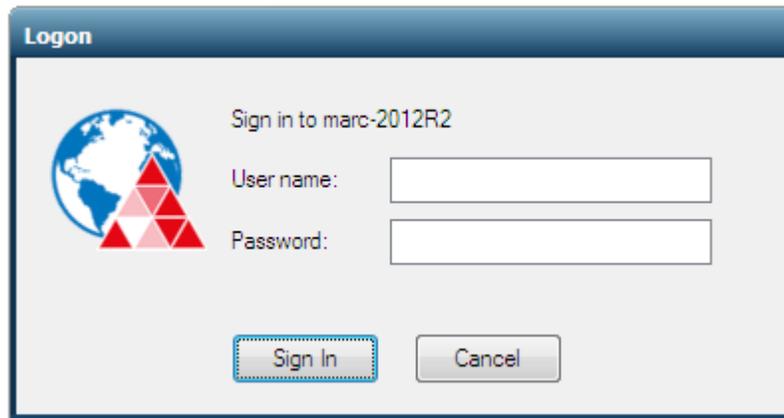
To install the Uniface Anywhere App

1. Start a Web browser.
2. In the Location box, type `http://` followed by the host name and Uniface Anywhere client installation page. For example, **`http://hostname/UAnywhere/logon.html`**
3. If the Uniface Anywhere App is not installed, Uniface Anywhere will start downloading automatically. Run the downloaded file. Otherwise, follow the on-screen instructions, which will prompt you to download and run the setup program from your computer's operating system. (e.g., **`UAnywhere.exe`**, **`ua-client.mac.dmg`**, **`ua-client.linux.deb`**, or **`ua-client.linux.rpm.`**)
4. On Mac OS X, open **`ua-client.mac.dmg`**.

After installing the Uniface Anywhere App, you can run Uniface Anywhere from a browser, from the Start menu, or from a shortcut.

To run Uniface Anywhere from the computer's menu

1. Select the Uniface Anywhere menu option:
 - a. On Windows, click the **Start** button on the Windows taskbar, and select Programs | Uniface Anywhere.
 - b. On Linux, select the Network or Internet category from the Applications menu, then click **Uniface Anywhere**.
 - c. On Mac OS X, select Go | Applications from the menu, then double-click **Uniface Anywhere**.
2. Type the address of the host in the **Connection** dialog.
3. Click **Connect**. When the **Sign In** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.



Note: Uniface Anywhere allows users three invalid logon attempts before shutting down the logon process.

On Windows computers, the Connection dialog has an option to create a shortcut to a Uniface Anywhere host. You can use this option to bypass the Connection dialog when connecting to a host.

To create a shortcut to a Uniface Anywhere Host on a Windows computer

1. Start Uniface Anywhere via one of the above methods.
2. Type the address of the host in the **Connection** dialog.
3. Select the **Create desktop shortcut** to this host check box.
4. Click **Connect**. A shortcut to the host will be created on the desktop of the computer.
- 4.

To create a Uniface Anywhere shortcut on Windows

1. Right-click on the desktop.
2. Click New | Shortcut.
3. In the **Create Shortcut** dialog box, browse to the Uniface Anywhere Client executable. For example, "C:\Program Files\Uniface\Uniface Anywhere Client\ua-client.exe"

4. Add parameters after the path to ua-client.exe. For example:

```
"C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -h hostname -a Wordpad -r "C:\Users\Public\Public Documents\test.rtf"
```
5. Type a name for the shortcut and click **Finish**.

Uniface Anywhere Web App

Developed with JavaScript and HTML5, the Uniface Anywhere Web App is a zero-install client that allows users to run Windows applications from popular web browsers on Windows, Mac, and Linux computers. In addition, no special host configuration is required to deploy the Web App. The Web App supports client-side password caching, printing to local printers via Uniface Anywhere's Preview PDF printer, and copying and pasting text between local and remote applications using CTRL keys.

Running the Uniface Anywhere Web App

Uniface Anywhere can be run from popular web browsers, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari.

To run Uniface Anywhere from a Web browser

1. Start a web browser.
2. In the Location box, type `http://` or `https://` followed by the host name, followed by **?useApp=false**
For example:
`http://hostname/UAnywhere/?useApp=false` or
`https://hostname/UAnywhere/?useApp=false`
3. When the **Sign In** dialog appears, type the following information:
 - Network user name in the **User name** box.
 - Network password in the **Password** box.

When **https://** is specified in the Location box, the **SSL Transport** must be enabled on the Security tab of the Admin Console's **Host Options** dialog, and the common name of the SSL Certificate specified on the tab must match the host name specified in the URL. These are new requirements in Uniface Anywhere v6. With earlier versions, Uniface Anywhere's browser plug-ins and add-ons (which used technologies most browsers no longer support) could connect to Uniface Anywhere Hosts using TCP Transport even when they were run from web pages that were downloaded to the browser over HTTPS. Uniface Anywhere's Web App, however, is subject to browser security restrictions, which require web apps to use WebSocket Secure connections when they are loaded over an HTTPS connection. See [Selecting SSL Transport](#) for more information.

Note:

By default, Uniface Anywhere attempts to automatically download and run the full Uniface Anywhere App. Appending **?useApp=false** to the logon URL will prevent Uniface Anywhere from downloading the Uniface Anywhere App and will run the Uniface Anywhere Web App instead.

Running the Web App with the Uniface Anywhere App

The Uniface Anywhere Web App allows users to run applications from a browser without installing anything on their computer. However, there are several limitations when only the Web App is run. For example, when running only the Web App, the following features are not supported or available: client file access, serial and parallel ports, smart cards, client sound, printing directly to client printers, and running Uniface Anywhere in loose windows mode. These limitations can be easily overcome by downloading and installing the full Uniface Anywhere App. After installing the full Uniface Anywhere App on a Windows, Linux, or Mac computer, users who run Uniface Anywhere from a web browser will have access to all these features.

Uniface Anywhere provides two URL parameters to control installation and execution of the Uniface Anywhere App. These parameters are:

- **useApp**
When useApp=true, the Web App will try to launch the full Uniface Anywhere App.
When useApp=false, the Web App will *not* try to launch the Uniface Anywhere App.
useApp=true by default.
- **installApp**
When installApp=true, the user will be prompted to install the full Uniface Anywhere App, if it is not already installed. If installApp=false, the user will *not* be prompted to install the Uniface Anywhere App and no link to install it will be displayed. When installApp=addLink, a **Get the App** link will be added to the Uniface Anywhere Web App's toolbar if the full Uniface Anywhere App is not already installed.

For example, if neither of these parameters is specified in the URL (e.g., if the URL is **http://hostname/UAnywhere/logon.html**), Uniface Anywhere will automatically start downloading the Uniface Anywhere App and will prompt the user to install and run it. Alternatively, if the installApp option is set to addLink (e.g., if the URL is **http://hostname/UAnywhere/logon.html?installApp=addLink**), a “Get the App” link will be added to the Web App’s toolbar. When users click this link, Uniface Anywhere will initiate the download and guide the user through the process of running and installing the Uniface Anywhere App.

When the Uniface Anywhere App is installed and enabled, the “embed” URL parameter can be used to control whether applications run within the browser window or outside the browser window. If the embed parameter is not specified or is set to “false” (e.g., if the URL is **http://hostname/UAnywhere/logon.html?embed=false**), the user’s applications will run outside the browser’s windows via the Uniface Anywhere App.

Alternatively, if the embed parameter is set to “true” (e.g., if the URL is **http://hostname/UAnywhere/logon.html?embed=true**) applications will run inside the browser window via the Web App. In this case, Uniface Anywhere will also start the Uniface Anywhere App (if it is installed and enabled), but the Uniface Anywhere App will only be used to provide access to the computer’s devices (e.g., printers and drives); it will not display the session’s applications.

Note:

When the Uniface Anywhere App is run inside the browser window, the default background color is white. The background color is specified by the **DesktopColor** property in the **HostProperties.xml** file. The color is specified as an RGB value in decimal format. For example, the default color of white is 16777215 in decimal (0x00FFFFFF in hexadecimal).

When the Uniface Anywhere App is not installed or `useApp = false`, the `embed` option is ignored. Otherwise, `embed` is set to `false` by default.

When the `embed` option is enabled, the Uniface Anywhere App is launched with the `-host` parameter set to the value in the `hostaddress` field of the host's `config.xml` file. The Uniface Anywhere installer initializes this value to the name of the computer. If users connect to the host with a different address (e.g., a public DNS address), the `hostaddress` field in the `config.xml` file must be set to this address.

To modify the `hostaddress` value

1. Stop the **Application Publishing Service**.
2. Locate the `config.xml` file in the `C:\ProgramData\Uniface\Uniface Anywhere` directory.
3. Open `config.xml` in Wordpad and locate the `<hostaddress>` field.
4. Update the `hostaddress` value.
5. Save the edited `.xml` file.
6. Start the **Application Publishing Service**.

Note:

When using the Web App, copying and pasting to the clipboard through an application's menu or toolbar is not supported. Instead, on Windows, use the keyboard shortcuts **CTRL+C** to copy and **CTRL+V** to paste. On the Mac, use the keyboard shortcuts **Command-C** to copy and **Command-V** to paste.

Accessing the Host or Relay Server Directly from the Internet

If users will be connecting to a Uniface Anywhere Host or relay server from the internet, the web server and host addresses in the URL must be public (internet) addresses.

When using a web server other than Uniface's, the URL must use the public address of the web server. For example: **`http://webservername.com/UAnywhere/?host=hostname`**

If users will be accessing a host or relay server from both the Internet *and* the internal network, the external and internal DNS should be configured so that the public and internal addresses of the web server are the same, and the public and internal addresses of the host are the same. Alternatively, administrators can provide external and internal users with different URLs, but this may be confusing to users.

When hosts are accessed via a third-party load balancer, the URL must include the address of the load-balancer. For example,

`http://loadbalancer.com/UAnywhere/?host=hostname&app=Notepad`

Mac OS X App

Uniface Anywhere's Mac OS X App is a lightweight application that provides seamless integration with the native Mac OS X environment. It has been completely re-written to use modern Mac OS X APIs, and provides simplified installation, sound support, multi-monitor support, and Mac OS X Gatekeeper support, which helps protect against malware and misbehaving apps downloaded from the internet.

To install the Mac OS X App

1. Launch your web browser.
2. In the Location box, type `http://` followed by the host name and the Uniface Anywhere client installation file. For example, `http://host/UAnywhere/clients.html`.
3. Follow the instructions to download and install `ua-client.mac.dmg`.
4. Open `ua-client.mac.dmg` and drag **Uniface Anywhere.app** into Applications.

To run the Mac OS X App

1. From the menu bar, click Go | Applications.
2. Double-click **Uniface Anywhere** to launch Uniface Anywhere.
3. Type the host address in the **Connection** dialog.
4. When the **Sign In** dialog appears, enter the following information:
 - Your network user name in the **User name** box.
 - Your network password in the **Password** box.

To uninstall the Mac OS X App, drag **Uniface Anywhere.app** from Applications to the trash.

To use startup parameters with the Mac OS X App

1. Open **Terminal**.
2. Change to the `/Applications/Uniface Anywhere.app/Contents/MacOS/` directory.
3. Type `./Uniface Anywhere` and append startup parameters.

Example, `./Uniface Anywhere -h 196.125.101.222 -ac all -hp 443`

Uniface Anywhere Startup Parameters

Uniface Anywhere supports the following shortcuts and parameters:

Shortcut	Parameters	Description
-u	user	The name of the user's account.
-p	password	The user's password.
-h	host*	The network name of the Uniface Anywhere Host.
-hp	port	The port on which the Uniface Anywhere Host accepts connections. (491 by default.)
-a	app	The application to run. This may be a command-line string or the application name, as registered with the Admin Console.
-r	args	Application arguments.
-c or -nc	compression	-c enables compression. -nc disables compression. compression="true" enables compression. compression="false" disables compression. Compression is enabled by default.
-ac	printerconfig	Determines how printers are initialized at startup. When printerconfig="all" or -ac is followed by all , all printers are automatically configured. When printerconfig="none" or -ac is followed by none , printers are not automatically configured. When printerconfig="default" or -ac is followed by default , the default printer is configured automatically. This is the default setting.
-f	clientframe	When set respectively to 1 or "true", all applications running in the session will be displayed within a bounding window. When set respectively to 0 or "false", applications will be displayed within their own individual windows.
-autoreconnect	autoreconnect	Determines how many times the client will automatically attempt to reconnect after a broken connection. When autoreconnect= <i>n</i> in a URL or -autoreconnect is followed by <i>n</i> , the client will automatically attempt to reconnect <i>n</i> number of times. (autoreconnect is set to 20 by default.)
-geometry		The width and height of the client window. For example: -geometry 800x600
	multimonitor	When set to "true", the session's desktop will span all monitors. When set to "false", applications will be confined to the primary monitor. multimonitor="true" by default.
	width	The width of the frame or embedded window. (800 by default.)
	height	The height of the frame or embedded window. (600 by default.)
	embed	When set to "true" applications run within the browser window. When set to "false" applications run outside the browser window.
	blnBrowser	Not supported in version 6.
	noscale	When noscale is set to "true" and the browser is resized, the resolution of the embedded Uniface Anywhere session will adjust accordingly, rather than scaling the displayed image on the client. (noscale="false" by default.)

	useApp	When useApp= "true", the Uniface Anywhere Web App will try to launch the full Uniface Anywhere App. When useApp="false", the Web App will not try to launch the Uniface Anywhere App. (useApp="true" by default.)
	installApp	When installApp="true", the user will be prompted to install the full Uniface Anywhere App, if it is not already installed. If installApp="false", the user will NOT be prompted to install the Uniface Anywhere App and no link to install it will be displayed. When installApp="addLink", the Get the App link will be added to the Uniface Anywhere Web App's toolbar if the full Uniface Anywhere App is not already installed.
-clientscale	clientscale	clientscale , followed by the percent scale factor, causes the Uniface Anywhere App on Windows to scale the applications running in the session relative to applications running locally on the client computer. For example, adding -clientscale 200 to the command-line will cause applications running in the Uniface Anywhere session to appear twice as large as applications running locally on the client computer.
-clientdpi	ClientDPIScaling Enabled	-clientdpi 1 or ClientDPIScalingEnabled="true" enables the Uniface Anywhere App's DPI scaling feature. -clientdpi 0 or ClientDPIScalingEnabled="false" disables the feature. When these options are specified, they override the value of the ClientDPIScalingEnabled property in the HostProperties.xml file on the host.
-cn	computerName	When -cn 1 or computerName=1, the Windows client sends the CLIENTNAME environment variable to the host rather than the actual computer name.
-krm	keyreportingmethod	This option instructs the client to send either unicode or keycode values to the host based on character type. -krm 0 — The client sends alpha keys as unicode and numeric keys as unicode. -krm 1 — The client sends alpha keys as keycode and numeric keys as unicode. -krm 2 — The client sends alpha keys as unicode and numeric keys as keycode. -krm 3 — The client sends alpha keys as keycode and numeric keys as keycode.

*If no host is specified in the logon HTML page, Uniface Anywhere detects the machine from where the logon file was downloaded, and makes the connection to that host. The **Connection** dialog is not displayed and the user is presented with the **Sign In** dialog only. If host= "?" users will be prompted for the address of the host.

Modifying the Logon HTML Page

When Uniface Anywhere is run from a Web browser, startup parameters can be specified by editing the Uniface Anywhere logon.html page.

To modify logon.html

1. Open logon.html in an HTML editor.
2. Locate the parameter you wish to edit. The most common parameters are listed in the logon page as follows:

```
//
// controlArgs.set([ "user",    "testuser1"  ]);
// controlArgs.set([ "password", "testpassword1" ]);
// controlArgs.set([ "embed",   "false"    ]);
// controlArgs.set([ "width",   "640"     ]);
// controlArgs.set([ "height",  "480"     ]);
// controlArgs.set([ "desktop", "false"   ]);
// controlArgs.set([ "app",     "testapp1"  ]);
// controlArgs.set([ "port",    "491"     ]);
// controlArgs.set([ "autoclose", "false"  ]);
// controlArgs.set([ "printerconfig", "default" ]);
// controlArgs.set([ "bInBrowser", "false"  ]);
// controlArgs.set([ "host",     "testhost1" ]);
// controlArgs.set([ "compression", "true"   ]);
// controlArgs.set([ "clientframe", "false"  ]);
// controlArgs.set([ "multimonitor", "true"  ]);
// controlArgs.set([ "noscale",   "false"   ]);
// controlArgs.set([ "authority",  "not_specified" ]);
// controlArgs.set([ "credentials", "not_specified" ]);
// controlArgs.set([ "sessionid",  "1234"   ]);
// controlArgs.set([ "autoreconnect", "0"    ]);
// controlArgs.set([ "windowless", "false"  ]);
// controlArgs.set([ "maxbpp",     "16"     ]);
// controlArgs.set([ "keyboard",   "ClientSideIME" ]);
// controlArgs.set([ "args",       "testargs1"  ]);
// controlArgs.set([ "useApp",     "true"     ]);
// controlArgs.set([ "installApp", "add_link"  ]);
```

3. Uncomment the corresponding controlArgs.set line by removing the // from the beginning of the line. Then edit the value, as desired. For example:

```
controlArgs.set([ "user",    "johng"  ]);
controlArgs.set([ "embed",   "true"   ]);
```

4. To specify startup parameters not listed, add controlArgs.set() for each parameter. For example:

```
controlArgs.set([ "parameter", "true"  ]);
```

5. Save the page.

Specifying URL Parameters

Startup parameters can also be specified by appending them to the URL.

To specify URL parameters

1. In the web browser's Location box, type `http://` followed by the host name and the Uniface Anywhere directory. For example, **`http://hostname/UAnywhere/`**
2. Append a question mark (?) to the URL followed by the desired parameter. For example, **`http://hostname/UAnywhere/?user=user1`**
3. Append an ampersand (&) to the URL to specify additional parameters. For example, **`http://hostname/UAnywhere/?user=user1&password=password1&app=wordpad`**

Web Files

The Uniface Anywhere Host setup installs the Uniface Anywhere web files under `C:\Program Files\Uniface\Uniface Anywhere\Web`. If Microsoft Internet Information Services (IIS) is detected during installation, a virtual directory will be created in IIS that points to the Uniface Anywhere web files. If IIS is not available, administrators will need to manually host the Uniface Anywhere web folder contents on the specified web server.

Administrators can edit the HTML pages to modify default options and limit which clients are made available to users. During installation, the initial web page is set to `logon.html`. Users accessing the host from a web browser should be directed to the following URL:

`http://hostname/UAnywhere/`

Uniface Anywhere automatically detects the user's platform and browser and runs the appropriate Uniface Anywhere Client. The `allclients.html` page lists all Uniface Anywhere clients no matter which client operating system is detected.

There are two versions of the Uniface Anywhere App for Windows: an **All Users** version, and a **Single User** version. The installer for **All Users** version (`UAnywhere.windows.exe`) installs the Uniface Anywhere App for all users who use the computer, but it can only be installed by users who have administrator rights on the computer. The installer for the **Single User** version (`UAnywhere.exe`) can be run by users who do not have administrator rights on the computer, but it is only installed for the user running the installer. If another user wishes to run the Uniface Anywhere App on the same computer, he or she will also have to run the installer for the Single User version of the app.

Note:

Installation of the Single User version of Uniface Anywhere may fail if normal users are prevented from installing software by local or group policy.

Resizing the Client Window

The command-line argument `-geometry` can be used to modify the size of the client window when the command-line argument `-f` is used. Without `-geometry` on the command-line, the client window will be maximized. When Uniface Anywhere is run in loose window mode, `-geometry` has no effect. To resize the client window, append `-geometry` to the Uniface Anywhere Client executable, followed by the desired width and height.

For example, on Windows:

```
"C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -f -geometry=800x600
```

On Linux:

```
./ua-client -h 196.125.010.222 -f -geometry=800x600
```

On Mac:

```
./Uniface Anywhere -h 196.125.010.222 -f -geometry=800x600
```

Uninstalling Uniface Anywhere

Instructions for uninstalling Uniface Anywhere depend on the platform and browser.

To uninstall the Uniface Anywhere Client on Windows

1. Open Control Panel.
2. Double-click **Programs and Features**.
3. Select **Uniface Anywhere Client**.
4. Click **Uninstall**.
5. Click **Uninstall**.

Note:

If users experience slow scrolling with Uniface Anywhere, try disabling the smooth scrolling option on the host. In Internet Explorer, click Tools | Internet Options. Click the **Advanced** tab. In the **Settings** box, under **Browsing**, disable **Use smooth scrolling**.

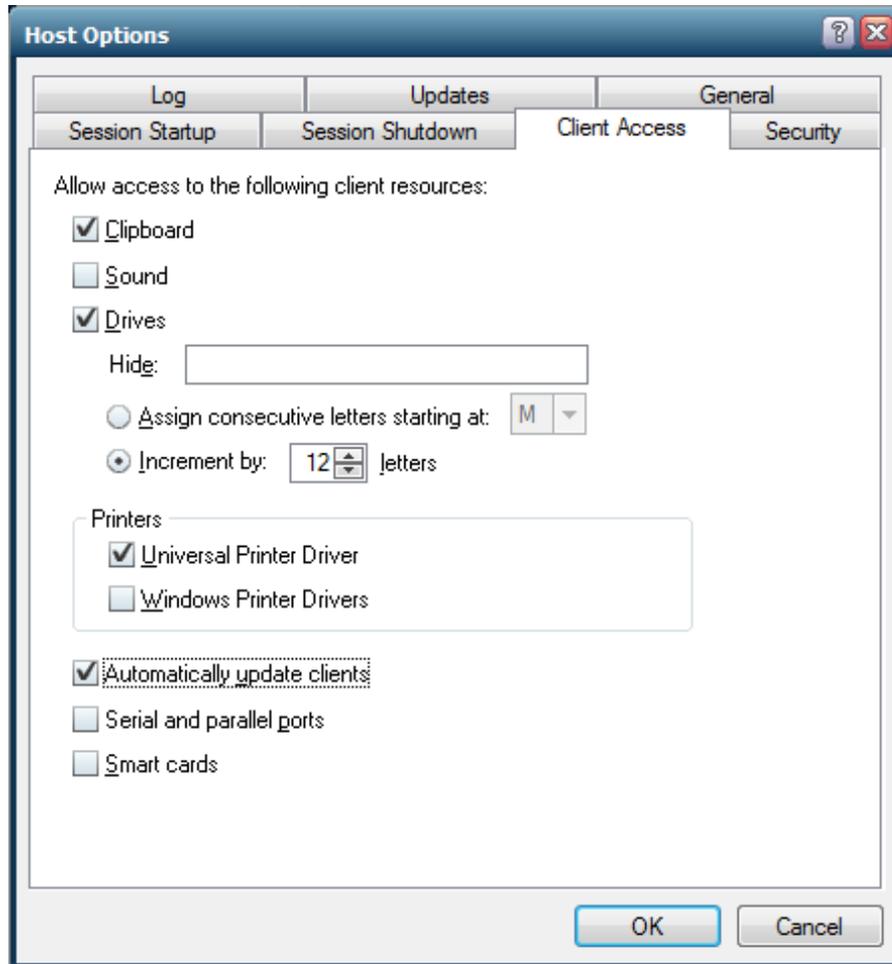
Automatic Client Updates

Administrators can configure Uniface Anywhere to automatically update the Uniface Anywhere Client when users connect to a Uniface Anywhere Host that is running a newer version.

To enable Automatic client updates

1. Install the Uniface Anywhere Client on client computers using the **UAnywhere.windows.exe** program. (The Automatic client update feature is only available for Windows computers.)
2. From the Admin Console, click Tools | Host Options.
3. Click the **Client Access** tab.
4. Enable **Automatically update clients**.
5. Click **OK**.

Mac and Linux users can download the updated version of Uniface Anywhere by connecting to the Uniface Anywhere logon page (e.g., <http://hostname/UAnywhere/logon.html>) and installing the full Uniface Anywhere App.



When **Automatically update clients** is selected in the Admin Console and a user signs in to the host from a Windows computer, Uniface Anywhere compares the version of the Uniface Anywhere App installed on the client computer to the version in the Updates directory on the Host. If the files in the Updates directory are newer, Uniface Anywhere copies the newer files to a temporary directory on the client computer. Then, when Uniface Anywhere closes, the **Uniface Anywhere Update Client** service installs the new files so they can be used in subsequent Uniface Anywhere sessions. Users will be updated on the screen when the new updates have completed installing.

In summary, a new version of Uniface Anywhere will be installed via the update client service when the following conditions are met:

- **Automatically update clients** is enabled in the Admin Console.
- The **Uniface Anywhere Update Client** service is installed and enabled on the client computer.
- A newer version of the client is available in the Updates directory on the host.

- All of the files in the new version have been downloaded to the client computer.
- The user has signed out of his or her Uniface Anywhere Client session.

The default location for the Updates folder is C:\Program Files\Uniface\Uniface Anywhere\Updates which is defined in the registry key:
Note: HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere\Updates.

Users are not required to perform any upgrade tasks. They can, however, prevent updates from being installed by disabling the Uniface Anywhere Update Client service on the client computer.

To disable the Uniface Anywhere Update Client service

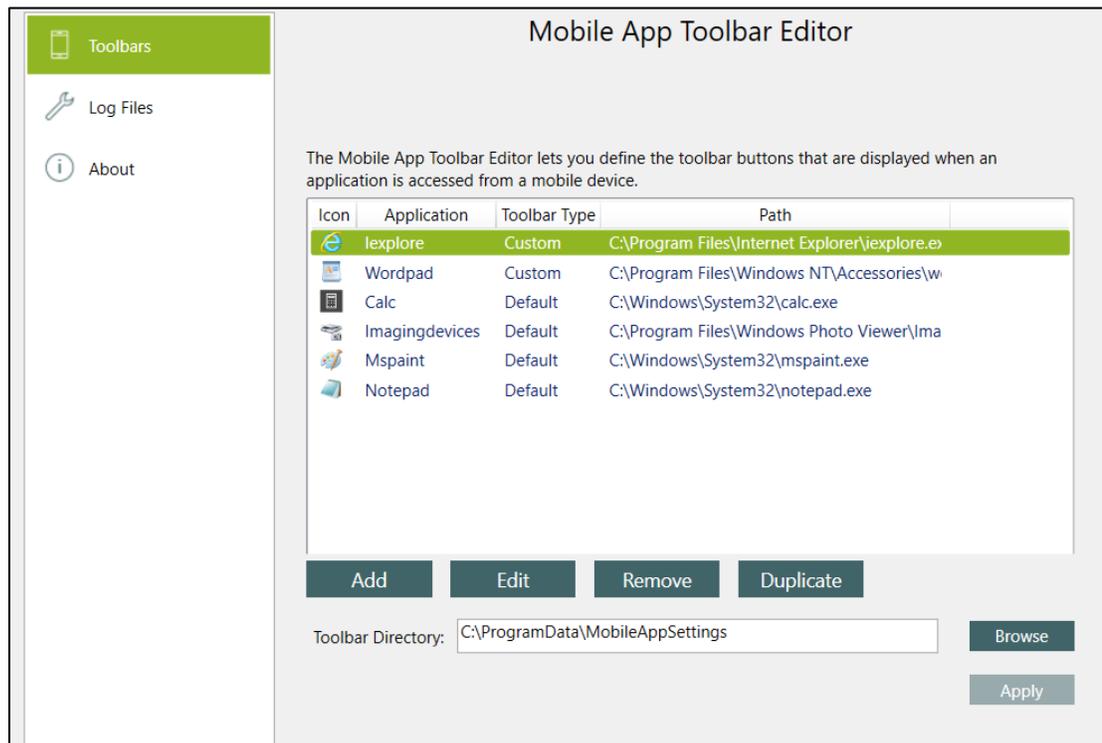
1. Right-click My **Computer**.
2. Click **Manage**.
3. Click Computer Management | Services and Applications | Services.
4. Select **Uniface Anywhere Update Client**.
5. Click **Properties**.
6. Under **Startup type**, select **Disabled**.
7. Click **Stop**.
8. Click **OK**.

Mobile App Toolbar Editor

The Mobile App Toolbar Editor is used to define the toolbar buttons and menus that are displayed when an application is accessed from a mobile device. Both the buttons and the menu items will appear in the toolbar at the bottom of the application. Menu items can include submenu items, which appear in another toolbar directly above the main toolbar.

To open the Mobile App Toolbar Editor

Click Programs | Uniface Uniface Anywhere | Mobile App Console.

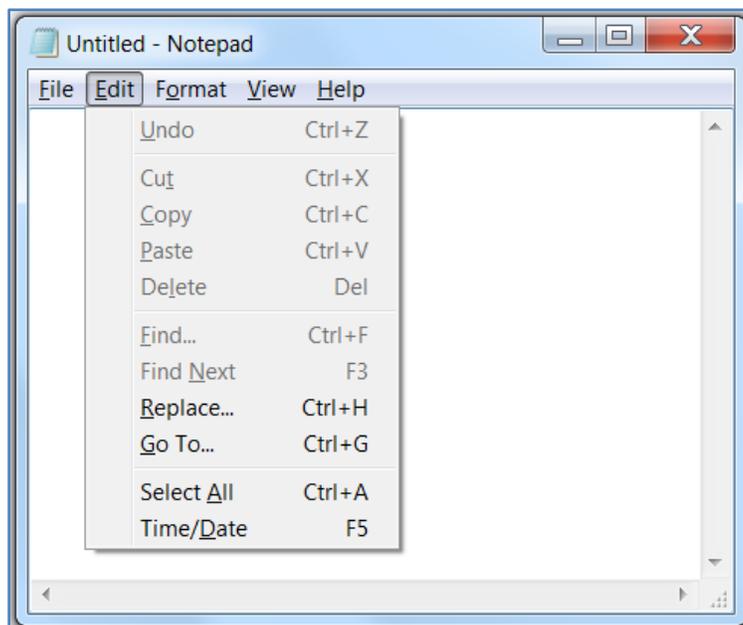


Applications that are published in the Admin Console will be listed, and each will be configured to use the default toolbar.

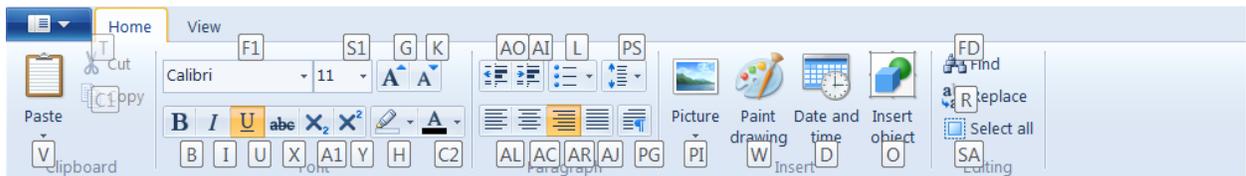
The **Add**, **Edit**, **Remove** and **Duplicate** buttons apply only to the custom toolbars, and not to the applications. For example, clicking the **Remove** button will remove the custom toolbar from the selected application. The application will still be published in the Admin Console and will still be available to users.

Creating Custom Toolbars

Check the menus of the applications you are creating custom toolbars for, to verify shortcut keys. Every application has its own shortcuts, and shortcuts that work in one might not work in another.



In applications that have toolbars, such as Microsoft Word and WordPad, click Alt + H while in the Home tab, to display available shortcuts.

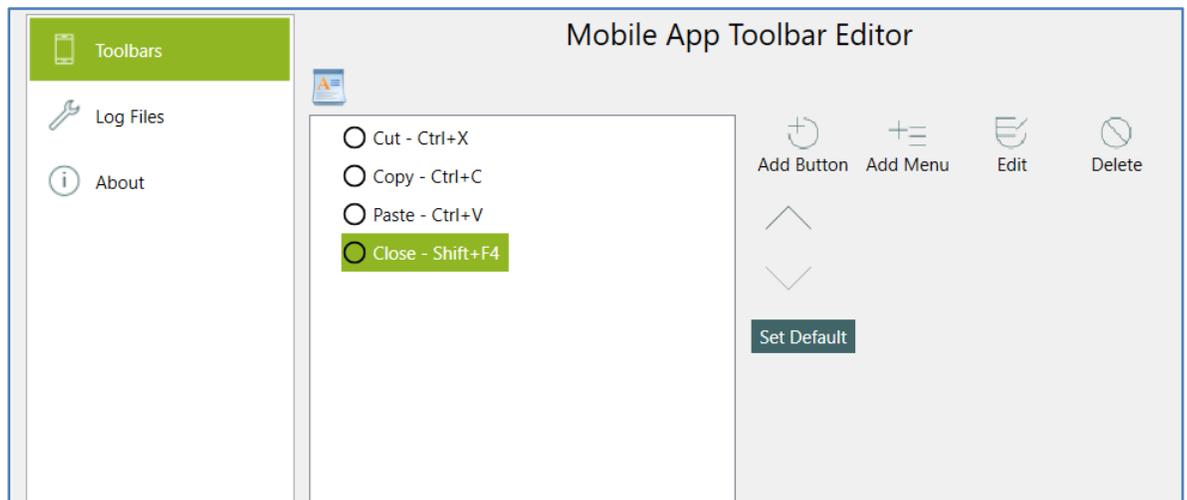


In the following instructions for creating a custom toolbar, WordPad is used as the example application.

To add a button

1. Select an application from the list of applications and click the **Edit** button.
2. Click the **Add Button** to open the **Add button** dialog.
3. Type a name for the new button in the **Label** field.
4. Add the associated shortcut. Do this by using the shortcut keystrokes on your keyboard. For example, press Ctrl + X on the keyboard, and this will appear in the **Shortcuts** field.
5. Click **Add**. This will add the button and the shortcut to the toolbar list.
6. Click **Apply**. This button will now appear in the application's toolbar on the mobile client device. You can continue to add buttons or menu items, or click the **Custom Toolbar List** button to add toolbar and menu items to a different application.

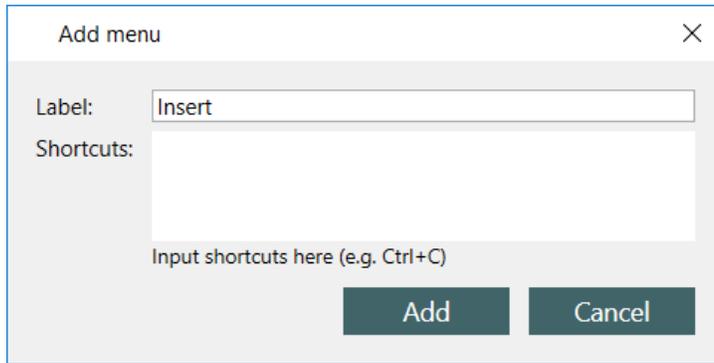
In the example below, buttons for **Cut** (Ctrl + X), **Copy** (Ctrl + C), **Paste** (Ctrl + V), and **Close** (Shift + F4) have been added to the custom toolbar:



A menu item is similar to a toolbar button, but can have up to three submenu items.

To add a menu item

1. Select an application from the list and click the **Edit** button.
2. Click the **Add Menu** button to open the **Add menu** dialog. Type the menu item name in the **Label** field.
3. For menus, the Shortcuts field is typically left blank. However, if you want the application to perform an action when the menu is opened, type the shortcuts for the action in the **Shortcut** field.
4. Click **Add**.
5. Click **Apply**. This menu item will now appear in the application's toolbar on the client device.

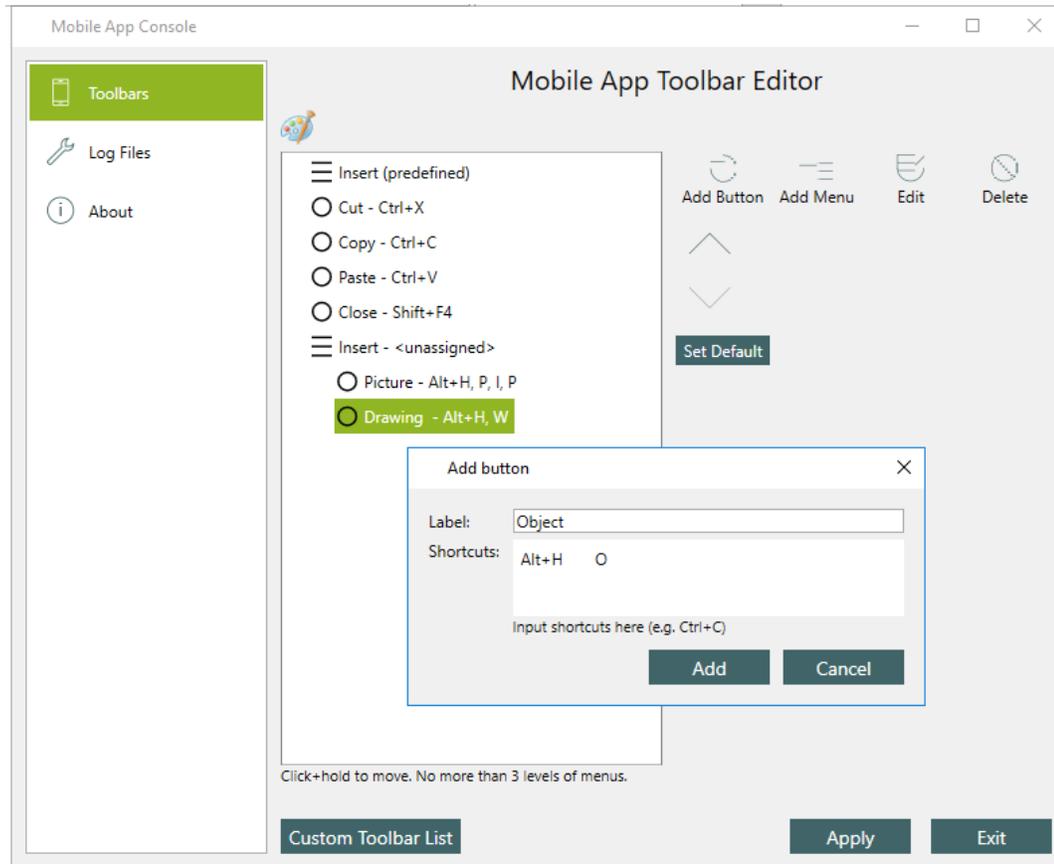


The screenshot shows a dialog box titled "Add menu" with a close button (X) in the top right corner. On the left side, there are two labels: "Label:" and "Shortcuts:". The "Label:" field contains the text "Insert". Below the "Shortcuts:" label is a large empty text area. Underneath this area is the text "Input shortcuts here (e.g. Ctrl+C)". At the bottom of the dialog, there are two buttons: "Add" and "Cancel".

To add a button to a menu

1. Highlight the menu item from the toolbar list and click **Add Button**.
2. In the **Add button** dialog, type a name for the new button in the **Label** field.
3. Type the shortcut(s) for the action in the **Shortcuts** field.
4. Click **Add**.
5. Click **Apply**.

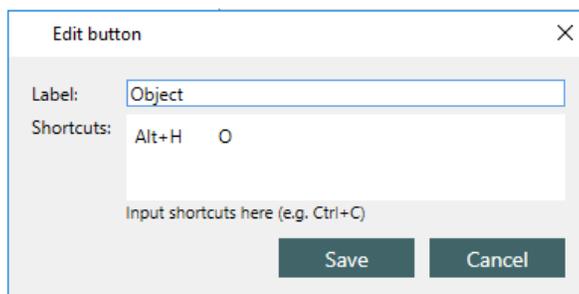
In the example below, an **Insert** menu was created, with buttons for inserting pictures, drawings, and objects. To insert an object in WordPad using shortcut keys, a user would click Alt + H, then O. By creating the submenu button for Object in the Toolbar Editor, with the appropriate shortcut keys (i.e., Alt + H, then O), a user on a mobile device can click the **Object** button on the custom toolbar to insert an object into a document.



You can add up to ten items per menu level and up to five shortcuts per button.

Editing toolbar buttons and menu items

1. To edit a button or menu item, highlight the item from the list and click **Edit**.
2. To delete an existing shortcut, hover the mouse over the text in the **Shortcuts** field. Click the x that appears over the gray highlighted text.
3. Type a new shortcut.
4. Click **Save**.

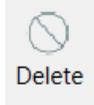


To move a button or menu item up or down

Highlight the item in the toolbar list and click the **Move up** or **Move down** button.

**To delete a button or menu item**

Highlight the item in the toolbar list and click the **Delete** button.

**To revert to the default toolbar**

Click the **Set Default** button. This will delete the custom toolbar settings.

**Adding a custom toolbar for an application's child program**

Some applications published in the Admin Console will launch one or more child programs that perform a subset of the application's tasks. In some cases, an application's main functionality may be provided by an unpublished child program. In these cases, you can add a toolbar for a child program using the **Add** button, and you can copy an existing toolbar to the child program using the **Duplicate** button.

To create a toolbar for a child process

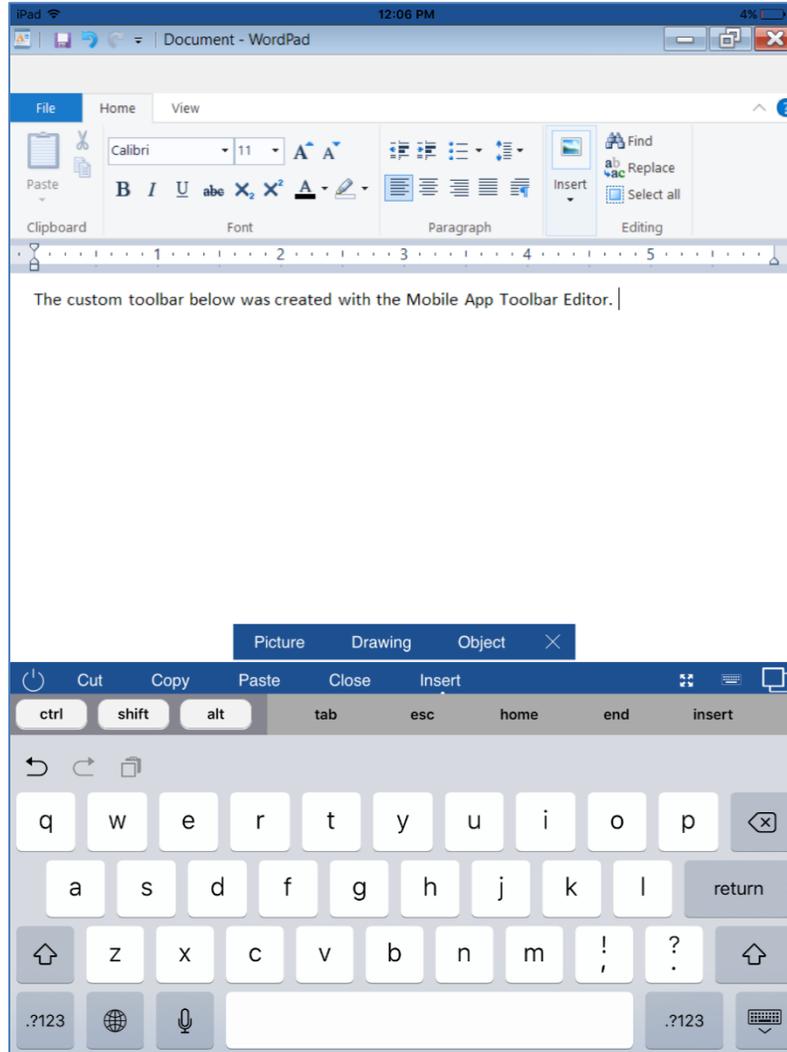
1. In the Toolbar Editor, click **Add**.
2. Browse to the child program's executable file.
3. Select the file and click **Open**.
4. Add buttons and menus as described above.

To copy a toolbar

1. To copy an existing toolbar to use with a child program, select the application's toolbar you want to copy from the list.
2. Click the **Duplicate** button.
3. Browse to the child program's executable file.
4. Select the file and click **Open**.

Viewing the Custom Toolbar

You can view the toolbar buttons you created by opening the Uniface Anywhere App on a mobile device. Launch WordPad, for example, to see the custom toolbar buttons at the bottom of the screen. Tap **Insert** to open the submenu. Tap the **X** to close the submenu.



Changing the Toolbar Directory

Toolbar files are stored in the **C:\ProgramData\Uniface\Uniface Anywhere\MobileAppSettings** directory by default. If you have multiple Uniface Anywhere Hosts, you can store the toolbar in a shared network directory and use the same toolbar files on all hosts.

To change the directory where toolbars are stored

1. Browse to or type the path to the desired directory in the **Toolbar Directory** field.
2. Click **Apply**.
3. If you have already created toolbars, you will be asked if you want to copy the existing toolbars to the new directory.

Log Files

When logging is enabled, the Mobile App Console records messages in log files that are stored in the **C:\ProgramData\Uniface\Uniface Anywhere\MobileAppLogs** directory. Logging can be enabled and disabled in the Log Files panel of the Mobile App Console. Logging is disabled by default.

To enable logging

1. Click the checkbox next to **Enable Logging**.
2. Click **Apply**.

When logging is enabled, you can change the directory in which log files are stored by entering the path to the desired directory in the **Log Directory** field and clicking **Apply**.

Load Balancing

Load balancing allows Uniface Anywhere sessions to be distributed across multiple hosts. Load balancing is required when the host resource requirements for a deployment exceed the capacity of a single host computer. Load balancing is done automatically and is transparent to the user. Uniface Anywhere can also be used with any third party TCP/IP based load-balancing service.

Load Balancing Requirements

- A Uniface Anywhere Host must be installed on each of the hosts in the cluster.
- For web deployment, if the load balancer is balancing connections to both the web server (e.g., port 80) and the Uniface Anywhere Host (e.g., port 491), each of the Uniface Anywhere Hosts in the cluster must have a web server running and the web server home directory should contain the Uniface Anywhere web files. If the load balancer is only balancing connections to the Uniface Anywhere Host, the web files do not need to be located on each Uniface Anywhere Host. Web files can be installed on the machine running the web server.
- If an application saves any user specific settings in the registry, (e.g., Corel WordPerfect, Microsoft Word, etc.) we strongly recommend that users operate with roaming profiles rather than local profiles. Since there is no way of predicting which server the user will actually be logged onto in a balanced server farm, working with roaming profiles is the only way to ensure that user specific settings are available to the user at all times.

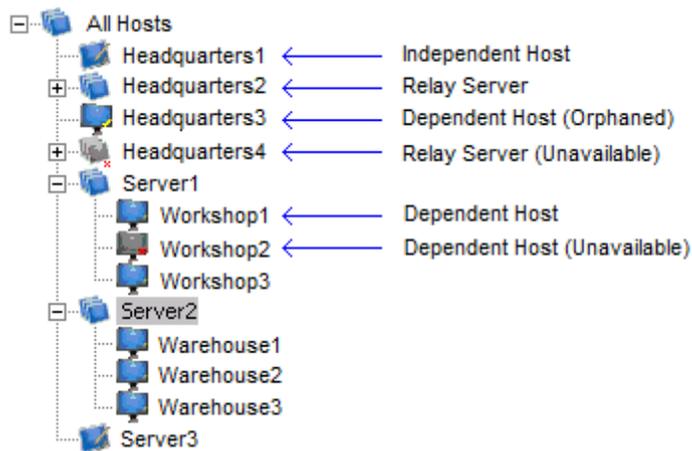
A Uniface Anywhere Host can be configured to operate as an independent host, a dependent host, or as a relay server. Please note that a relay server *cannot* be an application host.

When setting up a load-balanced relay server configuration, Uniface recommends using a license server. For more information, see the following sections from Chapter 2: **Configuring Uniface Anywhere to use a Central License Server**, **Three-Server Redundancy**, and **License-File List Redundancy**.

Independent Hosts

Independent hosts are Uniface Anywhere Hosts that do not interact with other Uniface Anywhere Hosts running on the network. Independent hosts appear in the Admin Console on the first level of the Uniface Anywhere Hosts tree view as an independent node. The Uniface Anywhere setup program configures hosts to operate as independent hosts. Uniface Anywhere clients can connect to independent hosts directly by specifying the name or IP address of the server in the **Connection** dialog or the location box of a web browser. Clients can also connect to independent hosts through a third-party network load balancer that distributes client connections among several servers. However, session reconnect is not supported in the latter configuration and must be disabled.

Uniface Anywhere Hosts



Relay Servers

A relay server is a Uniface Anywhere Host that provides centralized control over one or more hosts. Relay servers maintain client connections and distribute Uniface Anywhere sessions across a set of load-balanced application hosts. Relay servers appear in the Admin Console on the first level of the list of **All Hosts** as nodes with one or more dependent hosts.

To configure a Uniface Anywhere Host to operate as a relay server

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **General** tab.
4. Type the name or IP address of the computer in the **Relay server** box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** on the relay server has been restarted. Click **OK**.
7. Stop and restart the **Uniface Anywhere Application Publishing Service** from the Services option in the Control Panel.

After configuring a host to run as a relay server with one or more dependent hosts, Uniface Anywhere load-balances client connections and ensures that sessions start successfully. If a session fails to start on the selected host, the relay server selects another host and tries again until it finds one that can support the session.

When setting up a relay server environment, be sure the same **Log Folder** path for the relay server exists on the dependent hosts. Otherwise, the **Sign In** dialog will not appear when users attempt to sign in to Uniface Anywhere. Create a log directory on the C: drive of each relay server (e.g., C:\Data\APS_LOGS) or use C:\Program Files\Uniface\Uniface Anywhere\Log which already exists on the dependent host. Make sure this same path exists on the dependent host. In addition to changing the **Log Folder** path in the Admin Console, the \Log\Codes and \Log\Templates directories must be copied to the new location.

Note: When a relay server is selected in the Admin Console, the number of processes running on all dependent hosts is not listed in the Admin Console's status bar.

A relay server requires a minimum of 512 MB of RAM. For most deployments and for best results, 1 GB with a multiprocessor server is recommended. Depending on the number of dependent hosts attached to the relay server, more RAM may be required.

Memory and CPU requirements for the dependent hosts are determined by the applications that are published and the number of users accessing the system. In general, a dependent host can support 12 “heavy” users/500 MHz CPU and 25 “light” users/500 MHz CPU. (“Heavy” is defined as a user running one or more large applications with continuous user interaction. “Light” is defined as a user running one application with intermittent user interaction.)

Dependent Hosts

A dependent host is a Uniface Anywhere Host that is connected to a relay server. Uniface Anywhere clients cannot connect directly to dependent hosts. Instead, they connect to the associated relay server, and the relay server selects one of the connected servers to host the session.

To configure a Uniface Anywhere Host to operate as a dependent host

1. Select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **General** tab.
4. Type the name or IP address of the relay server in **Relay server** edit box.
5. Click **OK**.
6. A message box is displayed indicating that the change will not take effect until the **Application Publishing Service** has been restarted. Click **OK**.
7. Stop and restart the **Uniface Anywhere Application Publishing Service** from the Services option in the Control Panel.

When the Application Publishing Service is restarted, the dependent host will appear beneath the relay server in the Admin Console's list of Uniface Anywhere Hosts. A dependent host with a

yellow x indicates that the host has been “orphaned;” in other words, that its relay server has gone down. If a host’s icon has a red x, the administrator does not have administrative rights on the host. If the host’s icon has a red x and is grayed out, the host is no longer running the Application Publishing Service or it has been turned off. In either case, the administrator is unable to access that host from the Admin Console.

Users are authenticated on dependent hosts, not on relay servers. As a result, dependent hosts can be located on a different network than their associated relay server. For example, dependent hosts can be located behind a firewall on an internal, Active Directory network, and the associated relay server can be located in a demilitarized zone (DMZ) that is outside the firewall. If **Integrated Windows authentication** is used, clients and dependent hosts must be located on the same domain, but the relay server can be located on a different domain.

Note: We recommend installing the same set of applications on each dependent host and using the same installation path.

License Server Configuration

When an independent host is configured to run as a relay server or a dependent host, Uniface Anywhere does not automatically make any changes to the host's licensing configuration. For example, if an independent host is configured to use the license server that is installed on the same computer as the host, the host will continue to use the computer's local license server after the host is connected to a relay server. This is the default configuration, but not typically the best licensing configuration. A relay server and its dependent hosts should all be configured to use the same license server(s).

If high-availability is not required, Uniface recommends configuring the dependent hosts to use the license server on the relay server as a Central License Server. (See **Configuring Uniface Anywhere to use a Central License Server** and ensure that the dependent hosts are able to connect to the license server's port on the relay server.)

If high-availability is required, Uniface recommends configuring the relay server and its dependent hosts to use a set of **Three-Server Redundant License Servers**.

With both of these configurations, the **Licenses** tab on the Admin Console will report the same license information, regardless of which computer is selected.

Note: Licenses are checked out from dependent hosts, not the relay server. If a relay server is not configured to use a license server, sessions will start, but the **Licenses** tab in the Admin Console will not display licensing information when the relay server is selected.

Administering Relay Servers and Dependent Hosts on Different Networks

When a user starts the Admin Console on a relay server or a dependent host, the Admin Console connects to the relay server and attempts to authenticate the user using Integrated Windows authentication. If the Admin Console is running on a dependent host and the associated relay server is located on a different network, a message such as the following is displayed:

Failed to log you on to Server8. This computer (Server4) and Server 8 may be located on different networks. Would you like to log onto Server 8 and administer it remotely?

Clicking **No** will return you to the **All Hosts** node of the Admin Console. Clicking **Yes** will initiate a special remote administration session on the relay server as follows:

1. The Admin Console on the dependent host starts the Uniface Anywhere Client.
2. The client connects to the relay server and starts a session. The **Sign In** dialog is displayed to the user.
3. The user signs in, specifying the user name and password of an account that is a member of the Administrators group on the relay server.
4. The Admin Console starts on the relay server. The user can now administer the relay server and all of its dependent hosts.
5. A maximum of two administration sessions can run on the relay server at any given time, regardless of the **Maximum sessions on this host** setting in the Admin Console and regardless of license restrictions.

Dependent hosts inherit their list of published applications, server settings, and user settings from the relay server. Applications *must* be installed in the same directory on all dependent hosts. Applications do not need to be installed on the relay server. When a Uniface Anywhere Host is connected to a relay server all of its server settings are synchronized with those of the relay server.

When any changes are made to the relay server's settings, they are also made to **All Hosts** connected to that relay server. The only settings that are allowed to vary are the maximum number of sessions and the name of the relay server. All other settings in the **Host Options** and **Application Properties** dialogs are grayed out and cannot be modified.

When setting up a relay server, if an application is *installed* but not *published* on the dependent host, you will need to publish the application on the relay server through the Admin Console. For example, if Adobe Reader 8.0 is installed on the dependent host at C:\Program Files\Adobe\Acrobat 8.0\Reader\AcroRd32.exe, open the Admin Console on the relay server and type this path location in the **Location** box in the **Add Application** dialog.

Note: Before publishing an item on a mapped drive, verify that the drive is mapped to the same drive letter and location on the dependent hosts as it is on the relay server.

Host Selection

When a client connects to a relay server, the relay server attempts to start a session on the dependent host that has the lowest number of running sessions as a percentage of the maximum number of sessions allowed for the host.

If the session fails to start on the selected host, the relay server successively attempts to start the session on other available hosts until it finds one that can support the session.

If there are no available hosts (i.e., if the number of running sessions on All Hosts equals the maximum number allowed), Uniface Anywhere displays a message to the user:

You are already running as many sessions as you are allowed.

Otherwise, if the session cannot be started on any of the available hosts, the following message is displayed to the user:

Uniface Anywhere failed to launch the Program Window for your session.

In a relay server setting, Uniface Anywhere checks the maximum sessions settings on the relay server and its dependent hosts. The maximum sessions value on the relay server is the maximum number of sessions that can be run concurrently on all dependent hosts assigned to that relay server.

To modify the **Maximum sessions on this host** setting, open the Admin Console on the host, click Host Options | Session Startup.

Relay Server in a DMZ

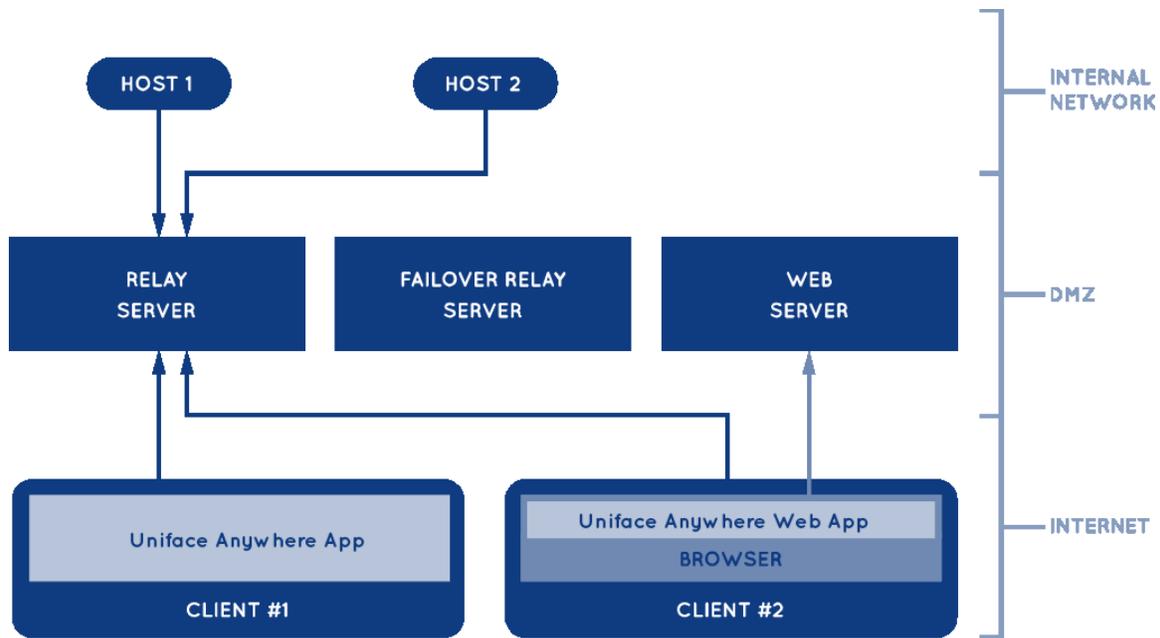
A relay server in a DMZ can be separated from its dependent application servers by a firewall, with the following requirements:

- The dependent application server must be able to connect to the relay server from behind the firewall. Please note that the reverse is *not* required. The relay server does not need to be able to connect to the dependent application server.
- The client must be able to connect to the relay server in the DMZ.

When a session starts on a dependent application server, the dependent application server opens a connection to the relay server. When the relay server receives data from the session's clients, it forwards the data to the session over this connection. Similarly, when the relay server receives data from the session over this connection, it forwards the data to the session's clients.

The relay server generally has two network interfaces: one that is accessible from clients outside the DMZ, and one that is accessible from dependent application servers behind the firewall.

The diagram below illustrates the recommended configuration for providing access to hosts on an internal network. The arrows show the direction in which the connections are made. Hosts connect to the relay server, not the other way around. As a result, the internal firewall does not need to allow any connections from the DMZ to the internal network. With this configuration, neither machines on the internet nor machines in the DMZ can connect directly to the hosts on the internal network. It is a highly secure configuration.



Relay Server Failure Recovery

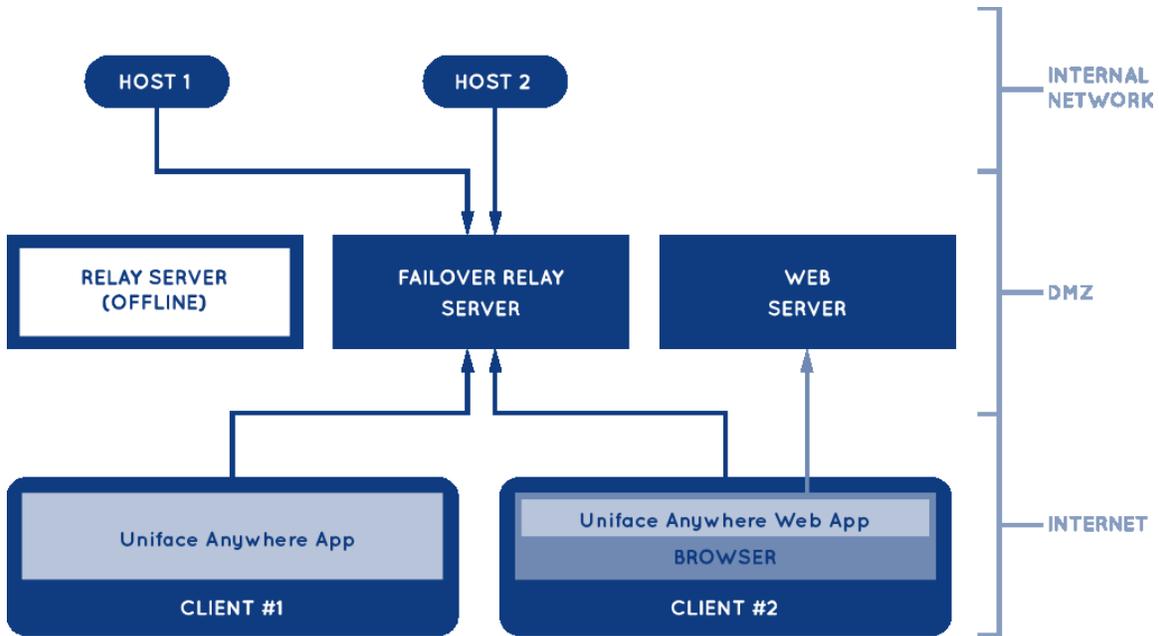
The Application Publishing Service can be configured to automatically restart if the service fails. If the Application Publishing Service stops on a relay server, clients are disconnected but sessions continue to run on the dependent hosts that were connected to the relay server. These dependent hosts will attempt to reconnect to the relay server every 15 seconds. When a dependent host reconnects to the relay server, it re-adds its sessions to the relay server and restores any state information associated with the disconnected sessions. Clients are then able to reconnect to their sessions. By default, clients automatically attempt to reconnect to the relay server 5 times. In order to provide higher service availability, a failover relay server can be configured.

To configure a failover relay server

1. Install the Uniface Anywhere Host on a separate computer, on the same network as the relay server. This computer will be the failover relay server. All clients and dependent hosts must be able to connect to the failover relay server. If clients connect to the cluster from the internet, the failover relay server must have a public address.
2. Configure the Uniface Anywhere Host to run as a relay server:
 - a. Run the **Admin Console** on the computer.
 - b. Click Tools | Host Options.
 - c. Click the **General** tab.
 - d. Type the computer's address in the **Relay server** field.
 - e. Click **OK**.
 - f. Restart the Application Publishing Service.

3. Export the published applications from the primary relay server and import them into the failover relay server:
 - a. On the primary relay server, run Regedit as administrator.
 - b. Select the following registry key:
`\HKEY_LOCAL_MACHINE\Uniface\Uniface Anywhere\AppServer`
 - c. Click **File | Export...**
 - d. Type a name for the file (e.g., Appserver.reg).
 - e. Click **Save**.
 - f. Copy the file to the failover relay server.
 - g. Double-click the file.
 - h. Click **Yes** to import the file.
 - i. Click **OK**.
4. Configure each dependent host so it will connect to the failover relay server when it is unable to connect to the primary relay server:
 - a. Run the Admin Console
 - b. Click Tools | Host Options.
 - c. Click the **General** tab.
 - d. Enter the addresses of both relay servers in the **Relay server** field, with their fully-qualified domain names. Enter the address of the primary relay server first, followed by a semi-colon, followed by the address of the failover relay server. For example:
`primary_relay_server.www.uniface.com;failover_relay_server.www.uniface.com`
 - e. Click **OK**.
5. Specify the addresses of both the primary and the failover relay servers in the URLs and shortcuts that are used to start the clients:
 - a. Provide users that connect via a browser with an HTML page or URL that sets the **host** parameter to the address of the primary relay server, followed by a semi-colon, followed by the address of the failover relay server (e.g., `host=primary_relay_server_address;failover_relay_server_address`).
 - b. Provide users that connect via an installed client, with a shortcut that sets the **-h** command line argument equal to the address of the primary relay server, followed by a semi-colon, followed by the address of the failover relay server (e.g., `-h primary_relay_server_address;failover_relay_server_address`).

In this configuration, if the primary relay server fails for any reason, dependent hosts and clients automatically reconnect to the failover server and users are generally reconnected to their sessions within 1-2 minutes of the primary relay server failure. This is illustrated in the diagram below.



If users' sessions fail to reconnect automatically, increase the value of the **autoreconnect** parameter in client URLs, web pages and shortcuts to a number greater than 5 (the default).

When the failover relay server is active (i.e., when dependent hosts are connected to the failover relay server), users' sessions will take longer to start. For this reason, the primary relay server should be re-activated when it comes back online. To re-activate the primary relay server, terminate the `aps.exe` process on the failover relay server using Task Manager at a time when users are unlikely to be connected to the cluster. When the `aps.exe` process is terminated on the failover relay server, dependent hosts and clients will reconnect to the primary relay server. Then, after the cluster's dependent hosts have reconnected to the primary relay server, restart the Application Publishing Service on the failover relay server.

Note: When the **Application Publishing Service** is stopped or restarted on a relay server via **Services**, Uniface Anywhere closes all the sessions that are running on the relay server's dependent hosts. Therefore, if you need to re-activate a primary relay server when there are sessions running on the cluster's dependent hosts, don't restart the Application Publishing Service on the failover relay server via **Services**; instead, terminate the `aps.exe` process on the failover relay server using Task Manager, as described above.

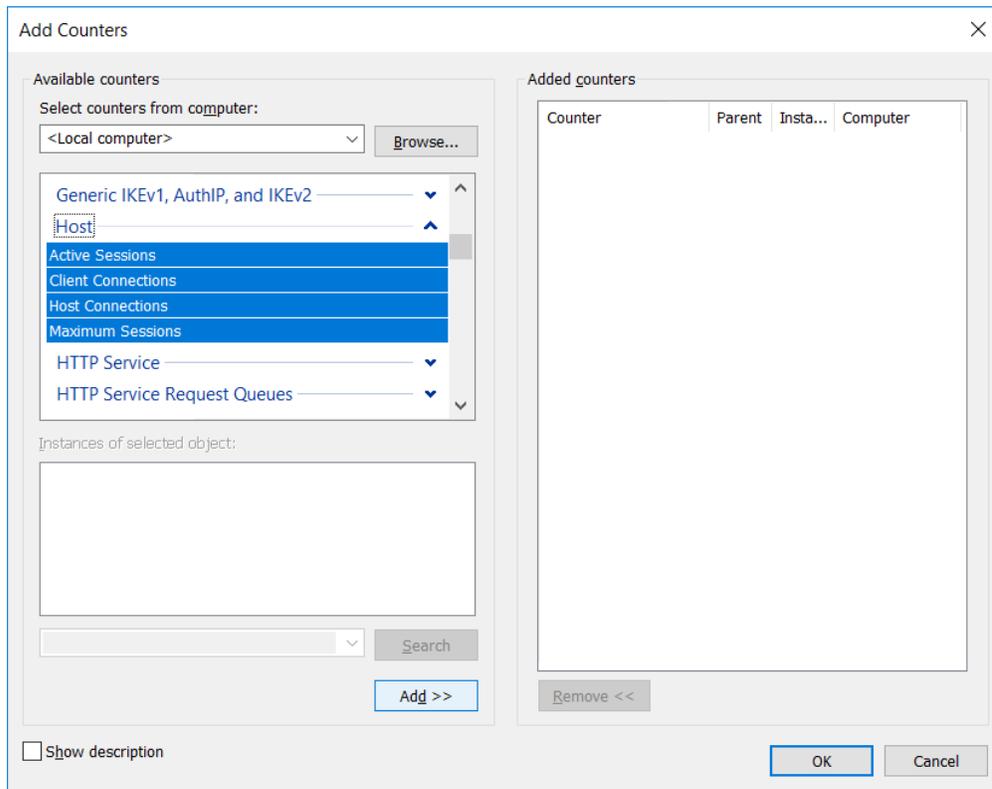
Uniface Anywhere Host Performance Counters

Uniface Anywhere Host performance counters can be added to the Windows Performance Monitor to track the number of active sessions and the number of clients connected to a host. Performance counters can also be added to track the number of hosts connected to a relay server and to identify the maximum number of sessions allowed on a host.

Uniface Anywhere Host performance counters allow administrators to monitor host activity from any machine with network access to a Uniface Anywhere Host. The Remote Registry Service (Regsvl.exe) must be enabled for remote performance monitoring to work.

To add Uniface Anywhere Host Performance Counters to the Performance Monitor

1. Click Start | Programs | Administrative Tools | Performance Monitor.
2. Click **Performance Monitor**, then click the **+** button to add counter(s).
3. From the **Available counters** list, locate and click **Uniface Anywhere Host**.
4. Click the **Add >>** button to add the four counters (Active Sessions, Client Connections, Host Connections, Maximum Sessions).
5. Click **OK**.



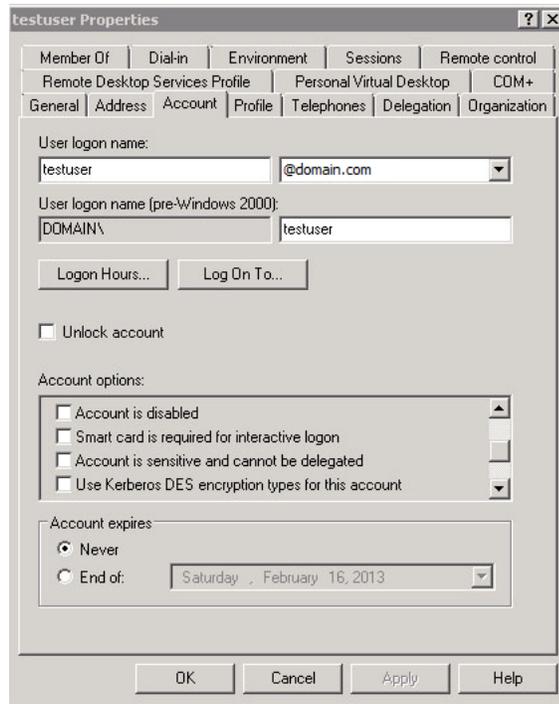
Uniface Anywhere Host Performance Counters include:

- **Client Connections.** The total number of client connections on independent hosts or relay servers. This value is always zero for dependent hosts.
- **Host Connections.** The total number of dependent hosts connected to a relay server. This value is always zero for independent or dependent hosts.
- **Active Sessions.** For independent or dependent hosts this is the number of sessions running on the host. For a relay server this is the total number of sessions hosted on all connected dependent hosts.
- **Maximum Sessions.** This displays the **Maximum Session Count** set in the Admin Console's **Host Options** dialog.

Configuration Requirements for Delegation Support

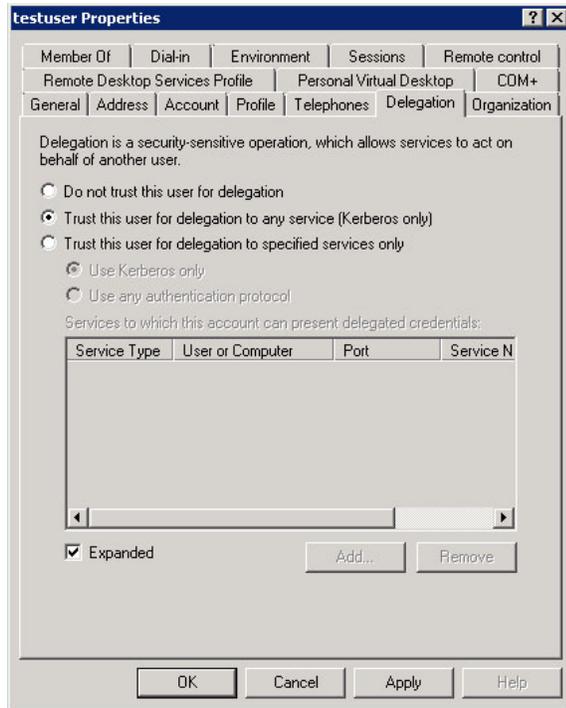
As described in Chapter 4, when Integrated Windows Authentication is used without the **Cache passwords on the host** option, Windows delegation may be required to access some network resources. For example, Group Policy may not be applied properly if delegation is not enabled. The configuration requirements for delegation support are as follows:

- Delegation requires the Kerberos authentication protocol and an Active Directory Domain.
- The Domain Name System (DNS) servers must support Service Location (SRV) resource records. It is also recommended that DNS servers provide support for DNS dynamic updates. Without the DNS dynamic update protocol, administrators must manually configure the records created by domain controllers and stored by DNS servers. The DNS service provided with Windows 2000 or later supports both of these requirements.
- The computers hosting the Uniface Anywhere client, the Uniface Anywhere Host, and any backend services, such as email or a database, must support Kerberos.
- The client's user account must support being delegated by the Uniface Anywhere Application Publishing Service. In the **Active Directory Users and Computers** Management Console, select the user and click **Action | Properties**. Click the **Account** tab. In the Account options list box, scroll down and ensure the **Account is sensitive and cannot be delegated** option is disabled. Enable the **Account is trusted for delegation** option.

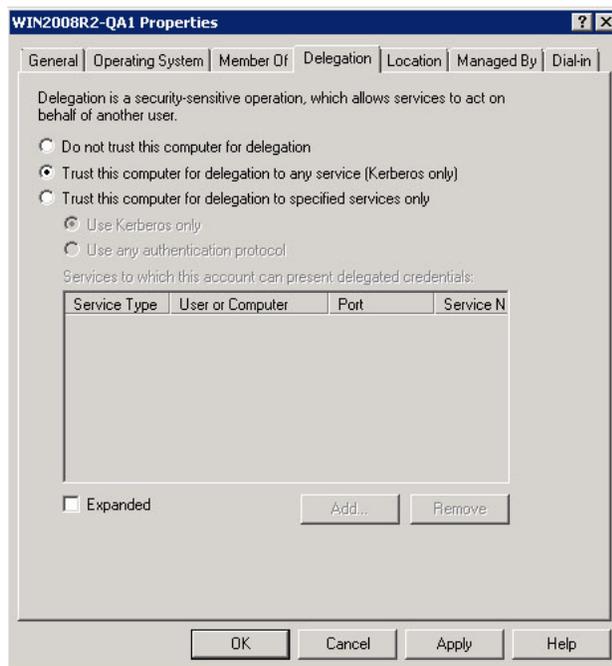


- If the Delegation tab is missing from the Properties dialog in Windows Server 2008, this is by design. The Delegation tab will only be displayed after a Service Principle Name (SPN) is created for the user account.

From an elevated command prompt, run the command `setspn -A HTTP/intranet.domain.local DOMAIN\Account`. Search for the `DOMAIN\Account` in Active Directory. The **Delegation** tab will now appear in the Properties dialog. Select **Trust this user for delegation to any service (Kerberos only)**.

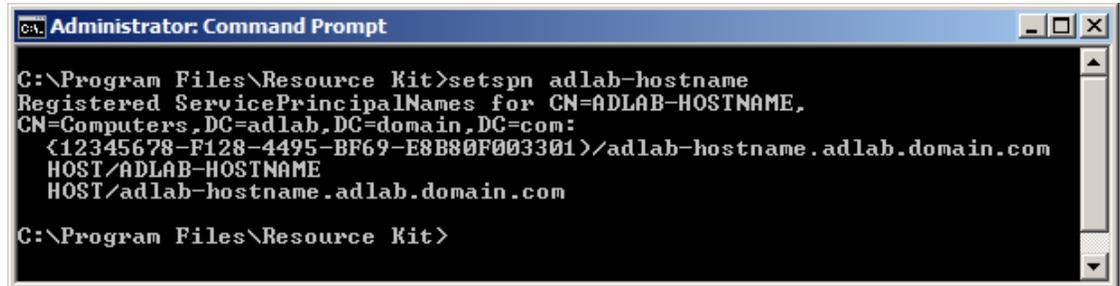


- The Uniface Anywhere Host must have the right to delegate the user's account to other computers. In the **Active Directory Users and Computers** Management Console, select the computer and click **Action | Properties**. Click the Delegation tab. Enable **Trust computer for delegation to any service (Kerberos)**. The Uniface Anywhere Application Publishing Service must be configured to run in the Local System account for these delegation rights to apply.



Note: After enabling **Trust Computer for delegation to any service (Kerberos only)** in the Active Directory, the Uniface Anywhere Host must be restarted in order for delegation to take effect.

- The **Uniface Anywhere Application Publishing Service** must be able to register its Service Principle Name (SPN) with the Active Directory. It attempts to do this every time the service is restarted. The **setspn.exe** utility (available in the Microsoft Resource Kit and as a separate download from Microsoft) can be used to verify the SPN is properly set. The following Command Window shows output obtained from **setspn.exe** when run on the Uniface Anywhere Host.



```
Administrator: Command Prompt
C:\Program Files\Resource Kit>setspn adlab-hostname
Registered ServicePrincipalNames for CN=ADLAB-HOSTNAME,
CN=Computers,DC=adlab,DC=domain,DC=com:
<12345678-F128-4495-BF69-E8B80F003301>/adlab-hostname.adlab.domain.com
HOST/ADLAB-HOSTNAME
HOST/adlab-hostname.adlab.domain.com
C:\Program Files\Resource Kit>
```

Replace **adlab-ggserver** with the computer name of your Uniface Anywhere Host. The {54094C05-F977-4987-BFC9-E8B90E088973} Globally Unique Identifier (GUID) is specifically used by the Uniface Anywhere Application Publishing Service to create the {54094C05-F977-4987-BFC9-E8B90E088973}/adlab-ggserver.adlab.www.uniface.com SPN.

The following Command Window shows output obtained by running **setspn.exe** on the Uniface Anywhere Host and indicates a network configuration error. If all the above requirements are met, this should not occur.



```
C:\WINNT\system32\cmd.exe
C:\Program Files\Resource Kit>setspn adlab-ggserver
Failed to bind to DC of domain ADLAB, 0x6ba
C:\Program Files\Resource Kit>_
```

Client Printing

Uniface Anywhere supports client-side printing on all client platforms. By default, Uniface Anywhere automatically detects the client's default printer information once the user has signed in to the Uniface Anywhere Host. This includes the default printer's port and printer driver. If the printer driver is not installed on the Uniface Anywhere Host, Uniface Anywhere will attempt to locate the driver and automatically install it.

When running applications on Uniface Anywhere Hosts, users can print to network printers and to printers that are directly connected to their computers (e.g., via serial, parallel and USB ports).

Administrators can control which, if any, printers are made available to users using the **-ac** and **printerconfig** Uniface Anywhere startup parameters.

When running Uniface Anywhere from a shortcut, use the **-ac** parameter with "all", "none" or "default" to respectively make all, none or only the default printer available from applications running on the Uniface Anywhere Host. For example, to make all printers available, create a shortcut with the target specified as follows: "C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -ac all

Similarly, when running Uniface Anywhere from the logon page, use the **printerconfig** parameter with "all", "none" or "default". For example, the following parameter will make all printers available: **<http://hostname/UAnywhere/logon.html?printerconfig=all>**

If no options are specified, Uniface Anywhere automatically configures the user's default printer only.

Note: The **Print Spooler Service** must be running on the Uniface Anywhere Host in order to configure client printers.

Designating Access to Printer Drivers

Uniface Anywhere can obtain printer drivers from the following sources:

- **Universal Printer Driver:** Uniface Anywhere includes a **Universal Printer Driver** that can print to any client printer. Enable this option to allow the use of the Universal Printer Driver for configuring client printers.
- **Windows Printer Drivers:** Enable the **Windows Printer Drivers** option to allow printers to be configured using already installed native drivers.

When only the **Universal Printer Driver** is enabled, only the Universal Printer Driver will be used as a printer driver. No native drivers will be used. This is the default setting.

When **Windows Printer Drivers** is enabled, native printer drivers that are installed on the host will be used. If a printer's native driver is not installed, or if a printer's native driver is a Type 4 printer driver (which Uniface Anywhere does not support), that printer will be configured to use the Universal Printer Driver if the **Universal Printer Driver option** is checked. Otherwise, if the Universal Printer Driver option is not checked, the printer will not be available to users.

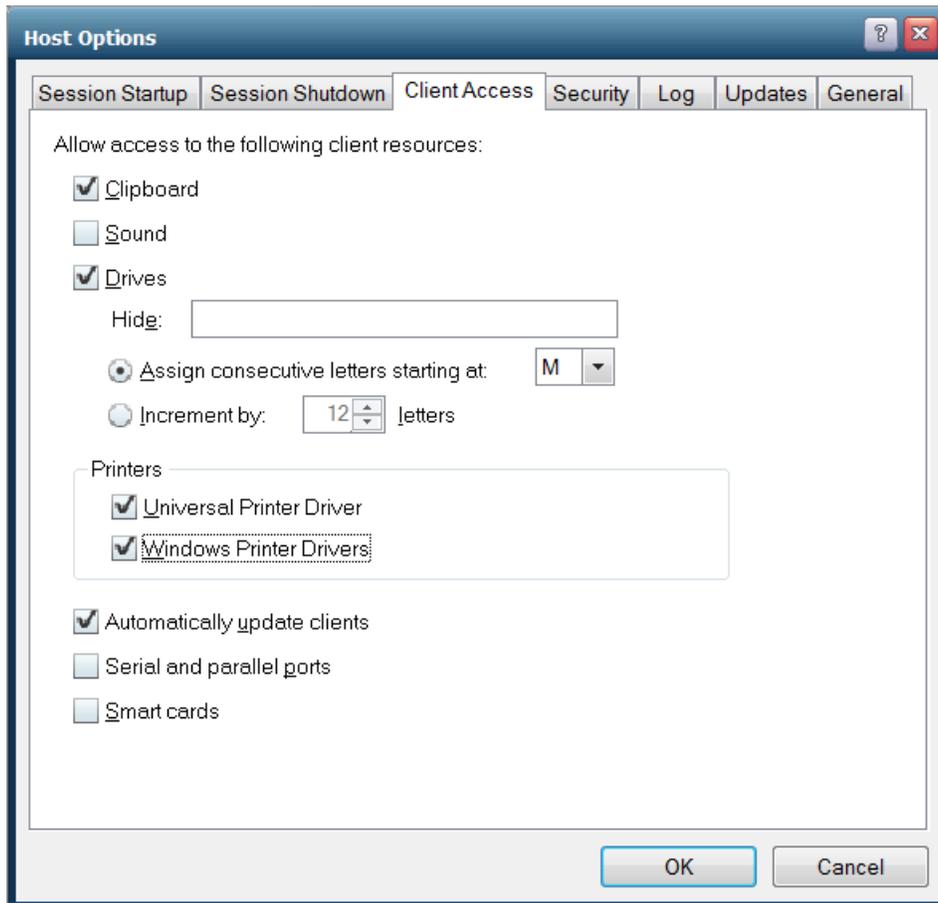
When neither the **Universal Printer Driver** or **Windows Printer Drivers** is enabled, no printers will be configured and client printing is disabled.

The Universal Printer Driver is supported on Windows, Linux, and Mac OS X. When printing with the Universal Printer Driver, the user (or group) needs to have full access to the temp directory.

A printer named **Preview PDF** is configured in each session when the Universal Printer Driver is enabled. Documents printed to this printer are automatically converted to a .pdf file and displayed on the client computer. Users can save, print, or email the document at their discretion. A PDF reader, such as Adobe Reader, is required on the client computer in order to use the Universal Printer Driver's PDF conversion feature.

Note: The **Universal Printer Driver** uses a standard printing properties dialog and may not offer some of the more advanced printing options other drivers do.

Administrators set access to printer driver sources through the **Host Options** dialog.



To designate access to printer drivers

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Printers** check box.
5. Click the box beside the desired driver source or sources.
6. Click **OK**.

Client-side printing is enabled by default. Administrators disable client-side printing through the Admin Console's **Host Options** dialog.

To disable support for client printers

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Disable **Universal Printer Driver** and **Windows Printer Drivers**. When neither of these options is selected, client printing is disabled.
5. Click **OK**.

Printer Configuration

When Uniface Anywhere clients connect to a host, **proxy printers** are automatically created on the host and serve as an interface for printing to the client printer. Proxy printers are printers Uniface Anywhere sets up on the host as a bridge between the applications running in a Uniface Anywhere session and the client printers. Proxy printers can be configured automatically or manually.

Native printer drivers are preferred when configuring proxy printers — *if* they are available and *if* settings allow them to be used. Alternatively, the **Universal Printer Driver** can be used when the native driver is not available.

There are several methods an administrator can use to manage which printer drivers should be used when creating proxy printers. Settings from client printers are replicated in their proxy printer counterpart. A session's proxy printers are removed when the session ends. Proxy printers are not removed when a session disconnects. All proxy printers on the system are removed when the Application Publishing Service starts.

When a proxy printer is configured, there is a hierarchy of preferences when selecting a native printer driver. If the **Windows Printer Drivers** option is disabled in the Admin Console, this hierarchy is not applied.

Native drivers are selected in the following order:

- **Printers Applet.** A user's manual selection of a printer driver in the Printers Applet takes precedence over all other driver selection methods.
- **Mapped Printer Drivers.** MappedPrinterDrivers.xml contains a list of driver names that can be used for each driver. This file is generated by the Application Publishing Service, but can also be manually edited by administrators.
- **Client driver name.** The driver with the exact name of the driver that is installed on the client is used to configure the proxy printer.

Printers Applet

Uniface Anywhere's Printers Applet allows users to add and remove printers, edit printer properties, set the default printer, select a printer driver, and print test pages. The Printers Applet is accessible via the Program Window. It lists all the client printers that are configured and all the host printers that the user has access to. The list of printers depends on the printer drivers setting in the Admin Console as well as the `-ac` and `printerconfig` parameters.

Icons in the Printers Applet are described below.

	Indicates that the printer is installed on the client
	Indicates the default printer, which is installed on the client
	Indicates the printer is installed on the host
	Indicates the default printer, which is installed on the host

Settings made with the Printers Applet are saved the next time the user signs in to Uniface Anywhere. These settings take precedence over command-line options. Printer changes made in the Printers Applet take effect immediately. Users do not need to restart their session.

Adding and Removing Printers

When a printer is added or removed via the Printers Applet, it does not add or remove it from the client computer, it only determines which printers are configured for use with Uniface Anywhere.

To add a client printer

1. From the Program Window, click File | Printers.
2. Click the **Add** button.
3. From the **Add Printer** dialog, select the desired printer and click **Add**. This adds the printer to the list of configured printers and is now available for use.

Note: When a printer is added through the Printers Applet, it gets configured at startup regardless of the `-ac` command-line option or `printerconfig` parameter.

To remove a printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Remove** button.

Removing a printer from the list prevents it from being configured the next time the user starts a Uniface Anywhere session. The printer can be re-added to the list at any time by clicking the **Add** button and selecting it from the list.

Setting the Default Printer

Users can specify their default printer in the Printers Applet. The default printer is indicated by a black circle and checkmark above the printer. Any printer, including host printers, can be designated as the default.

To set the default printer

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Set Default** button.

Editing Printer Settings

Through the Printers Applet, users can edit printer settings such as layout orientation and paper size.

To edit printer settings

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Edit** button.
4. Edit the properties, as desired, and click **Ok**.

Printing a Test Page

From the Printers Applet, users can print a test page to verify that the printer has been properly configured and to check if a printer is printing graphics and text correctly. A test page also displays information such as the printer name, model, and driver software version, which may be helpful for troubleshooting printer problems.

To print a test page

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Test Page** button.

Changing a Printer's Driver

Through the Printers Applet, users can select different drivers for their printers. This is useful if a driver is not working properly or if a user wants to switch between native drivers and the Universal Printer Driver.

To select a new driver

1. From the Program Window, click File | Printers.
2. Select the desired printer from the list.
3. Click the **Driver** button to open the **Select Printer Driver** dialog, which lists the drivers currently installed on the Uniface Anywhere Host machine.
4. Select a new driver, and click **Ok**. The printer is now configured with the new driver.

When only the Universal Printer Driver has been designated as a driver source in the Admin Console, users are unable to change drivers. Users cannot change the driver for Uniface Anywhere's Preview PDF printer or for server-based printer.

Resetting Printer Settings

At any time, users can reset printer data to its default settings, including preferences and printer settings. This may be useful if printers are not configuring properly or if users are experiencing printer issues.

To reset printer settings

1. From the Program Window, click File | Printers.
2. Click **Reset Printers**.

Resetting printer settings removes all proxy printers from the session. Users must restart their session in order to print to client printers again. This also resets the default printer to its original default setting.

Mapping Printer Drivers

Administrators can map printer drivers by editing **MappedPrinterDrivers.xml**. For most Uniface Anywhere deployments, administrators will not need to edit this file. It is used for specifying which driver to use when a host's driver name does not identically match the client's, or when the administrator wants to override native drivers and force clients to use a different printer driver or the Universal Printer Driver.

To specify a different printer driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\Uniface\Uniface Anywhere.
2. Open the file in Wordpad and search for the client printer driver name, for example,

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name= "HP LaserJet 2100 Series PS"> </alternate_driver_name>  
</driver>
```
3. Delete the alternate driver name from the alternate_driver_name entry. In the example above, delete HP LaserJet 2100 Series PS and replace it with the desired printer driver.
4. Save the file. This change will take effect the next time the user starts a Uniface Anywhere session.

In the example above,

```
<driver name="HP LaserJet 2100 Series PS">
```

is the driver that is used on the client.

```
<alternate_driver_name= "HP LaserJet 2100 Series PS" >
```

is the driver that should be mapped to on the host.

Mapping printer drivers can also be used to force printers to use the Universal Printer Driver.

To force the printer to use the Universal Printer Driver

1. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\Uniface\Uniface Anywhere.
2. Open the file in Wordpad and search for the client printer driver name, for example,

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name= "HP LaserJet 2100 Series PS"> </alternate_driver_name>  
</driver>
```
3. Delete the driver name from the value field. In the example above, delete HP LaserJet 2100 Series PS and replace it with Universal Remote Printer, as follows:

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name="Universal Remote Printer"> </alternate_driver_name>  
</driver>
```
4. Save the file.

The next time users connect to the host, their printer will be configured using the Universal Printer Driver.

Multiple alternate drivers can be specified using additional `<alternate_driver_name>` entries.

To designate an additional driver

1. Locate **MappedPrinterDrivers.xml** in `C:\ProgramData\Uniface\Uniface Anywhere`.
2. Open the file in a text editor and search for the client printer driver name, for example,

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name="HP LaserJet 2100 Series PS"> </alternate_driver_name>  
</driver>
```
3. Specify an additional driver. For example, add HP LaserJet 2100 Series PS to the list, as follows:

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name="HP LaserJet 2100 Series PS"> </alternate_driver_name>  
<alternate_driver_name="HP LaserJet 2200 Series PS "> </alternate_driver_name>  
</driver>>
```
4. Save the file.

Administrators can add an unlimited number of drivers. Uniface Anywhere attempts to configure client printers using the drivers in the order they are specified.

To remove printer driver mapping

1. Open **MappedPrinterDrivers.xml** in a text editor and delete the entire modified line. For example, delete:

```
<driver name="HP LaserJet 2100 Series PS">  
<alternate_driver_name=" HP LaserJet 2100 Series PS "> </alternate_driver_name>  
</driver>
```
2. Save the file.

The **MappedPrinterDrivers.xml** file can be deleted to remove any prior changes. The file is recreated when users sign in to the host.

Note: Client printers are temporarily installed on the Uniface Anywhere Host for the duration of the client's session. Printer drivers are installed permanently. Administrators can view the list of printers and drivers in the Printers folder on the Uniface Anywhere Host.

Exporting Printer Settings to a File

Most printers store their settings in the Windows DEVMODE structure. Uniface Anywhere saves the contents of each printer's DEVMODE structure when users sign out and restores these settings when printers are re-created when users sign back in. In some cases, printing problems may arise when a printer does not store all of its settings in the DEVMODE structure.

Administrators can add the entry, `<export_printer_settings>true</export_printer_settings>` to **MappedPrinterDrivers.xml** so when a user saves the settings for a printer, the settings will be written to a file rather than to the Windows DEVMODE structure.

To export printer settings to a file

1. Locate **MappedPrinterDrivers.xml** in `C:\ProgramData\Uniface\Uniface Anywhere`.
2. Open the file in a text editor and search for the client printer driver name, for example,
`<driver name="HP LaserJet 2100 Series PS">`
`<alternate_driver_name="HP LaserJet 2100 Series PS"> </alternate_driver_name>`
`</driver>`
3. Add the entry `<export_printer_settings>true</export_printer_settings>`, as follows:
`<driver name="HP LaserJet 2100 Series PS">`
`<alternate_driver_name="HP LaserJet 2100 Series PS">`
`<export_printer_settings>true</export_printer_settings>`
`</alternate_driver_name>`
`</driver>`
4. Save the file.

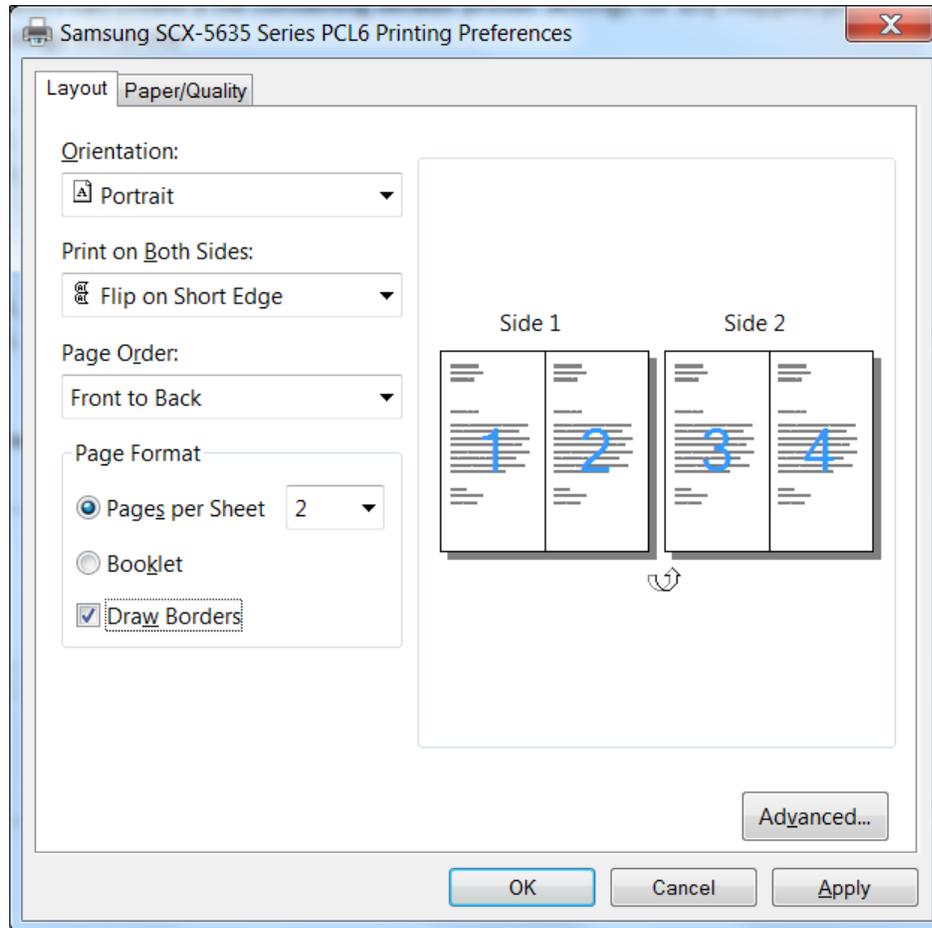
If `<export_printer_settings>` is set to false, printer settings will be stored in the DEVMODE structure.

Creating a Default Printer Setting File for a Mapped Printer

Administrators can create a file containing default printer settings for any mapped printer. Adding the entry `<default_printer_settings_file>` and specifying a printer settings file in **MappedPrinterDrivers.xml** allows administrators to specify default settings for a printer if the user's individual file does not exist, either because `<export_printer_settings>` is set to false or the user hasn't made any changes to the printer settings yet. After setting printer preferences, export the settings to a file, then add the default printer settings file to **MappedPrinterDrivers.xml**.

To set printer preferences

1. From the Control Panel, select **Devices and Printers**.
2. Right-click the desired printer and select **Printing Preferences**.
3. Edit the printer's preferences and click **Apply**.
4. Click **OK** to close the **Printing Preferences** dialog.



To export the new printing settings to a file

Run a Command Prompt as Administrator and type the following command:

```
rundll32.exe printui.dll PrintUIEntry /Ss /n "printer name" /a "full path to settings file"
```

For example,

```
rundll32.exe printui.dll PrintUIEntry /Ss /n "HP Officejet Pro 8600" /a
"C:\printersettings\Officejet.dat"
```

To create a default printer settings file in MappedPrinterDrivers.xml

1. Stop the **Uniface Anywhere Application Publishing Service**.
2. Locate **MappedPrinterDrivers.xml** in C:\ProgramData\Uniface\Uniface Anywhere.
3. Add the following:

```
<driver name="printer driver name">
<alternate_driver name="alternate driver name">
<export_printer_settings>true</export_printer_settings>
<default_printer_settings_file>"full path to settings file" </default_printer_settings_file>
</alternate_driver>
</driver>
```

For example:

```
<driver name="HP Officejet Pro 8600">
<alternate_driver name="OfficeJet Driver 1">
<export_printer_settings>true</export_printer_settings>
<default_printer_settings_file>"C:\printersettings\Officejet.dat."</default_printer_settings_file>
</alternate_driver>
</driver>
```

4. Save the file. This change will take effect the next time the user starts a Uniface Anywhere session.
5. Start the **Uniface Anywhere Application Publishing Service**.

Client Printer Naming Customization

Uniface Anywhere installs a printer on the host for each printer that is configured on the client machine. These printers are called proxy printers and are the printers that are seen by users when printing via Uniface Anywhere. Since multiple users connect to a Uniface Anywhere Host, these printers must be filtered so that users see only their own printers. This requires that each printer be assigned a unique identifier.

Through the Registry, administrators can specify the format of these proxy printer names and include information such as the user's name, the client computer's IP address, and the client machine name. The **PrinterNameFormat** Registry key is created after a Uniface Anywhere session is started.

Administrators can choose from the following tokens to create a suffix to the printer string name:

Token	Description	Example
%U	The user name	Wilson
%I	The client IP address	192.168.100.147
%M	The client's unique ID (GUID)	800fb6b5770-ed9e-11df-82ae-000874b1cdb1
%C	The client machine name	HRWorkstation
%S	The Uniface Anywhere session ID	7

To customize the client printer name

1. Run the Registry Editor (regedit.exe)
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **PrinterNameFormat** key:
[HKLM\Software\Uniface\Uniface Anywhere\AppServer\PrinterNameFormat]
4. Right-click **PrinterNameFormat** and select **Modify**.
5. In the **Value data** field, type one or more of the client printer customization tokens.
6. Close the Registry Editor.

The PrinterNameFormat key is set to (from %C) by default. Using the above examples, printer names would appear as: PrinterName (from HRWorkstation)

Any special characters other than % in the PrinterNameFormat string are taken literally, since they are not tokens.

There are 12 characters that are not allowed. These characters are ! , \ = / : * ? " < > and | . If any of these characters are used in the string, they are replaced with a hyphen.

Adjusting the Printable Area

In some cases, applications that print using the Uniface Anywhere Universal Printer Driver (UPD) will have areas of the document that are clipped — when portions of the document near the edges of the page are not printed. There are two methods for addressing this issue: by defining the printable area of a document with an alternate .PPD file, or by enabling print job scaling.

The first method requires installing an alternate .PPD file.

To install the alternate .PPD file

1. Download **UniversalRemotePrinter.ppd** from:
<https://www.uniface.info/display/TI/Uniface+Anywhere+Technical+Information>
2. Stop the **Application Publishing Service**.
3. Copy **UniversalRemotePrinter.ppd** to the following folders:
C:\Windows\System32\spool\drivers\x64\3
4. Delete **UniversalRemotePrinter.bpd** if it exists.
5. Start the **Application Publishing Service**.

The UniversalRemotePrinter.ppd file defines driver settings for the Universal Printer Driver. In the default version of this file, the area to which the driver can print is the full extent of a page. This means that text or images can be printed to the edges of a page. Most printers are not physically capable of this. The alternate .PPD file defines a 1/4 inch (6.35 mm) margin for the defined paper sizes. This allows applications to predict the printable area and thereby lay out print jobs without clipping.

The second method requires enabling print job scaling by setting the **EnablePrintOptions** property to true in the **HostProperties.xml** file. Or, if the host has been upgraded, edit **HostPropertyDefinitions.xml**.

To enable print job scaling

1. Stop the **Application Publishing Service**.
2. Open %PROGRAMDATA%\Uniface\Uniface Anywhere\HostProperties.xml in a text editor.
3. Find the **EnablePrintOptions** property and change its associated value to "true".
4. Verify that the value for the PrintOptions property is "-printerargins -xoffset 50 -yoffset 30"
5. Save **HostProperties.xml**.
6. Start the **Application Publishing Service**.

When print job scaling is enabled, print jobs that do not fit within the printable area are reduced so that the images or text fit on to the defined paper size. The scaling operation occurs in the Uniface Anywhere client application. It only affects printers configured to use the Universal Printer Driver. It does not affect the "Preview PDF" printer.

Client Clipboard

Uniface Anywhere allows client and host-based applications to exchange information using the clipboard. Users can cut and copy information from applications running on the client and paste it into applications running on a Uniface Anywhere Host, and vice versa. Clipboard support is disabled by default.

To enable client clipboard

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Clipboard** check box.
5. Click **OK**.

Client Sound

On Windows 7 and later, the Uniface Anywhere Host supports a virtual audio device that creates a private mixer for every Uniface Anywhere session. These components mix the audio played by applications running in the Uniface Anywhere session and encode it in Ogg Vorbis format. The host streams the Ogg Vorbis data to the client, and the client plays the audio.

To enable audio support

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Sound** check box.
5. Click **OK**.

A sound card must be installed on the host. Speakers are not required on the host. Client Sound is supported on Windows and the Mac OS X App. The client machine requires a sound card and speakers. Audio support is disabled by default.

Client Serial and Parallel Ports

Uniface Anywhere allows applications running on the host to access client machines' serial and parallel ports. Serial and parallel ports are disabled by default. Client serial and parallel port access is supported on Windows only.

To enable serial and parallel ports

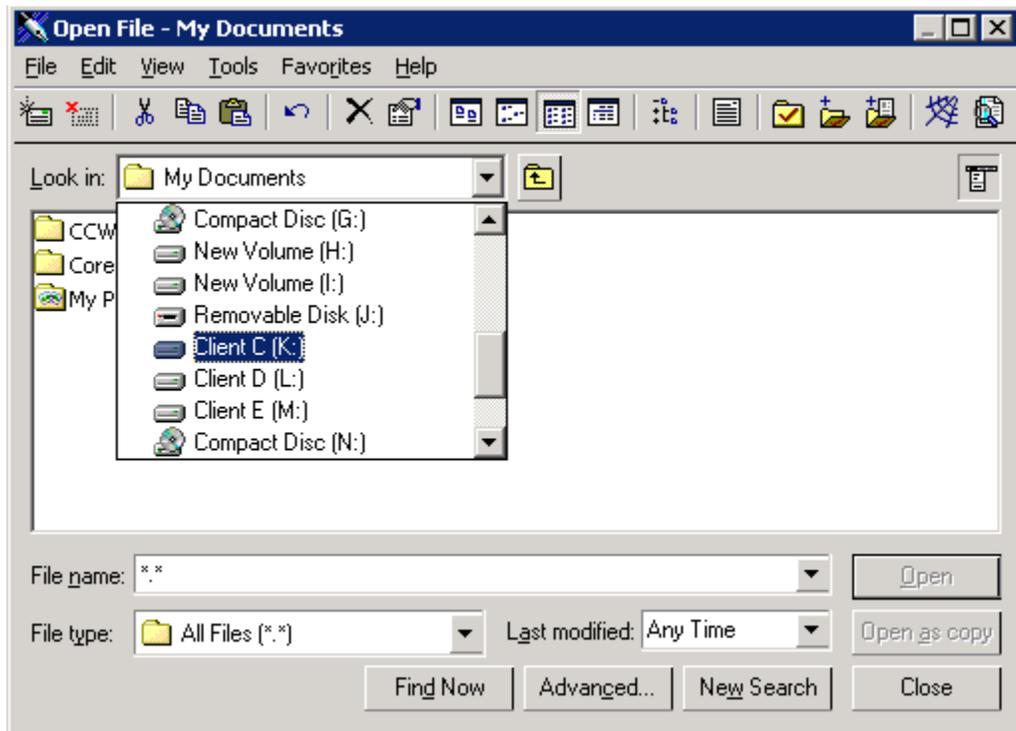
1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Serial and Parallel Ports** check box.
5. Click **OK**.

Note:

Access to serial and parallel ports requires the loading of Uniface Anywhere libraries into session processes. This can affect the startup of a process, make some processes incompatible with Uniface Anywhere, or have fatal consequences during suspend/resume operations. For information on advanced configurations options, please consult the [Advanced Session Process Configuration](#) section in this guide.

Client File Access

Uniface Anywhere allows users to access files stored on the client computer and to save files locally. Client drives will be listed in the application's **Open** and **Save as** dialog boxes, and are designated with a Client prefix. For example, Client C (K:), Client D (L:).



The dialog boxes list both client and host drives. Support for client drives is disabled by default.

To enable support for client drives

1. In the Admin Console, select the desired host from the list of **All Hosts**.
2. Click Tools | Host Options.
3. Click the **Client Access** tab.
4. Click the **Drives** check box.
5. Click **OK**.

Uniface Anywhere allows users to access USB drives. Removable media such as floppy disks, CD ROMs, and DVD-ROMs are not supported as client drives.

Remapping Client Drives

When applications are run in Uniface Anywhere sessions with the client Drives feature enabled, Uniface Anywhere must ensure there is a one-to-one mapping between drive letters and the drives of the client and host computers. If a drive on the client and a drive on the host are assigned the same drive letter, Uniface Anywhere must assign a new drive letter to one of the drives. Client drives can be remapped by either listing them sequentially starting at a given drive letter *or* incrementing their drive letters by a specified value.

To list client drives sequentially starting at a given drive letter

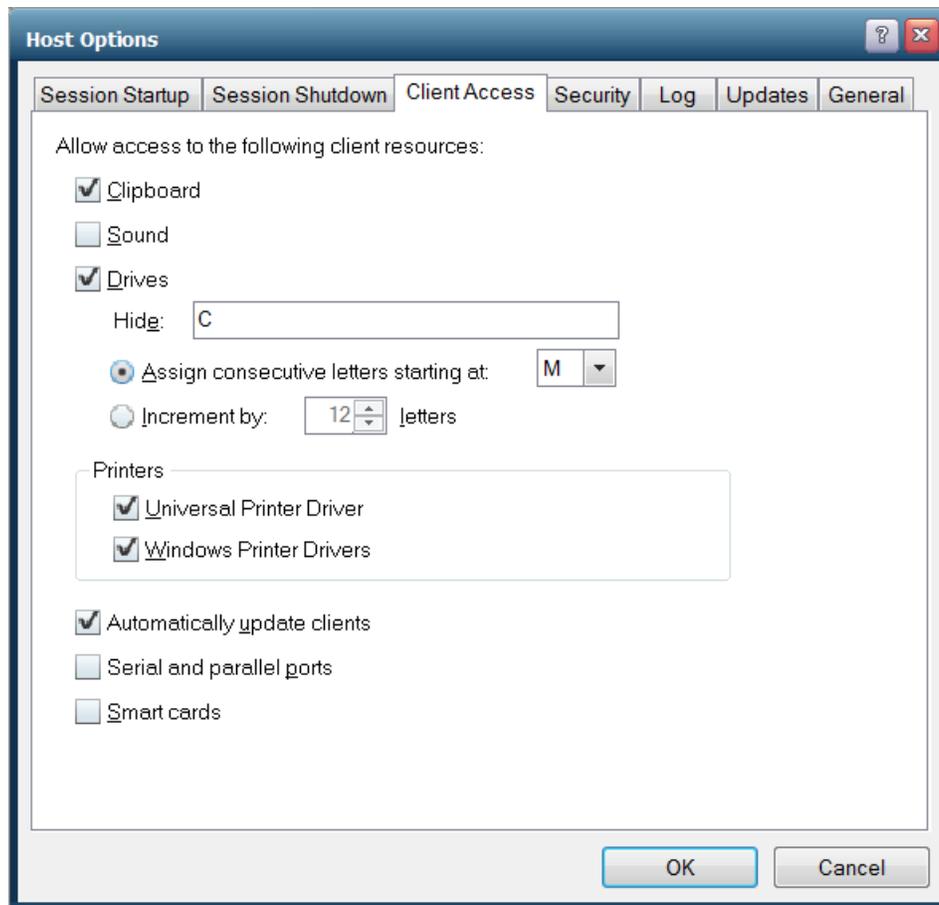
1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click **Assign consecutive letters starting at: ____**.
5. In the edit field, type the drive letter that should start the sequence.
6. Click **OK**.

For example, if a client computer has A, C, D, and H drives, and the starting point is set to drive letter M, the client's drives will be remapped respectively to M, N, O, and P. If a drive letter is already assigned to a drive, the next available letter is used. This feature is disabled by default. Once enabled, the default drive letter is M.

To increment client drive letters by a fixed value

1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. Click Increment by: ____ letters.
5. In the edit field, type a number greater than or equal to 1 that will yield the desired offset.
6. Click **OK**.

For example, if the client computer has the same drives as above (A, C, D, and H), and the offset is 12, each of the client's drives will be incremented by 12 letters. The drives will be remapped respectively to M, O, P, and T. The default value for this setting is 12.



Hiding Client Drives

Through the Admin Console, administrators can hide client drives such as the client's operating system drive and CD ROM drive, making them inaccessible to the user through Uniface Anywhere.

To hide one or more client drives

1. From the Admin Console, click Tools | Host Options.
2. Click the **Client Access** tab.
3. Enable client **Drives**.
4. In the **Hide** box, type the client drive letters you want to hide.
5. Click **OK**.

All client drives are mapped by default. Drives listed in the **Hide** box can be listed in any order. When hiding client drives on the Linux Client and the Mac OS X App, the user's home directory is mapped, in addition to the Root. For example,
 Client Home (N:)
 Client Root (O:).

Hiding Host Drives

Microsoft's Group Policy Objects lets you hide specific host drives. For instructions, see <http://support.microsoft.com/kb/231289>. To hide host drives, the **Apply Group Policy** option must be enabled in the Admin Console's **Host Options** dialog. Click the **Session Startup** tab and click **Apply Group Policy**.

Mapped Drives

Drive mappings are private within each Uniface Anywhere session. For example, if there are two sessions running on a Uniface Anywhere Host, a drive letter (H, for example) can be mapped to one network share in session 1 (e.g., \\servername\session1), and the same drive letter can be mapped to a different network share in session 2 (e.g., \\servername\session2).

Define drive letter mappings using logon scripts. You can also allow users to define their own drive letter mappings by publishing applications that provide this functionality.

Drive mappings defined within the interactive session on the Uniface Anywhere Host are not available to remote users. If all users require access to the same network share through a drive mapping, the drive mapping will generally need to be defined in a logon script.

Multi-Monitor Support

Uniface Anywhere supports multiple monitors on Windows and Mac OS X. Multi-monitor support is enabled by default, but can be disabled manually.

To disable multi-monitor support via a Uniface Anywhere shortcut

Add the argument `-mm 0` from the Uniface Anywhere shortcut.

For example, `gg-client.exe -h server1 -mm 0`

To enable multi-monitor support via a Uniface Anywhere shortcut

Append the argument `-mm 1` to the Uniface Anywhere shortcut.

For example, `ua-client.exe -h server1 -mm 1`

To disable multi-monitor support via the logon page

Set the `multimonitor` parameter to `false`.

For example, <http://hostname/UAnywhere/logon.html?multimonitor=false>

To enable multi-monitor support via the logon page

Set the `multimonitor` parameter to `true`.

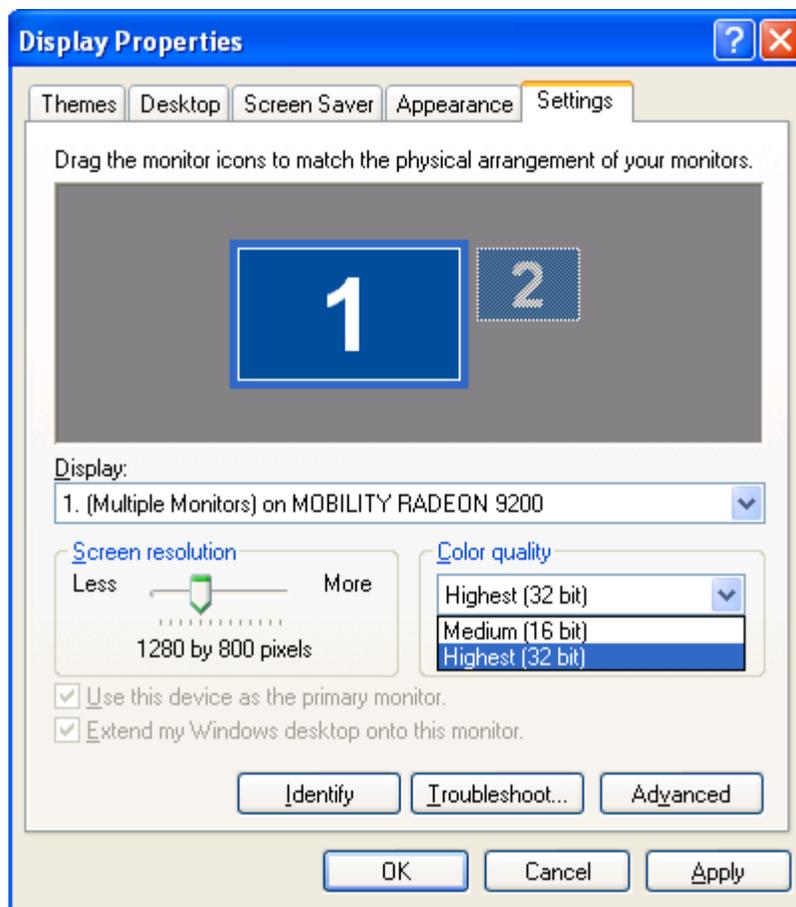
For example, <http://hostname/UAnywhere/logon.html?multimonitor=true>

Specifying the Maximum Color Depth for Uniface Anywhere Sessions

The color depth (or color quality) of a Uniface Anywhere session can affect the quality of images in some applications. Uniface Anywhere sessions will run at the color depth of the client system up to a maximum value. By default, the maximum depth is set to 16-bits per pixel.

To increase or decrease the maximum color depth of a Uniface Anywhere session, use the `-mx` option when running Uniface Anywhere from a shortcut. The maximum color depth can be specified as follows: `-mx 32`, `-mx 24`, `-mx 16`, or `-mx 8`. A Uniface Anywhere session will use the minimum value of the `-mx` option and the color depth of the client system. For example, in order for a Uniface Anywhere session to run at 32-bits per pixel, `-mx 32` must be added to the command-line and the client system must be running at 32-bits per pixel.

For example, "`C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe`" `-mx 32`



When running Uniface Anywhere from the logon page, use the **maxbpp** parameter with the values 8, 16, 24 or 32. For example, to set the maximum color depth to 24-bits per pixel, append `maxbpp=24`, as follows: <http://hostname/UAnywhere/logon.html?maxbpp=24>

Disabling Image Compression

By default Uniface Anywhere compresses all images to a maximum of 256 colors per image. As a result, complex images may lose some sharpness. To disable image compression on Uniface Anywhere clients, append `-qt 0` to the shortcut, as follows:

```
"C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -qt 0
```

To disable image compression via the logon URL, set the **quantize** parameter to false. For example, <http://hostname/UAnywhere/logon.html?quantize=false>

Please note that disabling image compression will likely result in a significant increase in bandwidth sent from the Uniface Anywhere Host.

Modifying the fontContrast Property

Font and text clarity can be adjusted by modifying the value of the **fontContrast** property in the **DefaultWorkspaceProperties.xml** file. The maximum value for **fontContrast** is 2200 and the minimum value is 1000. The property is set to 1400 by default.

To modify the fontContrast Property

1. Stop the **Application Publishing Service**.
2. Locate the **DefaultWorkspaceProperties.xml** file in the `C:\ProgramData\Uniface\Uniface Anywhere` directory.
3. Open **DefaultWorkspaceProperties.xml** in Wordpad and locate the following section:

```
</property>  
<property type="UINT32" group="Miscellaneous" id="fontContrast">  
<value>1400</value>  
</property>
```
4. Replace 1400 with the desired value.
5. Save the edited .xml file.
6. Start the **Application Publishing Service**.

Obtaining the Name of the Client Computer

For applications that require the client's computer name rather than the Uniface Anywhere Host's, administrators can add the name of that executable under the Registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere\Compatibility\GetComputerName** as a DWORD with a data value of **0x00000001**. Any time an executable matching any of the names listed under this Registry key with a data value of **0x00000001** calls the Windows **GetComputerName** API, the given buffer will be filled in with the client's name rather than the host's.

Additionally, there is an environment variable named **CLIENTCOMPUTERNAME** that exists as part of the running environment of a published application. This environment variable contains the

client's computer name. The **CLIENTCOMPUTERIPADDRESS** environment variable performs the same function, except it contains the IP Address of the client computer, rather than the computer name. The standard Windows environment variable **COMPUTERNAME** remains unchanged; its value is the host's computer name.

To obtain the name of the client computer

1. Run the Registry Editor (regedit.exe).
2. From the Registry Editor, expand the **HKEY_LOCAL_MACHINE** key.
3. Locate the **GetComputerName** key:
[SOFTWARE\Uniface\Uniface Anywhere\Compatibility\GetComputerName]
4. Create a **DWORD** entry for the executable. (For example, pw.exe).
5. Set the value of the new entry to **0x00000001**.
6. Close the Registry Editor.

When a client reconnects to a session, the **CLIENTCOMPUTERNAME** and **CLIENTCOMPUTERIPADDRESS** environment variables will be updated in each existing process once they have made an API call to acquire any environment variable. If another process attempts to acquire the environment variables of a session process prior to the session process calling one of these APIs, the value of these environment variables will not appear updated. The exact API calls that will trigger the update are:

```
UserEnv!CreateEnvironmentBlock()  
Kernel32!ExpandEnvironmentStringsA/W()  
Kernel32!GetEnvironmentStringsA/W()  
Kernel32!GetEnvironmentVariableA/W()
```

Application Script Support

Many Win32 applications were designed for installation on a client PC and run by only one user. When an application is deployed from a Uniface Anywhere Host, multiple users need to be able to run the application simultaneously, and a number of problems may be encountered if the application is not "multi-user ready."

The best way to solve multi-user deployment problems with an application is to modify the application so it properly supports multiple users. When it is not possible to modify the application, an application script may be used to perform the pre-launch configuration and post-shutdown cleanup that is required to allow the application to run in a multi-user environment. The process for creating and deploying an application script is as follows:

1. Write a batch file that:
 - Performs the tasks necessary to prepare the application environment for a user.
 - Launches the application.
 - Performs any cleanup tasks required after the application shuts down. The batch file should end with an EXIT command. Otherwise the CMD.EXE process will not shut down.
2. Publish the application script
 - a. Open the Admin Console.

- b. Click Tools | Applications | Add.
 - c. Type the path to CMD.EXE in the **Application Path** field.
 - d. In the **Command Line Options** field, specify "/K filename", where filename is the full path of the batch file to be run.
 - e. Type the application display name and specify an icon.
 - f. Click **OK**.
3. Test the application script
- a. Launch one of the Uniface Anywhere clients and connect to the Uniface Anywhere Host.
 - b. Double-click the icon for the application script. The user interface of the application should appear on the client display, and the application should be running in the environment configured by the application script.

Note: When an application script is launched using Uniface Anywhere, the CMD.EXE window is displayed only briefly. As such, the application script cannot contain any prompts for user input.

Advanced Session Process Configuration

This section covers some of the advanced configuration options that can be set for processes running within Uniface Anywhere sessions. These settings can be applied to specific executable (.exe) applications or as default settings applied to applications without specific configurations. Care should be taken when making any changes discussed in this section. An incorrect configuration can affect the startup of a process, make a process incompatible with Uniface Anywhere, or have fatal consequences during suspend/resume operations.

Most applications that run within a Uniface Anywhere session will have Uniface Anywhere libraries loaded within them to perform redirection in order to obtain desired behavior. There are two levels of redirection that these libraries can initialize.

The first level configures application and system modules to behave in a particular way. Most applications will need one or more level one settings enabled. Level one settings include Client Time Zone, Client Printing, and altered Windows API behavior.

The second level creates a communications channel between the application and client for duplex transmission of session related information. For the highest level of application compatibility with Uniface Anywhere, level two settings should be enabled in as few applications as possible. Level two settings include Client Sound and Client Serial and Parallel Ports.

The different configuration settings employed by the Uniface Anywhere libraries that redirect session processes are controlled by hexadecimal bit values within the registry. The desired bit values are logically ORed together to create a QWORD registry value. Here is the documented list of process redirector bits and a description of what they configure.

0x0000000000000001* - Prohibit a process from running within a session

0x0000000000000002 - Disable the loading of Uniface Anywhere libraries. All redirection will be disabled. The time required to perform the redirection operations is generally a small percentage of the time required to launch typical Windows applications, but it can be a large percentage of the time required to launch and run simple console applications. Some console applications do not require redirection and performing these tasks can significantly extend the time required to execute logon scripts. Including this bit allows administrators to bypass redirection of a process.

Applications execute faster since the Uniface Anywhere libraries are not loaded and initialized. This bit can also be used for applications that, for one reason or another, are incompatible with some or all of the Uniface Anywhere redirection settings.

0x0000000000000004 - Disable Client Time Zone. This bit can be used for applications that, for one reason or another, are incompatible with the Uniface Anywhere Client Time Zone redirection settings.

0x0000000000000008 - Disable Client Printing. This bit can be used for applications that, for one reason or another, are incompatible with the Uniface Anywhere Client Printing redirection settings.

0x0000000000000040* - Enable the Windows ProcessIdToSessionId() API to return the Uniface Anywhere session ID.

0x0000000000000200 - Disable Client Sound. This bit can be used for applications that, for one reason or another, are incompatible with the Uniface Anywhere Client Sound redirection settings.

0x0000000000000400 - Disable client Serial and Parallel Ports. This bit can be used for applications that, for one reason or another, are incompatible with the Uniface Anywhere Client Serial and Parallel Ports redirection settings.

0x0000000000000800* - Enable the Windows GetComputerName() API to return the client computer name. See also: **Obtaining the Name of the Client Computer**. Disable the updating of the client environment variables (CLIENTCOMPUTERNAME and CLIENTCOMPUTERIPADDRESS) when a client reconnects to a suspended session.

0x0000000000001000* - Disable, for optimization purposes, some of the normal processing performed when Explorer.exe is launched. This bit prevents Explorer.exe from launching processes listed under the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, RunOnce and RunOnceEx registry keys. This reduces the system resources needed to run Explorer in a session.

0x0000000080000000* - Enable application produced with Delphi to use the Client Serial and Parallel Ports feature. Applications built with Delphi do not properly process all return values from the Windows GetOverlappedResult() API. This bit prevents the returning of WAIT_TIMEOUT and instead returns WAIT_OBJECT_0.

0x0000000800000000* - Enable the NtQuerySystemInformation function to return the Uniface Anywhere session ID. This option may be required for .NET applications that make use of the Windows Session ID.

0x0000040000000000 - Make specific named pipes that the process creates or accesses session-private.

* Indicates advanced options that should only be used if instructed to by your support contact.

Note:

All the unlisted bits are purposely undocumented and reserved for internal Uniface use only. Do not alter any registry values that contain any unlisted bits and do not apply any unlisted bits to any Registry values you add. Uniface Anywhere Host operation will be compromised if this is done.

These bits can be combined to customize the redirector settings of specific applications or to change the default settings used by applications that do not have a Registry entry. In either case always include the default value bits set by the initial install of Uniface Anywhere, unless instructed otherwise by a support engineer.

To add custom redirector settings for a specific application

1. Click Start | Run.
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\Uniface\Uniface Anywhere\Loader\Processes.
4. Click Edit | New | QWORD value.
5. Type the name of the application's executable file. (For example, Beeps.exe.) The application's name can be specified as either a fully qualified path or as the file's base name and extension.
6. Select the new registry value.
7. Click Edit | Modify.
8. Verify that the Base selection is Hexadecimal.
9. Type the combined bits in the **Value data** edit box.
10. Click **OK**.

To make a named pipe session-private

1. Add a custom redirector setting for each process that uses the named pipe that includes the **0x0000040000000000** bit.
2. Create a **DWORD** registry value under the KEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere\System\Namedpipes registry key that identifies the named pipes that should be made session-private.
3. Set the name of the registry value equal to the string that will be compared to the name of the named pipes, and set the registry value to one of the following:
 - 1 - Make a named pipe session-private when the name of the named pipe matches the name of the registry value.
 - 2 - Make a named pipe session-private when the beginning of the name of the named pipe matches the name of the registry value.
 - 4 - Make a named pipe session-private when any part of the name of the named pipe matches the name of the registry value.

Comparison types 1 and 2 must be in the form of \\.\pipe\pipename and are made with a case-insensitive test. Comparison type 4 is case-sensitive.

To change the default redirection settings

1. Click Start | Run
2. Type Regedit.
3. Browse to the registry key: HKEY_LOCAL_MACHINE\Uniface\Uniface Anywhere\Loader\Processes.
4. Select the existing **DefaultLoaderOptions** registry value.
5. Click Edit | Modify.
6. Verify that the Base selection is Hexadecimal.
7. Type the new setting in the **Value data** edit box.
8. Click **OK**.

Example Configuration

A Uniface Anywhere host has the following applications installed and registered in the Admin Console.

- DataDownloader.exe
- DataProcessor.exe
- DataViewer.exe

The **DataDownloader.exe** executable is a Windows application that reads data from a serial device and saves it to a file. Client Sound is needed for error conditions alerts that can be signaled while data is being downloaded. Client Files Access will be used to store the data file on the client system. The Windows GetComputerName() API must be redirected so that the client computer name can be used to indicate the source of the data within the data file.

Because the serial device that contains the data is connected to the client computer, Client Serial and Parallel Ports will need to be enabled. Because this is the only process that will access Client Serial and Parallel Ports on this system, a registry entry specifically for DataDownloader.exe has been added. This minimizes the risks and overhead associated with this level two redirector setting by disabling Client Serial and Parallel Ports in all other applications.

The settings for this application are calculated as follows:

0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.

0x0000000000000800 - This is the bit that enables the Windows GetComputerName() API redirection.

0x0000000000000900 – This is the hexadecimal QWORD to be set in the DataDownloader.exe registry value.

The DataProcessor.exe executable is a console application that needs Client File Access to read in the serial data file from the client and write out the processed data file to the client. It will also use Client Time Zone to properly process the times recorded in the serial data file. All other settings will be disabled to minimize the risks and overhead associated with redirector settings.

The settings for this application are calculated as follows:

0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.

0x0000000000000008 - This is the bit that disables Client Printing.

0x0000000000000200 - This is the bit that disables Client Sound.

0x0000000000000400 - This is the bit that disables Client Serial and Parallel Ports.

0x0000000000000708 – This is the hexadecimal QWORD to be set in the DataProcessor.exe registry value.

The **DataViewer.exe** executable is a Windows application that displays the data so that it can be analyzed. It needs Client File Access to read in the processed data file from the client. It needs Client Sound so that application sounds can be heard. It needs Client Printing so that the analyzed data can be printed on paper. These are some of the settings needed by most applications, so the **DefaultLoaderOptions** registry value is used for the calculation below.

The default setting will be changed to disable the Client Serial and Parallel Ports. This can be done because the only application that uses Client Serial and Parallel Ports, DataDownloader.exe, has its own registry setting that specifically enables it.

0x0000000000000100 - These are the bits originally set in DefaultLoaderOptions.

0x0000000000000400 - This is the bit that disables Client Serial and Parallel Ports.

0x0000000000000500 – This is the hexadecimal QWORD to be set in the DefaultLoaderOptions registry value.

This example demonstrates how a combination of application specific and the default settings can be used to minimize the risk of application incompatibilities and allow an optimal environment to run in.

Running the Windows desktop in the background of Uniface Anywhere sessions

Some Windows applications use features and services that are provided by the Windows desktop (explorer.exe). Most applications run without the desktop, but some fail to start or run properly when the desktop is not running in the same session as the application. By default, the desktop does not run in Uniface Anywhere sessions. If an application fails to start or work properly in a Uniface Anywhere session, it may have a dependency on the desktop.

To register the Windows desktop (explorer.exe) to run in Uniface Anywhere sessions

1. From the Registry Editor, expand the HKEY_LOCAL_MACHINE key.
2. Expand \SOFTWARE\Uniface\Uniface Anywhere\System\Run\LocalMachine.
3. Create a DWORD value and name it explorer.exe.
4. Set the value to 0.

With this configuration, the desktop will run in Uniface Anywhere sessions but will not be visible.

Notes:

Registering the Windows desktop to run in the background of a Uniface Anywhere session adds significant overhead. Sessions will take longer to start and will consume more memory. Additional overhead can also result from other processes that are registered to run when the desktop starts up. Care should be taken to ensure that unnecessary processes are not registered in users' Startup folders or under the various Run commands in the Registry (e.g., HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run).

Explorer.exe will run in the session the first time that a user signs on to a host. This is done to fully initialize the user profile. Explorer.exe will not run in subsequent sessions started by the same user on the same host, unless configured to do so as described above.

Proxy Tunneling

Proxy tunneling via the **HTTP CONNECT** method allows a user who accesses the internet via a proxy server to connect to Uniface Anywhere Hosts on the internet when the following conditions are met:

- The user runs the Uniface Anywhere Client on a Windows computer;
- The address and port of the proxy server are stored under the client computer's Internet Options; and
- The proxy server is configured to allow HTTP CONNECT method tunnels to the port on which the Uniface Anywhere Host is configured to accept RapidX Protocol (RXP) connections.

Proxy Tunneling via the HTTP CONNECT Method

When users on Windows computers are unable to establish a direct connection to a Uniface Anywhere Host, and when the client computer is configured through its Internet Options to use a proxy server, Uniface Anywhere attempts to establish an HTTP CONNECT method tunnel to the Uniface Anywhere Host.

Specifically, the client:

1. Connects to the proxy server using the address and port specified in the client computer's **Internet Options**.
2. Sends a CONNECT request to the proxy server: i.e., `CONNECT address:port HTTP/1.0`, where *address* and *port* are respectively the IP address of the Uniface Anywhere Host and the port on which the server accepts RXP connections (e.g., 491 by default).
3. Reads the reply from the proxy server.
4. Responds to the proxy server's reply as follows:
 - a. If Basic authentication is required, Uniface Anywhere prompts users for their user name and password and then repeats Step 2, this time providing the user's credentials.
 - b. If the request failed, Uniface Anywhere displays the following message:
"Failed to connect to serverAddress via the proxy server at proxyAddress : [reason for failure]."

- c. If the request succeeded, Uniface Anywhere initializes the RXP connection and starts the session.

To allow HTTP CONNECT method tunnels using port 443

1. Configure the Uniface Anywhere Host to accept connections on port 443.
2. Specify port 443 in the Uniface Anywhere hyperlink.
3. If necessary, configure the proxy server to allow connections to the Uniface Anywhere Host on ports 80 (HTTP) and 443 (HTTPS).

Once you have configured the Uniface Anywhere Host and the Uniface Anywhere hyperlinks, users that meet the three requirements above will be able to connect to the host. Users running Uniface Anywhere from a shortcut will need to append the `-hp` argument followed by 443 to the shortcut. For example, `"...\ua-client.exe" -h server -hp 443`. Otherwise these users will be unable to sign in to Uniface Anywhere.

Notes:

Uniface Anywhere clients are unable to connect to Uniface Anywhere Hosts via proxy servers that are configured to verify that the traffic on port 443 is HTTPS.

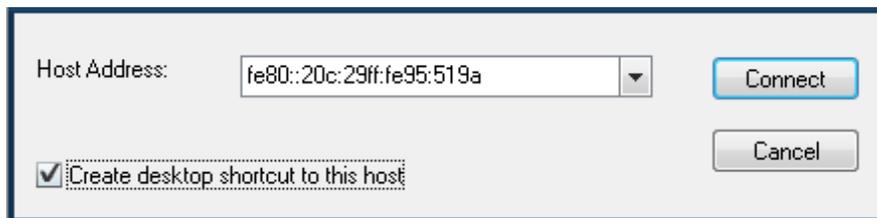
In a proxy server configuration, Uniface Anywhere only supports Basic authentication.

Support for Internet Protocol Version 6

Uniface Anywhere supports Internet Protocol version 6 (IPv6), the successor to IPv4, the dominant Internet layer protocol. IPv6 has a much larger address space than IPv4, and allows flexibility in allocating addresses and routing traffic.

Uniface Anywhere supports the following:

- Uniface Anywhere Hosts accepts connections from IPv4 and IPv6 clients.
- Uniface Anywhere relay servers accept connections from IPv4 and IPv6 dependent hosts.
- Administrators can specify a relay server in the Admin Console using a hostname, an IPv4 address, or an IPv6 address.
- Users can connect to a Uniface Anywhere Host using its hostname, its IPv4 address, or its IPv6 address.



Host Address:

Create desktop shortcut to this host

Smart Card Support

Uniface Anywhere provides support for smart card document signing on Windows only. Smart card document signing is enabled by granting applications access to client-attached smart cards via the **Smart cards** option on the **Client Access** tab of the Admin Console's **Host Options** dialog. SafeSign, SafeNet, or Aladdin must be installed on the client.

To enable smart card document signing

1. Start the Admin Console.
2. Click Tools | Host Options | Client Access.
3. Click **Smart cards**.
4. Click **OK**.

Performance Auto-Tuning

Performance auto-tuning is used in situations when an application is generating a large amount of graphical data or when a client system has limited processing speed. When Performance auto-tuning is enabled, the client machine reports the rate at which it is processing the data the host is sending. The host uses this information to reduce the total amount of data it sends by eliminating any graphical information that the client system is unable to keep up with, such as animations with a high frame rate, or by choosing to send an image of an application's contents rather than primitive graphical operations.

Performance auto-tuning allows any client to run even the most graphically intense applications. Performance auto-tuning is disabled by default.

To enable Performance Auto-Tuning for all clients connecting to a host

1. Locate the file **HostProperties.xml** in the following directory:
C:\ProgramData\Uniface\Uniface Anywhere.
2. Open **HostProperties.xml** in Wordpad.
3. Change the value of **ClientProcessingBatch** from 0 to 1.
4. Change the value or **ClientProcessingThrottleV2** from 0 to 1.
5. Open Regedit and create a DWORD registry value
HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface
Anywhere\AppServer\ClientOffscreenSurfaces and set its value to 0.
6. Stop and start the **Uniface Anywhere Application Publishing** Service.

Note: Make sure to create a backup of **HostProperties.xml** before making any changes.

How Performance Auto-Tuning Works

When performance auto-tuning is disabled, the host updates the client's display by sending primitive drawing commands such as "draw rectangle," "draw line," and "draw text" to the client.

The alternative is for the host to wait and send an image with the final result of the drawing operations to the client. This approach is referred to as "screen scraping." In most cases, it is much more efficient to update the client display using primitive drawing commands, but there are times when it is more efficient to "screen scrape."

When performance auto-tuning is enabled, the host attempts to determine the most efficient means of updating the client display each time display data is sent from the host to the client. For example, if the host estimates that the bandwidth required to send an image of the modified area of the screen will be less than the bandwidth required to send all of the drawing commands that were used to modify the screen, the host will send the image instead of the drawing commands. In other words, it will "screen scrape."

Enabling performance auto-tuning is recommended for applications that display animations or video because it allows the host to skip frames and remain responsive to user input even when the application on the host is drawing a large number of images. However, when this option is enabled, minor display anomalies can occur when parts of the screen are updated from the host's frame buffer (screen) and other parts are updated using drawing commands. Because of these anomalies, performance auto-tuning is disabled by default.

Silent Installation

Uniface Anywhere can be installed silently. In other words, installation is performed without user interaction except for the initial launch of the process. The version 6 Uniface Anywhere license must be copied to the Licensing directory before running the silent host upgrade.

To run a silent client install

1. Run cmd.exe as local administrator (Run as administrator).
2. Run the following command:
`UAnywhere.windows.exe /q`

This adds the Uniface Anywhere shortcut to the Start menu:
Start | Programs | Uniface Anywhere.

To install the Uniface Anywhere web clients, but not the shortcut to the native client, run the following command: `UAnywhere.exe /q CLIENT_SHORTCUT="No"`

The Uniface Anywhere Host can also be installed silently. These instructions are the same when upgrading the Uniface Anywhere Host.

To run a silent host install

1. Run cmd.exe as local administrator (Run as administrator).
2. Run the following command:
`ua-host.exe /q`
3. The host will reboot automatically.
4. Copy the license file into the **Licensing** directory.
5. Restart the **Uniface Anywhere License Manager** service.

To run a silent host install without automatically restarting the system, run the following command: `ua-host.exe /q /norestart`

Log Files

The Uniface Anywhere Host creates log files in which it records information about its own performance and that of certain Uniface Anywhere processes. Uniface Technical Support uses the data to diagnose and correct problems that may arise. This can be especially helpful for errors that are only reproducible on specific machines or with a specific application.

All log files, whether they pertain to the client or host machine, are located in the **Log** folder on the Uniface Anywhere Host. For example, D:\Program Files\Uniface\Uniface Anywhere\Log. In the Log folder are three subfolders: **Backup**, **Codes**, and **Templates**. Be careful not to delete these folders. Uniface Anywhere messages are recorded within log files prefixed with *aps* and followed by the date and time (to the nearest millisecond) the Application Publishing Service was started. (For example, *aps_2019-04-04_09-55-47-636.html*). A new log file is created each time the Application Publishing Service is started. The log file with the latest date and time stamp contains messages for the current, or most recent instance of the Application Publishing Service.

Problems detected in the execution of Uniface Anywhere are described by entries in the log file. Each entry is uniquely identified by an item number along with a date and time stamp, and a description of the event or program error. Uniface Technical Support uses this information to locate a problem's source and to determine its resolution.

Entries in the log file may also include prefixes for locating messages associated with an individual user's session and applications. If the event occurred within the context of a given session, the name of the session will appear at the beginning of the message, for example, *SuzyG on Server1*. If the event occurred within the context of a connection to the Application Publishing Service—a connection either from a client or from an application, the name of the connected process will be included in the message prefix, for example, *pw (1244)*. In this example, a problem occurred during the connection between the Program Window process and the Application Publishing Service. 1244 is the ID of the process in which the event took place. If the message prefix contains the connection name *aps*, the event occurred within the Application Publishing Service, but was not associated with a connection to another process.

Selecting a New Location for the Log Files

By default, log files are created and stored at \Program Files\Uniface\Uniface Anywhere\Log. You can select a new location for the log files through the Admin Console's **Host Options** dialog.

To select a new location for the Log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Type the path to the new directory in the **Folder** edit box or browse to its location.

You cannot specify a path to a remote system for the log file location. For example, if you type a UNC path or a mapped network drive in the **Folder** edit box, the following message is displayed:

Please specify a usable Windows folder where log files may be written.

Note: You should move the **Backup** folder and existing log files to the new location, along with the **Templates** and **Codes** subfolders.

Setting the Output Level

Uniface Anywhere offers six log output levels, as follows:

- 0: No output
- 1: Errors
- 2: Errors and Events
- 3: Errors, Events, and Warnings
- 4: Errors, Events, Warnings, and Diagnostic Messages
- 5, 6: Errors, Events, Warnings, Diagnostic Messages, and Trace Messages

To set the output level

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Type one of the above numeric values in the **Output level** box.
4. Click **OK**.

CAUTION! Setting the log output value to 5 or 6 will cause the host to generate very large log files and may adversely affect performance and scalability. These output levels should only be used in a controlled environment—preferably when no clients are accessing the Uniface Anywhere Host.

The default value for the Output level is 4.

Maintaining Log Files

Uniface Anywhere creates a new log file in the **Log** folder every time the Application Publishing Service starts. Over time these files can accumulate and consume a significant amount of disk space. To help manage these files, Uniface Anywhere lets you delete or backup log files and set file size or age limits.

To delete log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select **Delete**.
4. Specify how old (in days) log files can become before being deleted.
5. Specify at what size (in megabytes) log files are to be deleted.
6. Click **OK**.
7. Restart the **Application Publishing Service**.

To backup log files

1. From the Admin Console, click Tools | Host Options.
2. Click **Log**.
3. Under **Maintenance**, select Back up.
4. Specify how old (in days) log files can become before being moved to the Backup subdirectory of the Log folder.
5. Specify at what size (in megabytes) log files are to be moved to the Backup subdirectory of the Log folder.
6. Click **OK**.
7. Restart the Application Publishing Service.

Once every half hour, and each time it is started, the Application Publishing Service searches the **Log** folder for files that have reached the specified age or size limit. It then either deletes the files or moves them to the **Backup** subdirectory of the Log folder. If while sweeping the log files, the Application Publishing Service finds that the age or size limit has been met in the current log file, it closes the file and installs a newly created file in its place.

By default, log files are backed up after 7 days or when the file size has reached 20 MB.

Client Log Files

The Uniface Anywhere client records messages in a log file on the client device when the client is not connected to a host. In addition, after a user signs in to a host, the client synchronizes its log files with the host. Specifically, Uniface Anywhere determines if there are any log files on the client from previous sessions with the host that have not already been copied to the host. If there are, Uniface Anywhere copies the missing client log files to the host.

These changes make it easier for system administrators to determine the cause of connection problems. For example, if a user reports that his or her connection to the host is frequently getting dropped, the system administrator can check the host and client log files to determine the cause. In this scenario, the client log files from the user's previous sessions will generally be available on the host, and the administrator will not need to manually retrieve the client log files from the client device. Generally, administrators will only need to retrieve log files from a user's computer in cases where the user is unable to connect to a host at all.

The names of client log files include the *name of the user*, the *address of the host*, and the *date and time that the client was started*. Client log files are stored in the user's **%APPDATA%\Uniface\Logs** directory (on Windows clients) and in the **\Program Files\Uniface\Uniface Anywhere\Log\Clients** directory on the host.

When a log file is copied from the client to the host, the client's copy of the log file is moved to the **%APPDATA%\Uniface\Logs\Old** directory on the client computer.

Log files are stored on the client for the number of days specified in the **HKEY_CURRENT_USER\Software\Uniface\Uniface Anywhere\Client\LogFileAgeLimit** registry value. The default is 10 days.

Messages that the client outputs while it is connected to a host are recorded in the host's (APS_...) log file. The Uniface Anywhere client only records messages in the client log file when the client is not connected to a host.

Connection Monitoring

Uniface Anywhere monitors the latency and the input and output rates of connections to the host. When a new client connects to a host, the host tests the client's connection and records initial values for each of the metrics in the host's log file. Thereafter, the host monitors the connection for quality changes. If the quality of any of the metrics changes while the session is running, the host records the change in its log file.

The frequency of quality checks and the quality threshold values are specified in the **HostProperties.xml** file.

Support Request Wizard

The Uniface Anywhere Host includes a Support Request Wizard that gathers log files and information about the host that can be sent to technical support. Administrators can run the Support Request Wizard from the Admin Console by clicking Help | Support Request Wizard or via the Start menu by clicking Programs | Uniface Uniface Anywhere | Support Request Wizard.

The wizard prompts the administrator for a description of the problem, a time frame for when the problem happened, and the user or users that were affected. If the issue is associated with an existing support case, administrators can enter the Case Number. By default, the zipped report is placed on the user profile's desktop, but administrators can select an alternative destination via the wizard.

Administrators can also reply to an existing support email (customer.support@uniface.com) with the zipped file attached.

High Resolution Client Devices

When the Uniface Anywhere App is run on a high resolution client device that is configured to scale the display, the Uniface Anywhere App attempts to scale the Uniface Anywhere session's graphical output so the text and controls of applications running in the session are the same size as the text and controls of applications that are running locally on the client device. For example, if the client computer is configured to scale the display by 200%, the Uniface Anywhere App scales the graphics commands it receives from the host (e.g., text characters and images) by 200%.

When the client stretches graphic objects such as images and text, their quality is not as good as when the objects are drawn at 100%. The edges of text characters, for example, are not as smooth when they are stretched; characters may appear blocky or blurry. On high resolution screens (where display scaling is most often enabled) these effects are typically not very noticeable. On low resolution screens, however, the effects can be quite noticeable, especially when the display scale factor is set to a non-integral value such as 125%. If these effects are noticeable, Uniface Anywhere's scaling feature can be disabled as follows:

- When the client is run from a shortcut, add **-clientdpi 0** to the client's command-line
- When the client is run from a browser, add **&clientdpi=false** to the URL

- To disable the feature on the host for all users, change the value of the **ClientDPIScalingEnabled** property in the **HostProperties.xml** file on the host from “true” to “false”

When Uniface Anywhere's scaling feature is disabled, Uniface Anywhere will render the session using the scale factor specified for the user under the Control Panel's Display applet on the host. In this configuration, administrators can allow users to modify the DPI setting by publishing the Display applet to users.

To publish the Display applet to users

1. Sign in to the console on the host as an administrator.
2. Create a shortcut to the Display applet:
 - a. Click Start | Control Panel.
 - b. Right-click **Display**. A shortcut will be added to the Desktop.
 - c. Drag the shortcut to a directory that all users can access (e.g., C:\Users\Public\Desktop).
3. Publish the shortcut to users:
 - a. Run the Admin Console and click Applications | Add.
 - b. Type “Display Settings”(or some other descriptive name) in the **Display Name** field.
 - c. Enter the path to explorer.exe (e.g., C:\Windows\explorer.exe) in the **Executable Path** field.
 - d. In the **Command-Line Options** field, type the path to the shortcut created in step 2 (e.g., C:\Users\Public\Desktop\Display.lnk).
 - e. Click **OK**.

APPENDIX

Licensing

Uniface Anywhere licenses are based on the number of concurrent users required, and are perpetual. Uniface Anywhere license files are node-locked, meaning they are specifically identified with a host's MAC address (Host ID) and are usable only when installed on that host. Any Uniface Anywhere Host can be configured as a license server and/or an application server. A Uniface Anywhere Host which also includes a license is referred to as a *license server*.

Typical small end-user sites will operate with a basic configuration where there is one Uniface Anywhere Host which operates as both the *application server* and the *license server*. A typical larger site might operate with an advanced configuration where the license is installed on a *central license server* on the network, with several Uniface Anywhere application servers configured to check out licenses from that designated *central license server* on the network. Additionally, Uniface Anywhere licensing supports several different license server configurations for redundancy and high availability; these are explained in chapter II of this guide.

With each license purchase, Uniface creates a unique license database record referred to as a **License Master**. Each License Master is assigned a unique **Product Code** which is used for most security related transactions, and a unique **License Master ID** which is a simple sequential number. The License Master ID is used for license management as an easy reference for the license. The Product Code is longer and alphanumeric and is required for more secure functions such as activating a new license, renewing maintenance orders, and License Change Requests (LCRs). Both the License Master ID and the Product Code are identified in the license file, and both are *permanent* identifiers for a license.

Over time, updated license files will need to be issued to support a new version of Uniface Anywhere or if the license needs to be moved to a new server with a new MAC address (Host ID). With each change event, Uniface will provide an updated license file and VOID the old license file. The License Master ID and the Product Code will not change; they are permanent. Each new or updated license file issued will have a unique and random License ID for the license; the License ID is also identified within the license file.

Obtaining a License File

When an order for a new license is placed, Uniface processes the order and creates a new License Master. License information is emailed to the contacts identified on the order request. The License ID is used to format the name of the license file. (For example: **8d73e4k.lic** where 8d73e4k is the License ID). The user installs the attached license on the designated license server.

License Change Request

If an administrator moves the license file to a new license server, a License Change Request (LCR) must be made via the Customer Portal. Similarly, when a new version of Uniface Anywhere is released, a License Change Request is also required. License Change requests are typically processed within 1-2 days, but may take up to 5 business days to process. Updated licenses are sent as email attachments, with a new License ID. (License Master ID and Product Code do not change.) The old license file must be removed, as it has been voided/revoked by Uniface. The updated license must be installed, as per instructions provided in the license file.

Multiple Licenses

It is common for customers to order additional licenses over time. With each license order, Uniface creates a unique new License Master for each add-on license. The administrator does not need to modify or change the already installed license(s).

To install an add-on license

1. After receiving the add-on license Product Code; activate the license via the Customer Portal.
2. Install the license on the license server, as per the instructions within the license file.
3. Restart the **Uniface Anywhere License Manager Service**. Otherwise, the add-on license will not be recognized. Restarting the service does not interrupt actively logged in end users.

When multiple licenses are installed, the naming to the left of the decimal point must be unique. Uniface delivers the license files using the License ID, which is always unique. The administrator does not need to make any adjustments, and the license as received can simply be installed. However, if the administrator prefers to rename the license files for system management reasons, this is allowed, as long as the license file name is unique and the file extension is .lic. (For example, License1.lic, License2.lic, License3.lic.) If the extension is not '.lic', the Uniface Anywhere License Manager Service will not recognize the license. Uniface recommends installing the license as delivered with the 'LicenseID.lic' naming convention. If you have any questions regarding this procedure, please find contact at <https://www.uniface.info/display/SUP/Support+Processes+and+Contact> .

RapidX Protocol (RXP)

RXP is a proprietary protocol used for all Uniface Anywhere client-host data communications. By default, RXP runs over TCP port 491 but can be made to run over any compatible data port. RXP operates as part of the standard TCP/IP protocol stack. It is designed and optimized to handle low-bandwidth connectivity. The RXP display protocol is almost entirely asynchronous, which means the host and the client are rarely waiting for a response from its peer.

RXP is currently designed to handle encryption levels from 56-bit DES to 256-bit AES. When the TCP transport is selected, Uniface Anywhere uses Uniface's implementation of the Data Encryption Standard (DES). When the SSL transport is selected, Uniface Anywhere uses OpenSSL's implementation of Transport Layer Security (TLS) and OpenSSL's implementation of the selected cipher, for example, Advanced Encryption Standard (AES).

When a client opens a connection to the Application Publishing Service (APS), the APS first attempts to negotiate an RXP connection with the client. If the data that the APS receives from the client does not match the data that RXP clients send, the APS then attempts to negotiate a WebSocket (ws://) or WebSocket Secure (wss://) connection with the client.

During protocol negotiation, the APS closes the connection when any of the following occur:

- when the time required to negotiate the protocol exceeds the value of the **ProtocolNegotiationTimeout** property in the HostProperties.xml file
- when an error occurs while attempting to negotiate an RXP connection after the APS has determined that the client is trying to negotiate an RXP connection with the host
- when the client attempts to negotiate a WebSocket (ws://) connection with the host, and the host is configured to accept TLS connections (the SSL Transport is selected)
- when the client attempts to negotiate a Web Socket Secure (wss://) connection with the host, and the host is not configured to accept TLS connections (the TCP Transport is selected)

Creating Your Own Certificate Authority

Sites with many Uniface Anywhere Hosts can create their own certificate authority, then sign each server's certificate from this authority and install the certificate authority certificates onto each client. This will prevent any warnings about untrusted authorities, without requiring the site to obtain a third-party certificate for each server.

There are many third-party applications and systems to assist in the creation and maintenance of a certificate authority that interoperate with the OpenSSL toolkit. These tools should be able to generate signed server certificates for use with Uniface Anywhere without modification.

A certificate authority is a virtual organization that will sign each of your server keys, allowing the client to assert that the server keys are authentic and have not been tampered with.

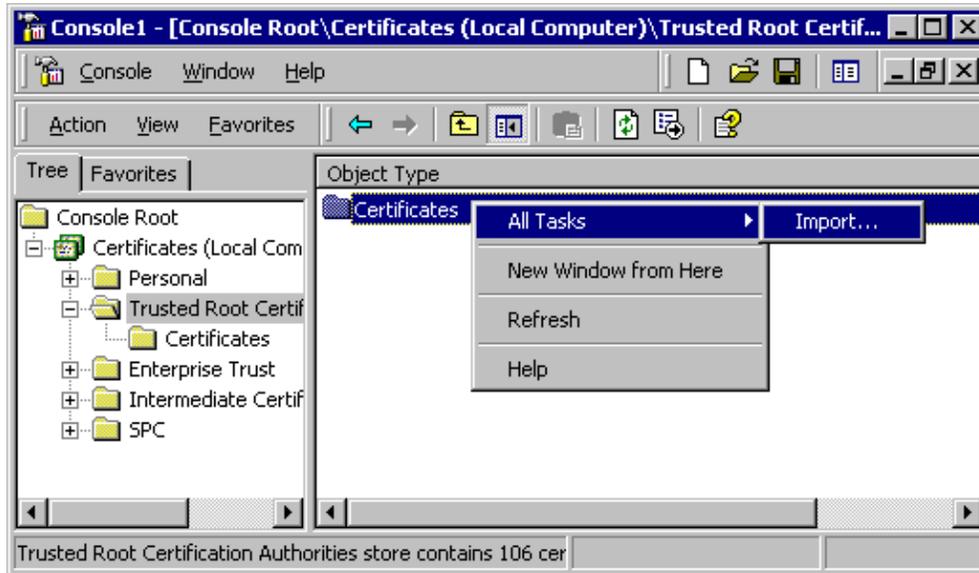
To establish the certificate authority, a CA key and self-signed certificate must be created. Once the CA certificate and key are created, import the CA certificate on the client device via the Internet Options dialog. Finally, the server keys are signed using the CA certificate, which will allow the client machines to recognize the authenticity of the signatures and allow connections to the server without warning the user about the trustworthiness of the CA.

Note: Nine files are created during this process: ca.key, ca.csr, ca.crt, ca.cfg, ca.serial, server.cfg, server.key, server.crt, and server.csr.

Importing the Trusted Server Certificate on a Dependent Host

To import the trusted server certificate on a dependent host, add a Policy in Microsoft Management Console. This is only required when using a self-generated certificate.

1. On the dependent host, click Start | Run. Type **mmc** in the **Open** box. This will open Microsoft Management Console.
2. Click Console | Add/Remove Snap-in. Click **Add**.
3. Click **Certificates** from the list of Available Standalone Snap-ins and click **Add**.
4. Select Computer account in the **Certificate Snap-in** dialog. Click **Next**.
5. In the **Select Computer** dialog, select Local computer. Click **Finish**.
6. Close the Add Standalone Snap-in dialog.
7. Return to the Add/Remove Snap-in dialog and click **Certificates (Local Computer)**.
8. Click **Ok**.
9. Under Console Root, expand **Certificates**. Click **Trusted Root Certification Authorities**. From the right pane, right-click **Certificates**.
10. Select All Tasks | Import. Browse for the Certificate **ca.cert**.



The server key and certificate files (e.g., server.key and server.crt) must have the same base filename and be located in the same directory on the Uniface Anywhere Host. Dependent hosts do not need SSL certificates, but their designated relay server must have a valid SSL certificate that is signed by a CA and that is recognized by the dependent hosts. You can verify that these conditions are met as follows:

1. Run the native Windows Client on the dependent host:
2. Right-click **My Computer**.
3. Click **Explore**.
4. Browse to the \Uniface Anywhere\Programs directory.
5. Double-click **ua-client.exe**.
6. Enter the name of the relay server as it is specified in the Admin Console.
7. If the relay server has a valid SSL certificate that is signed by a CA and is recognized by the dependent host, no **Security Alert** dialog will be displayed. If a **Security Alert** dialog is displayed, the dependent host will not be able to connect to the relay server.

Creating a CA Key and Certificate

The first step to establishing a certificate authority (CA) is to generate an RSA private key. This key should be kept very secret, as any entity with access to this key can generate false certificates that would certify unknown hosts as trusted. It is vitally important to protect the integrity of your certificate authority. To generate the CA key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa -out ca.key 2048
```

This command will generate your initial CA key, and place it in the file ca.key. After the key is created, generate a Certificate Signing Request (CSR) that will be used to create the CA certificate.

To generate the CSR, use the following command:

```
[OPENSSL_DIR]\bin\openssl req -sha256 -new -key ca.key -out ca.csr
```

This command will run interactively and prompt you for the information to be contained in the certificate. Example responses are shown below:

Country Name (2 letter code) [AU]:*US*

State or Province Name (full name) [Some-State]:*Washington*

Locality Name (e.g., city) []:*Bellevue*

Organization Name (e.g., company) [Internet Widgits Pty Ltd]:*Uniface B.V.*

Organizational Unit Name (e.g., section) []:*Uniface B.V. CA*

Common Name (e.g., YOUR name) []:*Uniface B.V. CA*

Email Address []:*hostmaster@www.uniface.com*

Please enter the following *extra* attributes to be sent with your certificate request:

A challenge password []:*[enter]*

An optional company name []:*[enter]*

The prompts should be answered as:

Country Name: your two-letter country abbreviation

State or Province Name: your full state or province name

Locality Name: your city or town or suburb name

Organization Name: the name of your organization or company

Organizational Unit Name: the organizational name should be a representation of your CA's name

Common Name: This should either be a person responsible for the operation of the CA or a generic name representing the CA itself

Email Address: This should be an e-mail address that can be used to address concerns about certificates to someone responsible for the CA

The final step is establishing the CA certificate. To do this, create a settings file that contains some information about the CA. The file should be named **ca.cfg** and should contain the following:

```
extensions = x509v3
[ x509v3 ]
subjectAltName = email:copy
basicConstraints = CA:true,pathlen:0
nsComment = "[your company] site CA"
nsCertType = sslCA
```

After creating this file, you can sign your CA certificate with the following commands:

```
OPENSSL_DIR]\bin\openssl x509 -req -sha256 -extfile ca.cfg -days 1825 -  
signkey ca.key -in ca.csr -out ca.crt
```

The resulting certificate file, **ca.crt**, is the certificate that will need to be imported into the certificate store on each client device. It is also necessary to create a configuration file for signing server keys. This file should be named **server.cfg**, and should contain the following:

```
extensions = x509v3  
[ x509v3 ]  
subjectAltName = email:copy  
nsComment = "Certificate signed by your company CA"  
nsCertType = server
```

You must also create a file that will store the serial numbers of certificates signed by this CA. Use the following command:

```
echo 01 > ca.serial
```

Creating and Signing Server Keys

To create a new server key, use the following command:

```
[OPENSSL_DIR]\bin\openssl genrsa -out server.key 2048
```

This will generate a new server key and place it in the file **server.key**. Next, generate a Certificate Signing Request (CSR) for the server key. This is essentially the same process used for generating the CSR for the CA key, but the inputs are slightly different. Use the following command:

```
[OPENSSL_DIR]\bin\openssl req -sha256 -new -key server.key -out server.csr
```

This command will run interactively and prompt you for information about the server certificate that will be generated. Example input is shown below:

Country Name (2 letter code) [AU]:*US*

State or Province Name (full name) [Some-State]:*Washington*

Locality Name (eg, city) []:*Bellevue*

Organization Name (eg, company) [Internet Widgits Pty Ltd]:*Company Name*

Organizational Unit Name (eg, section) []: *Engineering*

Common Name []:*server*

Email Address []:*user@company.com*

Please enter the following 'extra' attributes to be sent with your certificate request:

A challenge password []: *[enter]*

An optional company name []: *[enter]*

Your answers to these prompts should be:

Country Name: Your 2-letter country abbreviation

State or Province Name: Your full state or province name

Locality Name: The city, town, or suburb where your organization is located

Organization Name: The name of your company or organization

Organizational Unit Name: Either a department name or some name representing this server

Common Name: The name of this server, as it should appear on the certificate. Note that this is not the name of a person.

Email address: The e-mail address of a party responsible for this server

The Common Name *must* match the host name of the Uniface Anywhere Host. Any variation in the name will cause the client to issue a warning when connecting.

Finally, sign the server's key with the CA's certificate.

Use the following command:

```
[OPENSSL_DIR]\bin\openssl x509 -req -sha256 -extfile server.cfg -days 1825 -CA ca.crt -CAkey ca.key -CAserial ca.serial -in server.csr -out server.crt
```

Note that the `-days 1825` parameter will cause our server certificates to expire in 1825 days, or roughly 5 years. If you want certificates to expire earlier or later, adjust this number to fit your requirements.

Copy the **ca.crt**, **server.key** and **server.crt** files to a directory on the target server that can be accessed from the System account but cannot be accessed from the accounts of users who will sign in to the host. Finally, select the server certificate in the Admin Console.

To select the server certificate

1. From the Admin Console, click Tools | Host Options.
2. Click the **Security** tab.
3. In the **Transport** list, select SSL.
4. Type or browse to the path to the server's certificate (e.g., `server.crt`) file in the **SSL Certificate** box.
5. Click **OK**.

Your Uniface Anywhere Host now has a new SSL certificate, signed by your own custom certificate authority.

Generating a CSR Using IIS Certificate Wizard

The following example uses Microsoft's **IIS Certificate Wizard** to generate a Certificate Signing Request (CSR), and then uses OpenSSL to generate the certificate. In this example, the administrator is the CA.

In order for this certificate to work in Uniface Anywhere a private key is required. When you generate a CSR with the IIS Certificate Wizard, a private key is created but it is not presented to the user by default. As a result, the private key needs to be backed up separately using the MMC (Microsoft Management Console).

For instructions, see:

<https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=AR214>, and look under the Microsoft IIS 6.0 heading.

The private key in this case is a .pfx file, not a .key file, and it must be converted to PEM format in order to work with Uniface Anywhere. Use the following command to convert the pfx file to the PEM format:

```
openssl pkcs12 -nocerts -in server.pfx -out server.pem -nodes
```

Change the extension of the file from .pem to .key. The resulting file is called **server.key** and is required for SSL to work in Uniface Anywhere. It must have the same file prefix as the certificate generated by the CA (i.e., server.crt).

Uniface Anywhere requires that the certificate be in PEM format. When requesting a Certificate from a third-party CA, we recommend requesting a certificate in PEM format. If this is not possible and the certificate can only be delivered in DER format, it can be converted to PEM using the following command:

```
openssl x509 -inform der -in MYCERT.cer -out MYCERT.pem
```

The resulting **MYCERT.pem** file can then be renamed to **MYCERT.crt** for use in Uniface Anywhere.

Disabling Automatic Client Keyboard

Automatic client keyboard lets administrators configure Uniface Anywhere Hosts to automatically work with any client keyboard. This feature is enabled by default, but can be disabled by editing the HostProperties.xml file.

To disable automatic client keyboard

1. Locate the file **HostProperties.xml** (e.g., C:\ProgramData\Uniface\GO-Global)
2. Open **HostProperties.xml** in WordPad and locate the **ClientSideIMEEnabled** property.
3. Set the **ClientSideIMEEnabled** property to false.
4. Save the file.

When automatic client keyboard is disabled in the HostProperties.xml, it can still be enabled per user as follows:

Add **-kb ClientSideIME** to the client shortcut.

For example, on the Windows Client:

```
"C:\Program Files\Uniface\Uniface Anywhere\Client\ua-client.exe" -kb ClientSideIME
```

Or, when Uniface Anywhere is run from a Web browser, add the following argument to hyperlinks that reference the logon.html page: **&keyboard=ClientSideIME**

For example, <http://hostname/UAnywhere/logon.html?direct=true&keyboard=ClientSideIME>

Configuring Support for Client Keyboards and/or IMEs

Windows uses input languages, keyboard layouts, Input Method Editors (IME), and code pages to map keys on a keyboard to the characters on the display. When a key is pressed on the client's keyboard, Uniface Anywhere sends a key code to the host, which translates the key code into a Windows input message using the session's active keyboard layout. The Uniface Anywhere setup configures the host to support clients that use the same operating system, keyboard, and/or IME as the host. Uniface Anywhere supports clients with different operating systems and keyboards with keyboard mapping files.

The following section describes mechanisms and procedures to manage keyboards and IMEs in sessions on client computers that do not match the host system.

Installing Additional Keyboards and IMEs

Before clients can use keyboards and/or IMEs that are different from the host's, the files used to support them must be installed on the Uniface Anywhere Host. In most cases the layouts are copied during the installation of the operating system, but East Asian and right-to-left input languages are not.

To add keyboard layouts on a host running Windows Server 2016

1. From the Start menu, click **Control Panel**.
2. Click **Language**.
3. Select the desired language (and Regional variant, if applicable) and click **Add**.

Additional files will be copied to your machine. You may need to provide the OS install CD or the network share name. Support for the new languages will become available after restarting.

To add keyboard layouts on a host running Windows Server 2008

1. From the Start menu, click **Control Panel**.
2. Double-click the Regional and Language Options icon.
3. Click the Keyboard and Languages tab. Then click the Change keyboards... button.
4. In the **Text Services and Input Languages** window, click the **Add...** button to add the desired language(s). Select the language(s) by clicking the check boxes in the **Add Input Language** window.
5. Click **OK**.

6. Click the **Apply** button in the Text Services and Input Languages window.
7. Click **OK**.

The following is a list of keyboards that each Uniface Anywhere client supports.

Linux supports:

Linux Keyboard Layout Name(s)	Linux Keyboard Layout	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S. English	us	English (United States)	US	00000409	us.kbm
Japanese	jp	Japanese	Japanese (106/109 Key)	E0010411 (IME)	jp.kbm
French	fr	French (France)	French	0000040C	fr.kbm
Belgian (be-latin1)	be	French (Belgian)	Belgian French	0000080C	be.kbm
German, German (Latin1), German (Latin1 w/ no dead keys)	de	German (Germany)	German	00000407	de.kbm
Polish	pl	Polish	Polish (214)	00010415	pl.kbm
Brazilian (ABNT2)	br	Portuguese (Brazil)	Portuguese (Brazilian ABNT2)	00010416	br.kbm
*See the Client Keyboard Mapping Files section below for more information.					

Mac OS X supports:

Mac OS X Keyboard Layout Name	Windows Input Language	Windows Keyboard Layout Name	Windows Keyboard Layout	Keyboard Mapping File*
U.S.	English (United States)	U.S. International	00020409	us.kbm
French	French (France)	U.S. International	00020409	fr.kbm
German	German (Germany)	U.S. International	00020409	de.kbm
*See the Client Keyboard Mapping Files section below for more information.				

Note: Due to physical differences between the Mac OS X and Windows keyboards, the Mac OS X keyboard mapping files use the **U.S. International** Windows keyboard layout to translate a majority of the keys to Windows applications.

Windows clients support any keyboard that the Uniface Anywhere Host has drivers for.

Client Keyboard Mapping Files

Uniface Anywhere uses keyboard mapping files on Linux and Mac OS X to ensure that the proper keyboard layout is loaded on the host and that the correct key codes are sent for each key press and release. Keyboard mapping files allow support for new keyboards to be added by simply copying a new keyboard mapping file to the client. Keyboard mapping files are installed into the **/etc/ua-client/kbd** directory on Linux and the **/etc/Uniface Anywhere/kbd** directory on Mac. An internal version of the **us.kbm** keyboard mapping file will be used if a keyboard mapping file is not found.

These clients can automatically load keyboard mapping files based on information obtained from the operating system.

The Keyboard Mapping File Installation Locations (i.e., default root paths)

Client OS	Native Install	Browser Plug-in Install	Default Layout	Layout Obtained by...
Linux	/etc/ ua-client/kbd	~/.mozilla/ ua-client/kbd	U.S. English	Environment variable or automatically from the OS
Mac OS X	/etc/ Uniface Anywhere/kbd	/etc/ Uniface Anywhere/kbd	U.S.	Environment variable or automatically from the OS

Keyboard/IME Identifiers Used by Uniface Anywhere

Uniface Anywhere uses two identifiers, collectively known as **Uniface Anywhere Input Identifiers** (GGII), to specify a keyboard/IME for a session. The first is a keyboard layout. These are 8-digit string identifiers that Windows operating systems use to load keyboard drivers and IME programs. They are similar to locale IDs in that the last four digits typically match the 4-digit locale ID of the language supported by the keyboard. Keyboard layouts that specify an IME typically start with an "E". The list of available keyboard layouts can be viewed in the registry under the [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts] key.

The second identifier used by Uniface Anywhere is the layout text string, which is a registry value of each keyboard layout registry key. These strings are displayed in the dropdown box under Keyboard layout/IME when adding input languages.

In the following examples, the first has a keyboard layout GGII of 00000409 and a layout text GGII of US. The second example has a keyboard layout GGII of E0010411 and a layout text GGII of Japanese Input System (MS-IME2002).

EXAMPLES:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\00000409
Layout File = KBDUS.DLL
Layout Text = US
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layouts\E0010411
Ime File = imejp81.ime
Layout File = Kbdjpn.dll
Layout Text = Japanese Input System (MS-IME2002)
```

Environment Variable	Description
<p>UA-CLIENT_KBD_FILE</p>	<p>This environment variable is used to specify the fully qualified path name of the mapping file to use. If specified, this will override all other means of obtaining the filename path. For example: On Linux, UA-CLIENT_KBD_FILE=/home/someuser/KeyMappingFiles/MyCustomKeyMappingFile.kmf will cause that exact file to be loaded. If that file is not found the internal version of the us.kbm keyboard mapping file will be used.</p>
<p>UA-CLIENT_KBD_FILE_ROOT</p>	<p>This environment variable is used to specify the root path name to the keyboard mapping files. The kbd directory that contains the keyboard mapping files will be expected to be in this directory. For example: On Linux, UA-CLIENT_KBD_FILE_ROOT=/home/someuser, will cause the file /home/someuser/kbd/xxx.kbm to be loaded, where 'xxx' indicates the LAYOUT obtained from the following UA-CLIENT_KBD_FILE_LAYOUT environment variable or automatically from the OS.</p>
<p>UA-CLIENT_KBD_LAYOUT</p>	<p>This environment variable is used to specify which LAYOUT (or file name prefix) to use. This LAYOUT name along with the appended .kbm extension will be used as the file name. For example: UA-CLIENT_KBD_LAYOUT=MyCustomKeyMappingFile will load the file /ect/ua-client/kbd/MyCustomKeyMappingFile.kbm. If the above example for UA-CLIENT_KBD_FILE_ROOT is also used, the file /home/someuser/kbd/MyCustomKeyMappingFile.kbm will be loaded. A subdirectory of the root path name to the mapping files can also be included here. For example: UA-CLIENT_KBD_LAYOUT=thinclient/us will load /etc/ua-client/kbd/thinclient/us.kbm provided a different root path is not specified. This will override the LAYOUT obtained automatically from the OS.</p>

Configuring Client Keyboard Options

You can specify the keyboard/IME for a session using the **-kb** shortcut parameter or the "keyboard" hyperlink parameter. These take both types of GGIs described above. On Windows computers, if the **-kb** shortcut parameter is not specified, Uniface Anywhere will use the layout text of the currently active keyboard layout. On Linux computers, Uniface Anywhere does not send a layout text to the server if one is not specified on the command-line.

EXAMPLE:

Windows shortcut using a keyboard layout:

```
ua-client.exe -h server1 -kb 00000409
```

Specifying Layout Text Substitutions

Layout text substitutions can be specified on the server to map between client and server keyboard layout names. They can be used to:

1. Overcome differences in layout text names on different versions of Windows. For example, the **Japanese Input System (MS-IME2000)** layout text from a Windows 2000 Uniface Anywhere client system can be substituted with the **Japanese Input System (MS-IME2002)** layout text from a Uniface Anywhere Host.
2. Substitute an ANSI name for a keyboard layout that has a UNICODE name. For example, when specifying a keyboard layout with a UNICODE name through the “keyboard” applet parameter in an ASCII HTML page, it is necessary to substitute an ASCII name for the UNICODE name.

Keyboard Layout Substitutions are specified under the [HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere\System\Keyboard\Layout\Substitutes] registry key. Each REG_SZ value within this key has the name of a GGII, and the value is the name of a layout text from the server that should be used in place of the client name.

Setting the Fallback Layout Text

If there is no GGII specified from the client, or the one specified fails to load a valid keyboard layout, the Uniface Anywhere Host uses a fallback mechanism to determine which keyboard layout should be used for the session. The fallback layout text should be the layout text for the keyboard layout that will be used by all clients connecting to the server, exclusive of those passing a valid GGII. The fallback layout text is automatically set during installation if the keyboard layout that is active is an IME. It may be modified after installation by editing the **Fallback Layout Text** value under the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Uniface\Uniface Anywhere\System\Keyboard Layout

Note: When connecting to a Chinese Uniface Anywhere Host, the **Sign In** dialog appears from the shortcut along with the IME bar specifying Chinese as the default language. Clicking CTRL+spacebar does not toggle the languages. Users must manually click the IME bar with the mouse pointer to select English. Without manually clicking the IME bar, users will be unable to type a user name and password.

Configuring Multiple Input Locales

The **Default User** account profile can be configured with different and/or multiple input locales. Account profiles for new users logging on to a Uniface Anywhere Host are automatically configured with the **Default User** account's input locales. Users can switch to any input locale that is defined in their account profile.

Note: Users with roaming profiles or profiles that already exist on the Uniface Anywhere Host will not receive these new settings. These accounts must be configured manually.

As an example, the following instructions describe how to install and use the German input locale on an English Windows Server 2016.

1. Enable German on Windows Server 2016.

- 1.1 Sign in to the Uniface Anywhere Host interactively with a user account that you wish to set the Input Local for.
- 1.2 Click Start | Control Panel | Language.
- 1.3 Click Add a language.
- 1.4 Select Deutsch (German) and click **Open**.
- 1.5 Select Deutsch (Deutschland) as the Regional variant and click **Add**.

2. Verify that the input locale is correctly installed and configured.

- 2.1 Launch **Notepad** in this interactive session.
- 2.2 Type a few characters in English.
- 2.3 Type Left Alt + Shift.
- 2.4 Type a few characters (for example, [; and ') and verify that they display in German.

The German input locale is now enabled for the **Default User** profile and the user that was logged on to the system in step 1.1.

3. Switch between input locales during a Uniface Anywhere session.

- 3.1 Start a Uniface Anywhere client and connect to the server with the account used in step 1.1.
- 3.2 Launch **Notepad**.
- 3.3 Type a few characters in English.
- 3.4 Type Left ALT + Shift.
- 3.5 Type a few characters and verify that they display in German.

Notes:

Users will not be able to switch input locales when the **Sign In** dialog is displayed. The input locale for the default language of the Uniface Anywhere Host will be used.

On Windows clients, the selected input locale of server-based applications is not displayed in the system tray of the client computer.

Third-Party Components

Uniface Anywhere contains software provided by third parties, including open source software. These components are listed below.

Third-Party Component	License Agreement
Apache Tomcat	http://www.apache.org/licenses/LICENSE-2.0
Adobe Integrated Runtime	https://labs.adobe.com/technologies/eula/air.html
BlazeDS	http://www.gnu.org/licenses/lgpl.txt
Codejock Software Xtreme Skinframework	http://www.codejock.com/products/licensefaq.asp
Flex	https://labs.adobe.com/technologies/eula/flexbuilder_linux.html
Java Runtime Environment	https://www.oracle.com/technetwork/java/javase/jre-8-readme-2095710.html
libpng	http://www.libpng.org/pub/png/src/libpng-LICENSE.txt
OpenSSL	http://www.openssl.org/source/license.html
PostgreSQL	https://wiki.postgresql.org/wiki/FAQ#What_is_the_license_of_PostgreSQL.3F
Qt	http://www.gnu.org/licenses/lgpl.txt
VeryPDF	http://www.verypdf.com/custom/license_agreement.htm
win-acme	https://github.com/PKISharp/win-acme/blob/master/LICENSE
XML Parser Library	https://www.applied-mathematics.net/tools/xmlparser_doc/html/index.html
Zlib	http://www.zlib.net/zlib_license.html

Known Limitations

The following are known limitations of Uniface Anywhere:

- Uniface Anywhere does not support Group Policy logon or logoff scripts.
- Microsoft's VBScripts are not supported as logon scripts unless they are run in a batch file.
- Copying a file on a Uniface Anywhere Host and pasting it to the client, while attempting to overwrite an existing file, may not work.
- Uniface Anywhere does not support Parallels Virtuozzo.
- Uniface Anywhere supports Adobe Acrobat 8.0 in a Uniface Anywhere session. Previous versions of Acrobat are not supported.
- Apple's Preview application is not supported when printing from a Mac. Adobe Reader is required in order to print when running the Mac OS X App.
- Uniface Anywhere's Universal Printer Driver uses port 9010. This port cannot be changed. If any other software on a Uniface Anywhere Host uses port 9010, users will be unable to print with the Universal Printer Driver.
- The Uniface Anywhere License Manager Service must be restarted whenever license files are added or removed.
- Japanese keyboards are only supported on Mac OS X with the `-kb ClientSideIME` option.
- Painting problems may occur if a client's Task Manager is set to "Always On Top".
- Colors may display incorrectly when the client's display is set to 256 colors.
- Journal record hooks are not supported. As such, macros may fail to record in some applications.
- OLE objects embedded in a client-side file cannot be edited. If the application required to edit the OLE object is available on the host, copy the file to a drive on the host, edit it, and then, if desired, copy it back to the client.
- On non-Windows clients, only text and images can be copied and pasted between applications running on the client and applications running on the host.
- When a Uniface Anywhere Host is connected to a relay server, no warning is displayed that the host's settings (published applications, etc.) will be replaced by those of the relay server.
- Users are unable to reconnect to a disconnected session while the session is being shadowed.
- Uniface Anywhere does not support running the Application Publishing Service in any account other than the System account.
- The keyboard mapping command-line argument `-kb` is case sensitive on Linux and Mac OS X. `-KB` will not work.
- Uniface Anywhere does not support the `/3GB` switch.
- PDFCreator from pdfforge is not supported.
- Microsoft's XPS Document Writer is supported as a client printer when using the Universal Printer Driver, but the XPS Printer Driver is not.
- When administering Uniface Anywhere from a dependent application server, the Admin Console cannot be used to connect to the relay server if you are interactively logged on to the two systems with different accounts. Instead, run the Admin Console on the relay server.
- Uniface Anywhere does not support applications that integrate with the system tray.
- Sessions take longer to start when the Apply Group Policy is enabled in the Admin Console.
- The host's Theme is not applied when users authenticate with Integrated Windows Authentication and server-side password caching is disabled.

INDEX

A

- ac, 112, 116
- Active Directory, 46, 101, 111
- Active Directory Domain, 108
- Active Directory Domain Controller, 46
- Active Sessions, 108
- addLink, 80
- Adjusting the Printable Area, 124
- Admin Console, 25, 27, 31, 32, 53, 99, 102
 - accessing, 25
 - accessing from a client machine, 74
 - refreshing, 59
- All Hosts, 25, 60, 102, 113, 126
- AllowWindowsUpdates, 69
- Always in front, 61
- Apple Safari, 7
- Application Link, 28, 29
- Application Publishing Service, 22, 25, 39, 99, 100, 104, 145, 146, 147
- Application Script Support, 133
- Application Users/Groups, 32
- Applications, 58
 - adding, 26
 - duplicating, 30
 - editing properties, 30
 - installing, 26
 - publishing, 27
 - removing, 31
 - renaming, 30
- aps, 145
- ARGS, 83
- Audio support, 126
- Authentication, 46
- autoconfigprinters, 83
- Automatic client keyboard, 21
- Automatic client updates, 87
- Automatic Client Updates, 3
- autoreconnect, 83

B

- Backup, 147
- Backup folder, 146
- Backward Compatibility, 3
- Basic authentication, 139
- BLM, 16
- Broadcast Interval, 60

C

- CA, 158
- CA certificate, 153, 155
- CA key, 153, 154
- ca.cfg, 155
- ca.crt, 156, 157
- Cache password on the client, 48

- Cache passwords on the host, 52
- Case Number, 148
- Central license server, 14
- Certificate Authority, 38
- Certificate Signing Request, 43, 154, 156, 158
- Certificate Wizard, 158
- Change Icon, 27, 31
- Change Password, 51, 52
- Client clipboard, 126
- Client Connections, 108
- Client drive letters, 128
- Client drives, 127, 128, 129
- Client file access, 127, 137
- Client File Access, 1
- Client keyboards, 159
- Client printer name, 123
- Client Printer Naming, 123
- Client printers, 83
- Client printing, 112
- Client Printing, 3, 134
- Client Serial and Parallel Ports, 4, 127
- Client Sound, 4, 126, 138
- Client Time Zone, 134
- Client updates, 87
- CLIENTCOMPUTERIPADDRESS, 133
- CLIENTCOMPUTERNAME, 132
- clientdpi, 84, 148
- ClientDPIScalingEnabled, 84, 149
- clientscale, 84
- Client-side password caching, 48
- Clipboard support, 126
- Cloud environments, 20
- cm.exe, 74
- cn, 84
- Codes, 146
- Color depth, 7, 131
- Command-line options, 28, 30, 33
- Common Name, 43, 155, 157
- Compression, 83
- computerName, 84
- Connected Clients, 35, 58
- Connection dialog, 40, 99
- Consecutive letters, 128
- Copy and paste, 126
- CPU, 60
- CPU requirements, 7
- CPU utilization, 60
- Critical, 71
- Cross-platform Compatibility, 1
- Custom toolbars, 91

D

- Data Encryption Standard, 152
- DataDownloader.exe, 137
- DataProcessor.exe, 137
- DataViewer.exe, 137
- Default printer, 116, 117
- DefaultLoaderOptions, 137
- Defer Windows Updates, 69

- DelayWindowsUpdates, 69
- Delegation, 46, 110
- Delegation Support, 108
- Demilitarized zone, 101
- Dependent application server, 103
- Dependent host, 98, 102
- Dependent hosts, 103
- DES encryption, 41
- Device Guard, 6
- Diagnostic Messages, 146
- Disconnect, 53, 54, 66
- Disconnecting a session, 54
- Display applet, 149
- Display name, 27
- Display scaling, 148
- DMZ, 103
- DNS servers, 108
- Domain Controller Security Policy, 23
- Domain name, 22
- Domain Name System, 108
- Domain Security Policy, 23
- Drive letters, 128
- Drive mappings, 130
- DWORD, 136
- Dynamic Display Resize, 3

E

- Elastic IP address, 20
- Elastic Network Interface, 20
- Encryption, 41
- Errors, 146
- Events, 146
- Explorer.exe, 135

F

- Failover server, 105
- Failure recovery, 104
- Fallback Layout Text, 164
- File Permissions, 23
- Firewall, 6, 16, 39, 101, 103
- FLEXnet, 14, 16

G

- geometry, 87
- Get Link, 28
- GetComputerName, 133
- GGII, 162
- Global logon script, 64
- Global scripts, 62
- Go Daddy, 44
- Google Chrome, 7
- Grace period, 68
- Group Policy, 61, 167
- Group Policy Support, 3

H

- Hiding client drives, 129
- High resolution, 148
- High Resolution Displays, 4
- Host, 9

- Host activity, 58
- Host address, 29
- Host Monitoring, 1
- Host Options dialog, 53
- Host Port, 39
- Host Updates, Pending and Installed, 73
- hostid, 17
- HostProperties.xml, 124, 149
- HTML5, 4
- HTTP, 140
- HTTP CONNECT method, 139
- HTTPS, 140
- Hyper-V, 6

I

- Idle limit, 66
- Idle time, 66
- IIS, 86
- Image compression, 132
- IME, 159
- inbrowserprocess, 83
- Increment, 128
- Independent hosts, 98, 99
- Input Method Editor, 21
- Input Method Editors, 159
- installApp, 80, 84
- Installing the Uniface Anywhere Host, 9
- Integrated Windows authentication, 46, 53, 101, 102
- Integrated Windows Authentication, 52
- INTERACTIVE group, 45, 46
- Intermediary certificate, 44
- Internet Options, 139, 153
- IP address, 58
- IPv4, 140
- IPv6, 40, 140
- isembeddedwin, 83

K

- Kerberos authentication protocol, 108
- Keyboard layout, 162
- Keyboard Mapping Files, 162
- keycode, 84
- keyreportingmethod, 84
- km, 84

L

- Launch Parameters, 32
- Layout text, 164
- Layout text substitutions, 164
- License Change Request, 151
- License ID, 36
- License Manager Port, 16
- License Master, 150
- License Master ID, 36, 151
- License-file list, 16
- License-file list redundancy, 17
- Live collaboration, 34
- LM_LICENSE_FILE, 14, 16, 18, 19
- lmtools, 17
- Load Balancing, 3

- Local logon rights, 23
- Local Security Policy, 23
- Locality, 43
- Locality Name, 155, 157
- Log Directory, 97
- Log Files, 145, 146
- Log folder, 146, 147
- Log Folder, 100
- Logon Manager, 62
- Logon scripts, 62, 130

M

- Mac OS X, 82
- Mac OS X Gatekeeper, 4
- Maintenance, 146
- maintenance expiration date, 36
- Mapped drive, 31
- Mapped drives, 130
- MappedPrinterDrivers.xml, 115, 119, 120
- Master, 17
- Maximum number of sessions, 65, 107
- Maximum Sessions, 108
- Maximum sessions count, 65
- MEM, 60
- Mem usage, 60
- Memory requirements, 7
- Messages, 145
- Microsoft Management Console, 158
- Mobile App Console, 97
- Mobile App Toolbar Editor, 4
- Mobile Sense, 4
- MobileAppLogs, 97
- MobileAppSettings, 96
- Modifying the Host Port Setting, 39
- Multiple Input Locales, 164
- Multi-user deployment, 26, 133

N

- named pipe, 136
- NETWORK group, 46
- Network Printer, 24
- Network share, 130
- New Password, 50, 51
- noscale, 83
- NTFS, 32

O

- ODBC data sources, 31
- Ogg Vorbis, 126
- OpenSSL toolkit, 43, 153
- Optional, 71
- Options dialog, 75
- Organization Name, 155, 157
- Organizational Unit, 43
- Organizational Unit Name, 155, 157
- Output Level, 146

P

- password, 83
- Password Caching, 47

- Password Change, 50, 52
- Password Locations, 49
- PEM format, 158
- Performance Auto-Tuning, 142
- Performance counters, 3, 107
- Performance problems, 65
- Physical memory, 65
- port, 83
- Port, 39
- Port 491, 6, 98
- Port 80, 98
- Preview PDF, 113
- Print job scaling, 124
- Print Spooler Service, 112
- Printer Configuration, 115
- Printer drivers, 112, 120
- Printer Drivers, 119
- printer settings, 117
- printerconfig, 112, 116
- PrinterNameFormat, 123
- Printers Applet, 115, 116, 118
- Process
 - ending, 34
- Process ID, 59, 145
- Process information, 59
- Processes, 60
- Procs, 60
- Product Code, 36, 151
- Program Window, 30, 32, 53, 116
- Progress message, 61
- Progress Messages, 61
- proxy printer, 120
- Proxy printer names, 123
- proxy printers, 115
- Proxy server, 139
- Proxy tunneling, 3
- Proxy Tunneling, 139

Q

- QWORD, 138

R

- RapidX Protocol, 139, 152
- Recommended, 71
- Red x, 25, 101
- Redirection settings, 137
- redirector settings, 136
- Redundant license levers, 16
- Refresh rate, 59
- Relay server, 99, 101, 102, 103, 104, 107
- Remapping client drives, 128
- Remote Registry Service, 107
- Reset Printers, 118
- Resource limits, 61, 65
- Revoked,, 38
- Roaming user profiles, 23, 98
- RSA algorithm, 48
- RSA private key, 154
- RXP, 152

S

- Scaling, 149
- Screen scrape, 143
- Seats, 36
- Secure Socket Layer, 38
- Security, 22, 41
- Security Alert, 41
- Security Rollup Package, 6
- Serial and Parallel Ports, 126, 134, 138
- Server Connections, 108
- Server keys, 156
- Server Performance Counters, 108
- server.cfg, 156
- server.crt, 154, 157
- server.key, 154, 157
- Server-side password caching, 47
- Service Principle Name, 109, 111
- Session
 - encrypting, 41
 - terminating, 33, 34
- Session information, 58
- session license, 37
- Session limit, 66
- Session Name, 58
- Session Process Configuration, 134
- Session reconnect, 53, 99
- Session Reconnect, 3
- Session shadowing, 34
- Session Shadowing, 3
- Session Startup, 64
- Session termination, 53
- Session timeout, 53
- Sessions, 60
- Sessions tab, 53
- Shadowing a session, 34
- Shared account, 56, 57
- Shortcut, 144
- Silent installation, 144
- Sound, 126
- Sound card, 126
- SSL, 38
- SSL Certificate, 38, 42, 44, 154, 157
- SSL Security, 3
- SSL transport, 41
- Standard authentication, 45, 46
- Start Directory, 28, 30, 31, 33
- Start menu, 77, 144
- Startup State, 27, 30, 33
- Startup Time, 58
- Status bar, 60, 75
- strong encryption license, 37
- Support Request Wizard, 148
- System requirements, 6

T

- TCP, 38
- TCP packets, 6
- TCP/IP, 6, 98
- Templates, 146
- Test Page, 117
- Theme, 167
- Themes, 21
- Three-server redundancy, 16

- Time Zone Redirection, 3
- Toolbar Directory, 96
- Toolbar Editor, 90
- Trace Messages, 146
- Transmission Control Protocol, 38
- trial license, 38

U

- [ua-client.windows.exe](#), 87
- UNC, 31
- unicode, 84
- Uniface Anywhere App, 4, 80
- Uniface Anywhere Application Publishing Service, 10, 40, 110, 111
- Uniface Anywhere Host, 6, 23, 34, 53, 133, 146
- Uniface Anywhere Host Performance Counters, 108
- Uniface Anywhere Input Identifiers, 162
- Uniface Anywhere License Manager, 14
- Uniface Anywhere licenses, 5
- Uniface Anywhere Licenses, 36
- Uniface Anywhere shortcut, 77
- Universal Driver, 112
- Universal Printer Driver, 118, 119, 124
- UniversalRemotePrinter.ppd, 124
- Updates, 71
- USB drives, 127
- useApp, 80, 84
- User, 58
- User Accounts, 22
- User Profiles, 23
- User-specific scripts, 62

V

- VBScripts, 167
- Virtual memory, 65
- VMware, 6

W

- Warning period, 67
- Warnings, 146
- Web access, 87
- Web App, 4, 80
- Web proxy server, 139
- Web server address, 29
- Windows 7 Theme, 21
- Windows Client, 76
- Windows Compatibility Assurance, 69
- Windows Compatibilty Assurance, 5
- Windows Explorer, 23
- Windows folder, 112
- Windows Performance Monitor, 107
- Windows Updates, 69

X

- XPS Document Writer, 167

Y

Yellow x, 101