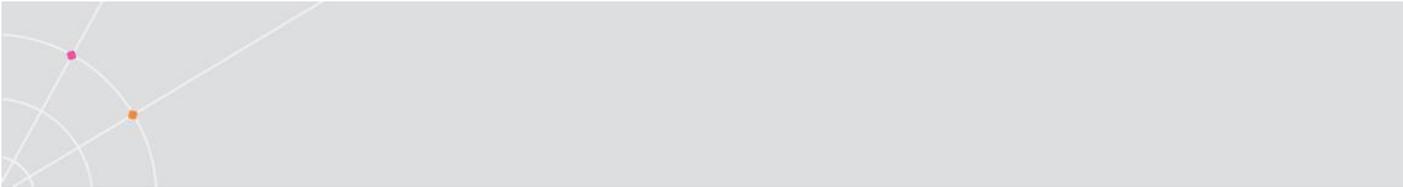# Ericom AccessNow™

HTML5 RDP Client

Administrator's Manual

Version 1.01

Legal Notice

This manual is subject to the following conditions and restrictions:

This Administrator's Manual provides documentation for Ericom AccessNow™.

The proprietary information belonging to Ericom® Software is supplied solely for the purpose of assisting explicitly and property authorized users of Ericom AccessNow™.

No part of its contents may be used for any purpose, disclosed to any person or firm, or reproduced by any means, electronic and mechanical, without the prior expressed written permission of Ericom® Software.

The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.

The software described in this document is furnished under a license agreement. The software may be used or copied only in accordance with the terms of that agreement.

Information in this document is subject to change without notice. Corporate and individual names, and data used in examples herein are fictitious unless otherwise noted.

Table of Contents

ABOUT THIS DOCUMENT

This manual provides instructions on how to install and use Ericom AccessNow to connect to virtual desktops and Terminal Servers from within HTML5 compatible web browsers. Follow the instructions in this manual and start enjoying the benefits of Ericom AccessNow within minutes!

This manual includes the following information:

- Overview of Ericom AccessNow

- Preparation and installation procedures

- Usage instructions

- Known issues and limitations

This manual assumes that the reader has knowledge of the following:

- Enabling RDP on Windows operating systems

- Firewall configuration

- Web server administration

Important terminology used in this document:

- RDP – Remote Desktop Protocol. A remote display protocol developed by Microsoft. RDP is a standard component of Microsoft Windows.

- RDP Host – a Windows system that can be remotely accessed using Microsoft RDP, such as a Terminal Server (RDS Session Host) or Windows workstation with remote access enabled.

- HTML5 – a new update to the HTML specification. Extends HTML with new features and functionality for communication, display, etc.

- WebSocket – a bi-directional, full-duplex communication mechanism introduced in the HTML5 specification.

- SSL – Secure Sockets Layer is a cryptographic protocol that provides communications security over the Internet.

For more information about this product and other Ericom products, please visit the Ericom website (www.ericom.com).
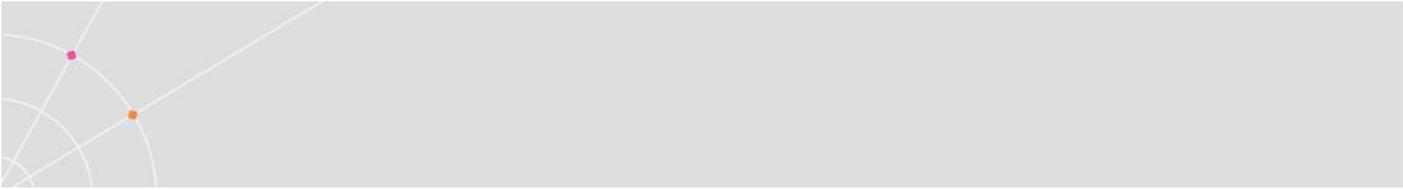
1. OVERVIEW

Ericom AccessNow provides end-users with remote access to Windows desktops and applications from any HTML5 compatible web browser. Any browser that supports HTML5 WebSockets and canvas can be used to launch the client, and enable users to interactively view and interact with the desktops and applications from within the browser window itself. This provides the following benefits:

- Access Windows desktops and applications from any device that has an HTML5 compatible web browser (currently limited to devices that have a physical keyboard and mouse)

- Perform remote access without needing to install or configure any software on the end-point device

- Works on platforms that only support web applications, and do not allow application installation, such as Google Chrome OS

- Same look-and-feel and functionality on any platform that has a HTML5 compatible browser

- No need to perform software updates or patches on end-point devices – new versions are simply downloaded from web server on-demand

- Remote Windows desktop and applications can be seamlessly integrated with other web-based applications and portals

- Very small download to the clients – approximately 500Kb

Architecture

*Ericom AccessNow* is comprised of three installable components:

a. A collection of web resources (HTML files, CSS, JavaScript, images, etc.), which are installed on a web server

b. AccessNow server (*WebSocket serv*er) that is installed on the RDP hosts

c. (Optional) Secure Gateway Service that provides secure, encrypted remote access to desktops and applications

This diagram describes how the components of AccessNow work together:
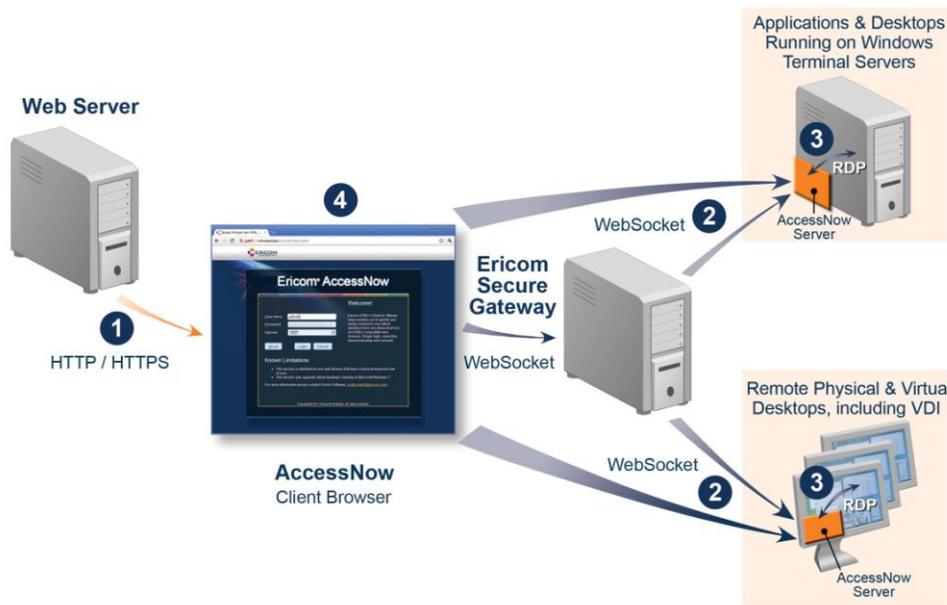
1. *The user initiates the process by directing the browser to the* **start.html** *page that is hosted on the web server. This page and its resources are downloaded to the browser using HTTP/HTTPS.*

2. *The browser opens a WebSocket connection to the AccessNow Server, which is usually running on the RDP host itself.*

   a. *If the optional Ericom Secure Gateway is used, the AccessNow browser session will connect through it using secure WebSockets.*

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

4. *The browser then displays the content of the remote desktop or application.*
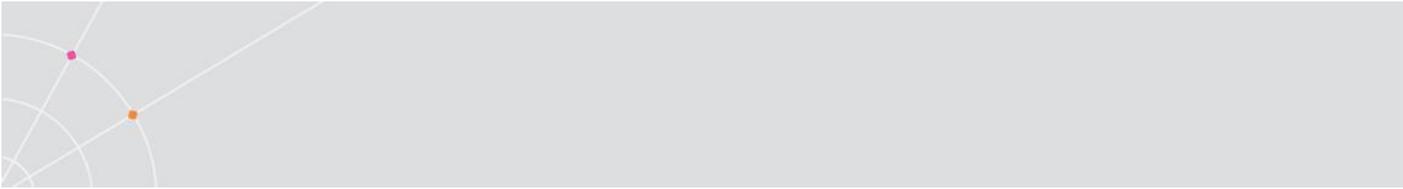
RDP Compression and Acceleration

Ericom AccessNow contains Ericom's technology for RDP compression and acceleration. This enhances remote desktop performance over the Internet. There are three main features in this technology:

- Image compression

- Packet shaping

- Whole frame rendering

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

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

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

2. INSTALLATION

Pre-requisites

The *AccessNow Server* must be installed on one of the following RDP hosts: Windows 7 Professional or higher, 2003, 2008, 2008 R2. Windows XP connections are supported by installing the AccessNow server on one supported platforms. The AccessNow Server cannot be installed on Windows XP yet, this functionality will be available in a future release.

The *AccessNow WebComponent* must be installed on a web server.

The session communication between the end-user and the remote desktops utilizes RDP, so *RDP access must be enabled on the desktops*.

Configure Firewalls

By default, the client (browser) connects to the virtual desktops using port 8080 for encrypted WebSocket communication and port 8081 for unencrypted WebSocket communication. In order to enable direct connection from the client to the RDP host (without using the gateway), the RDP host must be directly accessible from the client over the RDP port (default=3389). The default WebSocket port can be changed.

On the AccessNow Server, perform the following to configure the firewall on a Windows 7 or 2008 Server. Go to *Control Panel* and then *Windows Firewall.* Select *Advanced settings* and select *Inbound Rules*. Click *New Rule*.
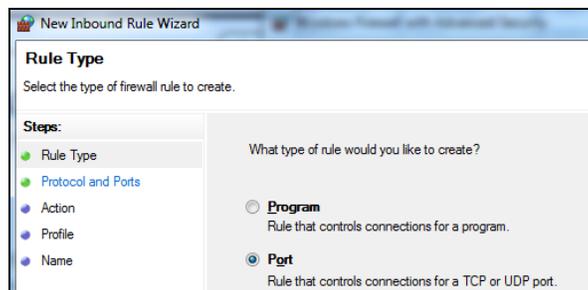
Select *Port* and click *Next*. Enter the specific ports: *8080, 8081*
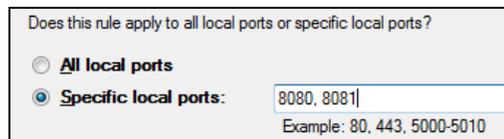
Click *Next* and select *Allow the connection*

Click *Next* and select the networks to apply the rule (Select All)

Click *Next* and give the rule a name (Ericom) and click *Finish*.

Disable Network Level Authentication

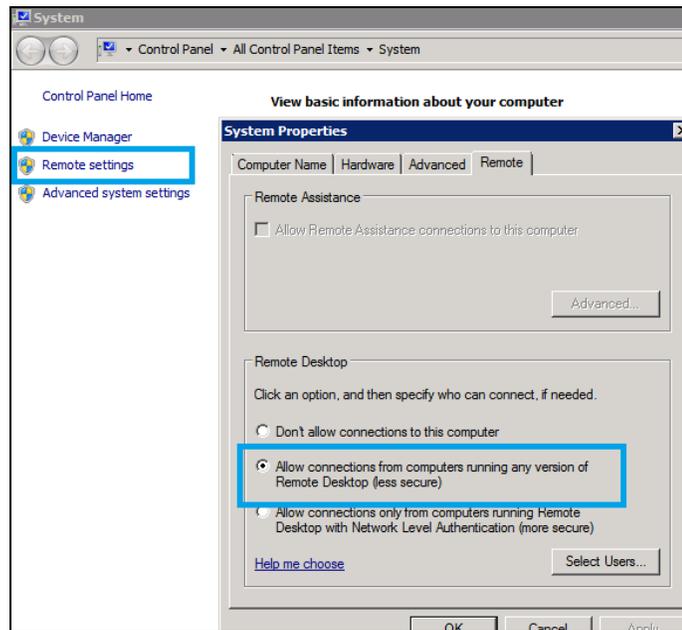AccessNow does not currently support *Network Level Authentication*. If this is enabled on the RDP Host, it must be disabled under the *Remote settings* properties.

To use Ericom AccessNow with the RDP host, select *Allow connection from computers running any version…*

AccessNow Server

Ericom AccessNow Server is the server-side service that translates RDP into WebSocket communication. The AccessNow Server should be installed on the RDP hosts. The AccessNow client interface, running inside the browser, connects to this service using WebSockets directly or through the Ericom Secure Gateway.

Installation

To install, launch *EricomAccessNowServer.msi* on the desired RDP hosts. When prompted, accept the *License Agreement* and then click *Install* to perform the installation. Authorization may be required to perform the installation on some workstations. At the end of the process click *Finish*:

The *Ericom AccessNow Server* runs as service, and can be started and stopped from the Windows Services Manager:
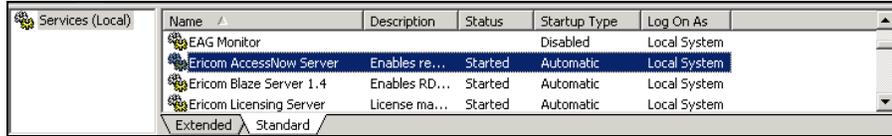
The service is configured to run automatically on system startup. If the service is stopped or is unable to listen on its default WebSocket ports (8080 and 8081), the end-user will not be able to connect to that host using the browser client. Make sure to configure firewalls and proxies between the end-point devices and the server-side component to allow communication using port 8080 or 8081 or both, or use Ericom Secure Gateway.

Changing the default WebSocket port

It is possible to change the default port for WebSocket communication between the client and the server.

Use a Registry editor and open the registry to:

On 32-bit (x86) Windows:

HKEY_LOCAL_MACHINE\SOFTWARE\Ericom Software\AccessNow

On 64-bit (x64) Windows:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ericom Software\AccessNow

Add a DWORD value named *Listening Port* and set it to the desired port number. After updating the registry, restart the AccessNow Server service. This port will then be used for encrypted communication instead of 8080. The value plus one will be used for unencrypted communication instead of 8081.

Uninstallation

Uninstall the Ericom *AccessNow Server* by using the Control Panel | Add/Remove Programs or Programs and Features. Select *Ericom AccessNow Server* and click *Uninstall*.
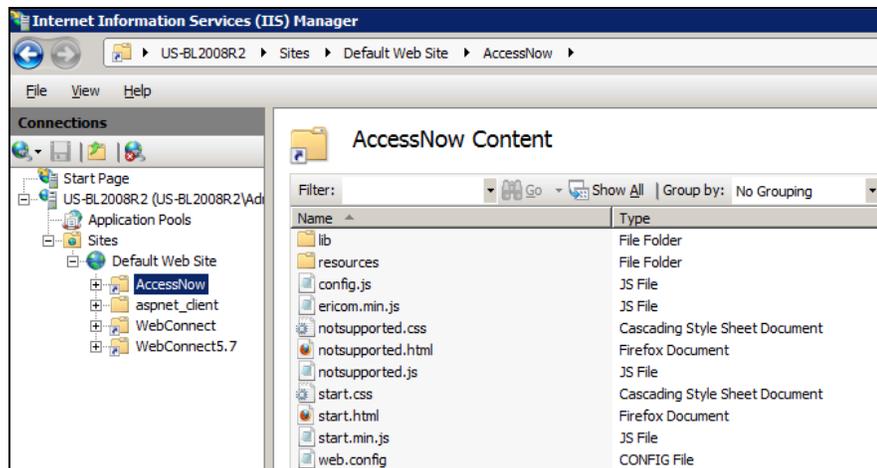
AccessNow Web Component

The web component provides the interface for users to connect to their remote application or desktop using a HTML5 compatible browser. The web resources are automatically downloaded from a web-server to the browser on the end-point device when the user connects to the provided Ericom URL.

Installation on Microsoft IIS web server

The web component for IIS servers is provided as an installer named **EricomAccessNowWebComponent.msi**. During the installation, a virtual directory named *AccessNow* will be automatically created in IIS. The *Start.html* page will be set as the default document for this virtual directory, so there is no need to explicitly enter the file name in the URL.

Once the web server files are installed, direct the users the appropriate URL (i.e. http://webserver/accessnow or http://webserver/accessnow/start.html).

Installation on web server

The web component is also provided as a zip file named *EricomAccessNowWebComponent.zip*.

On the target web server, create a virtual directory and extract the contents of the zip to that location. Once the web server files are installed, direct the users the appropriate URL. (i.e. http://webserver/accessnow/start.html).

Some web servers are case sensitive so make sure the correct URL is provided to the end users.
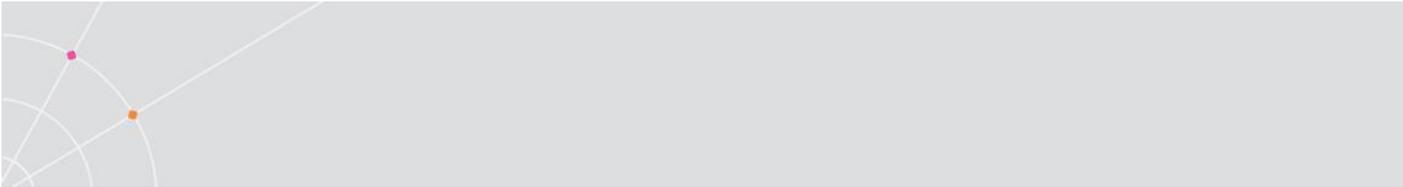
Configuration

An administrator can modify configuration settings for AccessNow by editing the **config.js** file that is installed as part of the web component onto the web server. This is a JavaScript file that can be modified using any text editor, such as Windows Notepad. Most settings in the file have the following format:

var name = value;

where the value can be a number, a flag (**true** or **false**), or string surrounded in quotes. To change the configuration, modify the file and save it.

The config.js contains the following configuration settings:

wsport	The WebSocket default port that will be used by the client. The value specified in the file (8080 by default) will be used for encrypted WebSocket communication. The value specified in the file plus one (8081 by default) will be used for unencrypted WebSocket communication. The user can override this value by explicitly specifying a port address in the client UI
gwport	The default gateway port that will be used if it is not explicitly specified in the address field
dialogTimeoutMinutes	Timeout period, in minutes, after which an inactive dialog is automatically closed and the session is logged off. This is only relevant for dialogs that have a logoff button.
sessionTimeoutMinutes	Timeout period, in minutes, after which an inactive session is disconnected. This timeout is reset whenever user clicks on the keyboard or a mouse button. The default value is 0, which disables this feature.
allowSpecialKeys	Enables support for special RDP key combination commands, such as CTRL+ALT+END which starts the Windows NT Security dialog box (similar to local CTRL+ALT+DEL).See http://support.microsoft.com/kb/186624 for the list of key combinations

defaults	Specify default values for all the fields in the connection dialog and the advanced settings dialog. To specify a field value:
	1. Remove the two forward slashes (//) at the beginning of the relevant line
	2. Change the value after the colon (:)
	A special setting is autostart – set this value to **true** to instruct AccessNow to start a session immediately without prompting the user for connection settings. Make sure to properly set all the required defaults before enabling this mechanism.
overwriteSaved	By default, changes to settings made by the user in previous sessions override the defaults. Set this flag to **true** to have the defaults overwrite previously saved settings.
showDownload	If set to **true**, displays a link in the connection dialog to download the AccessNow Server installer.

These settings only take effect after the user starts a new session. In some cases the local browser must be closed and reopened before changes take effect.

Secured WebSocket communication to remote desktops

The AccessNow Server uses a self-signed certificate for secure SSL connection by default. Google Chrome supports the default certificate for SSL-encrypted WebSocket connections.

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

Chrome OS, Safari 5.x, and Firefox will not allow connections using the default certificate so using direct, secured WebSocket communication with these browsers is currently not supported. The Ericom Secure Gateway is required if one of these browsers needs to be used with secured WebSockets.
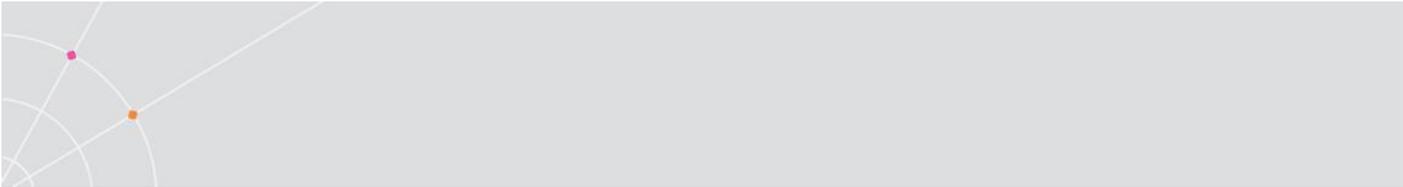
Secured WebSocket connections via Ericom Secure Gateway

When using the Ericom Secure Gateway, the connection between the AccessNow browser client and the Secure Gateway is always secured. The *Enable SSL* checkbox will secure the connection between the Secure Gateway and the AccessNow server.

✓ Enable SSL encryption for desktop session
✓ RDP Compression and Acceleration

Google Chrome and Chrome OS support the default certificate for SSL-encrypted WebSocket connections via the Secure Gateway. Opera browsers will notify the user that the server certificate is not signed, and prompt the user to continue.
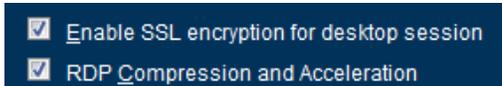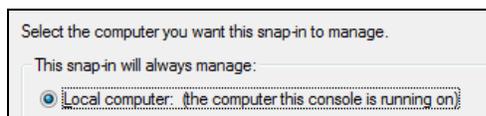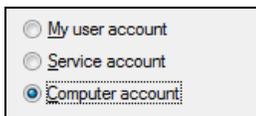
Safari 5.x and Firefox will not allow connections using the default certificate. A trusted certificate is required on the Ericom Secure Gateway server if one of these browsers will be used. These browsers will work with unsecured (no SSL) connections.

The Ericom Secure Gateway obtains the certificate from the Windows Certificate Store. The certificate will be located under the *Computer Account* store of the *Local Computer* location (this is where a trusted certificate would be imported to).

○ My user account
○ Service account
● Computer account

Select the computer you want this snap-in to manage.
This snap-in will always manage:
● Local computer: (the computer this console is running on)

The Ericom Secure Gateway identifies a certificate using a unique thumbprint that is configured in the Gateway's configuration file (EricomSecureGateway.exe.config).

<add key="CertificateThumbprint" value="<enter trusted cert val here>" />

The thumbprint value of the trusted certificate must be typed in (do not copy/paste). All spaces must be ignored. After the thumbprint has been updated, restart the Ericom Secure Gateway service.

3. USER ACCESS

With Ericom AccessNow, users can access remote Windows desktops and applications from HTML5 compatible web browsers. To start a session, users must navigate to *start.html* file that is installed in the AccessNow virtual directory on the web server.

Supported Browsers

Google Chrome 11 or higher, Apple Safari 5 or higher, Firefox 4 or higher, Microsoft IE 9 with Google Chrome Frame installed and Opera. For Firefox 4 and Opera WebSocket support must be enabled in the browser configuration. Multiple AccessNow sessions may be opened in different tabs within the web browser, or in different browser windows. When a session is not in use (its tab or window is not displayed) it will significantly reduce its CPU and memory utilization.

Configuration

When the user navigates to the URL, a login form will be displayed.
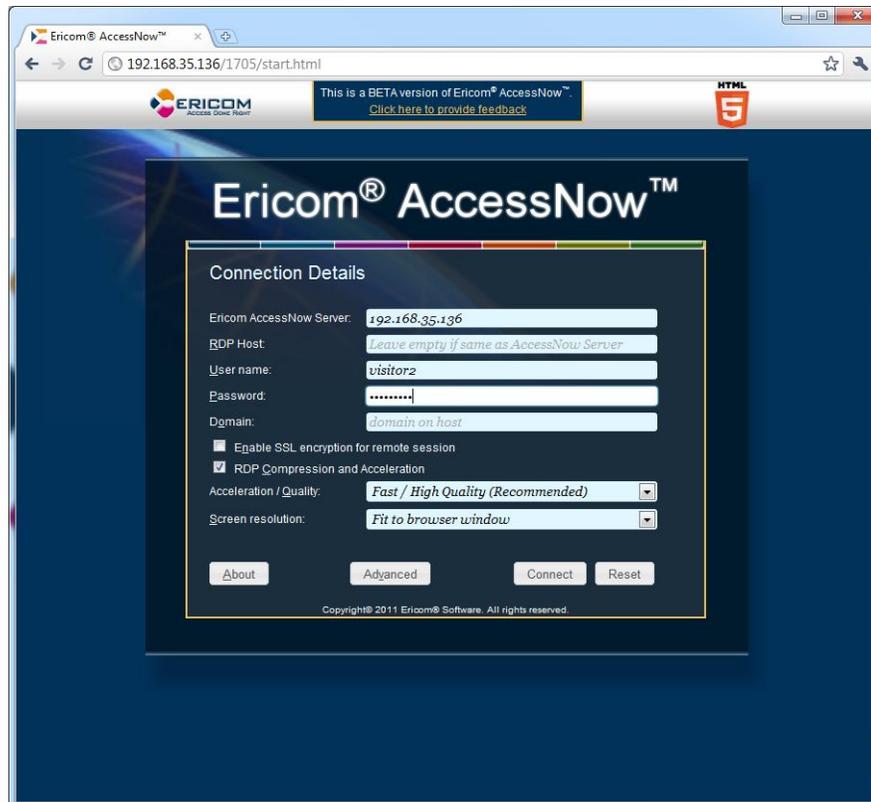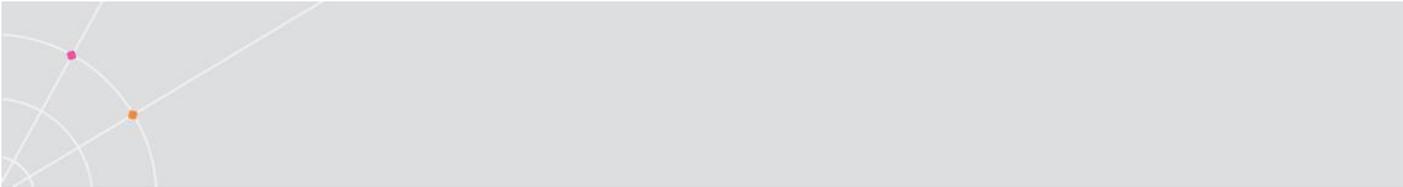
The user must enter the connection parameters to the target RDP host and press the *Connect* button to initiate the connection.

Connection Details	
Ericom AccessNow Server	The address (host name or IP address) of the AccessNow Server. If not specified, the web server host address (as it appears in the browser address line) will be used. Override default port settings by appending a colon and port number.
RDP Host	The address of the destination system that has RDP enabled. Leave this field blank if the AccessNow server is installed on the RDP host itself.
User name	The user's credentials to login to the RDP host. Can optionally contain domain specification, e.g. domain\user. When using Ericom Secure Gateway this field is mandatory. Otherwise this field is optional – if not specified then user will be prompted for credentials by the RDP host.
Password	Corresponding password for the user name. For security reasons, this value is never saved for future connections. When using Ericom Secure Gateway this field is mandatory. Otherwise this field is optional – if not specified then user will be prompted for credentials by the RDP host.
Domain	The user's domain if it is not specified in the user name.
SSL encryption for desktop session	When checked, the client utilizes SSL encrypted WebSocket communication to the AccessNow Server.
RDP compression and acceleration	When checked, enables lossy image compression for the session. Degree of quality loss / acceleration can be specified using drop down list.
Acceleration Quality	Controls the degree of acceleration that is enabled in the session. Faster acceleration will result lower quality images.

Screen resolution	Size of the virtual desktop for the session. The browser window will not be resized. If the remote desktop is larger than the browser window then scrollbar will be displayed. Select "fit to browser window" (default) to utilize the current browser window size. Select "fit to screen" to create a session that can cover the entire local screen; enable the browser's full screen mode to cover the entire local display.
About button	Displays the version number of the AccessNow client.
Advanced button	Configures the Secure Gateway and Application Launch setting
Connect button	Starts the connection based on the entered parameters. When the user clicks the *Connect* button, all configured settings are saved for future sessions.
Reset button	Clears all values that are saved and entered into the form and resets them to the defaults.

Advanced Settings

Click the *Advanced* button to set additional settings for the connection.

Advanced Settings ✕

☑ Use Ericom Secure Gateway
Gateway address: `192.168.35.136:4343`

☑ Start program on connection
Program path and file name: `c:\qf\app\qet.bat`
Start in the following folder:

OK   Cancel

Use Secure Gateway	Select this to use the Ericom Secure Gateway to connect to the RDP host. By default the port that is used is 443. To specify a custom port, add a ':' and the port number to the address (i.e., gateway.com:4343)
Start program on connection	Select this to only launch the specified application upon connection to the RDP host. The remote desktop will not be displayed.

Connecting to a Desktop

After a successful login, the user is connected to the specified desktop; the content of the virtual desktop is displayed within the browser window.
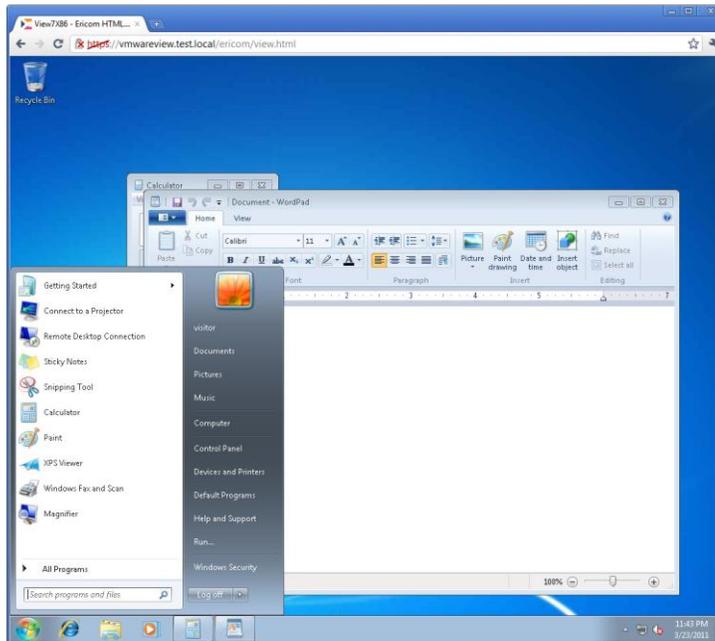
While it is connected AccessNow intercepts mouse button and keyboard events, and transmits them to the RDP host. As a result, various keyboard keys and mouse buttons that are usually handled by the browser, will behave differently. For example, clicking the F5 button usually causes the browser to reload the current page. When using AccessNow, F5 will not reload the page. Instead it will be transmitted to the remote application or desktop, and handled by them.

Clicking the Back, Forward or Reload browser buttons will cause AccessNow to display a message asking the user if he/she wishes to leave the current page. If the users decides to proceed, the remote session will be disconnected.

Connecting to a Windows XP Desktop

In order to connect to a Windows XP based RDP host, the connection must go through an AccessNow Server that is running on a supported platform (i.e. Windows 7). In the example below, the AccessNow server is running on a Windows 7 system. The user specifies the desired Windows XP based RDP host in the *RDP host* field. The AccessNow Server and RDP host should be in close proximity to each other to minimized latency.

Connecting to an Application

If an application is enabled and configured under *Start program on connection,* only the application will appear once the session is connected, covering the entire session area. The remote desktop will not be displayed.

Remote applications only work when connecting to Terminal Servers. Microsoft blocks this functionality when connecting to Windows workstation operating systems (i.e. Windows 7).
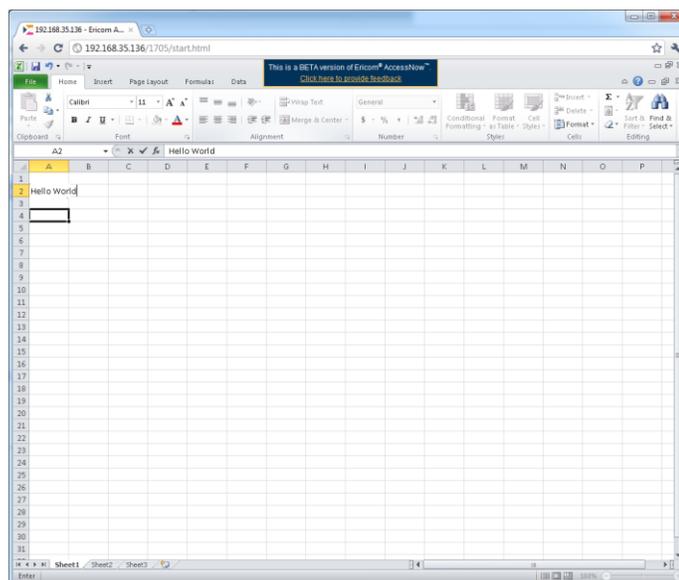
Connecting using a URL Query String

All settings under the *defaults* variable in the *config.js* file can be passed to the client as parameters in the URL.

Example: *http://server/accessnow/**?**autostart=true**&**address=192.168.1.100*

Common variables used in a query string	
autostart	(true, false) Starts a session automatically without the need to press the Connect button
address	(string) Address of the AccessNow server
full_address	(string) Address of the RDP Host
username	(string) Username to pass into the RDP session
password	(string) Password to pass into the RDP session (Warning: unencrypted in the URL)
domain	(string) User's domain if not specified in the username
blaze_acceleration	(true, false) Enables acceleration and compression

Supported RDP Shortcut Keys

Key combination	Description	Supported Modes
ALT+PAGE UP	Switches between programs from left to right.	Remote Desktop session only
ALT+PAGE DOWN	Switches between programs for right to left.	Remote Desktop session only
ALT+INSERT	Cycles through the programs in the order they were started.	Remote Desktop session only
ALT+HOME	Displays the **Start** menu.	Remote Desktop session only
CTRL+ALT+END	Brings up the **Windows Security** dialog box. Similar to CTRL+ALT+DEL on a local system.	Remote Desktop session and Application Launch modes

Ending a Session

After the user logs out or disconnects, a "Session ended" message appears. The browser returns to the connection dialog after the user clicks *OK*.

After the session ends, no trace of the session will remain on the device.

Google Chromebooks

Ericom AccessNow operates on a Google Chromebook just like it does with a Google Chrome browser. Here are some tips to keep in mind when using AccessNow on a Chromebook:

Function	Description
Mouse Left-click	Click the Chromebook trackpad with *one* finger
Mouse Right-click	Click the Chromebook trackpad with *two* fingers
Scrolling a document or website	Drag *two* fingers on the Chromebook trackpad up or down to scroll
Configure Chromebook	Enter into the address field: *chrome://settings*

Configuring Firefox and Opera browsers

Firefox and Opera browsers disable WebSocket by default. WebSocket must be enabled on these browsers to use the Ericom AccessNow. Note that browser updates may reset these values.

Enabling WebSocket for Firefox

1. Type **about:config** in the Location bar

2. If a warning is displayed, click button to proceed

3. In the Filer box type: **websocket**

4. Double-click on the displayed items to change their values to **true**

5. Close the browser (all windows / tabs) and launch it again

Enable WebSocket for Opera

1. Type **opera:config** in the Location bar

2. In the Quick find box type: **websocket**

3. Enable the checkbox

4. Click on the Save button

5. Close the browser (all windows / tabs) and launch it again

Configuring Microsoft Internet Explorer

AccessNow supports Microsoft Internet Explorer 9 with Google Chrome Frame installed. Visit this website for more information: http://www.google.com/chromeframe

Unsupported Browsers

If a user tries to access the Ericom AccessNow URL from an unsupported browser an error message will be displayed:

This browser does not support WebSockets

You are using Microsoft Internet Explorer, which does not support HTML5 WebSockets. For this product to work you must use a different web-browser such as the latest versions of Google Chrome or Apple Safari.

Known Limitations

- The current version only works on devices with a physical keyboard. Support for virtual keyboards on Apple iPad, Apple iPhone, and Android devices will be available in a future release.

- Printing functionality is not available yet. This feature is on the roadmap and scheduled for a future release.

- The AccessNow Server cannot be installed directly on Windows XP yet, this functionality will be available in a future release.
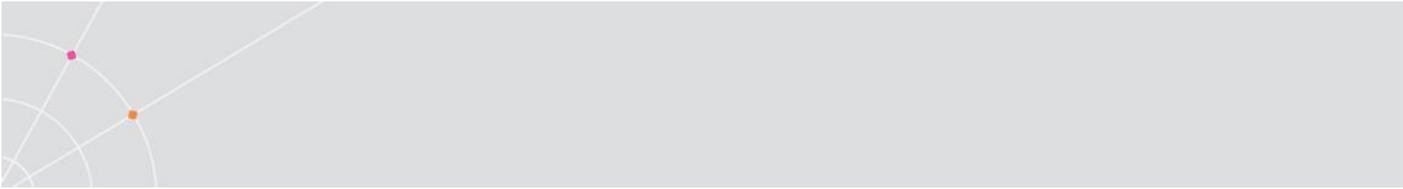
ABOUT ERICOM

Ericom® Software is a leading provider of Application Access and Virtualization Solutions. Since 1993, Ericom has been helping users access business-critical applications running on a broad range of Microsoft® Windows® Terminal Servers, Virtual Desktops, Blade PCs, legacy hosts, and other systems. Ericom provides concrete business value by helping organizations realize the benefits of their IT investments. With offices in the United States, United Kingdom, EMEA, India and China, Ericom also has an extensive network of distributors and partners throughout North America, Europe, Asia, and the Far East. Our expanding customer base is more than 30 thousand strong, with over 7 million installations.

For more information on our products and services, contact us at the location nearest to you.

And visit our web site: http://www.ericom.com

North America	**Western Europe**	**International**
Ericom Software Inc.	Ericom Software (UK) Ltd.	Ericom Software Ltd.
231 Herbert Avenue, Bldg. #4	11a Victoria Square	8 Hamarpeh Street
Closter, NJ 07624 USA	Droitwich, Worcestershire	Har Hotzvim Technology Park
Tel +1 (201) 767 2210	WR9 8DE United Kingdom	Jerusalem 91450 Israel
Fax +1 (201) 767 2205	Tel +44 (0) 845 644 3597	Tel +972 (2) 591 1700
Toll-free 1 (888) 769 7876	Fax +44 (0) 845 644 3598	Fax +972 (2) 571 4737
Email info@ericom.com	Email info@ericom.co.uk	Email info@ericom.com