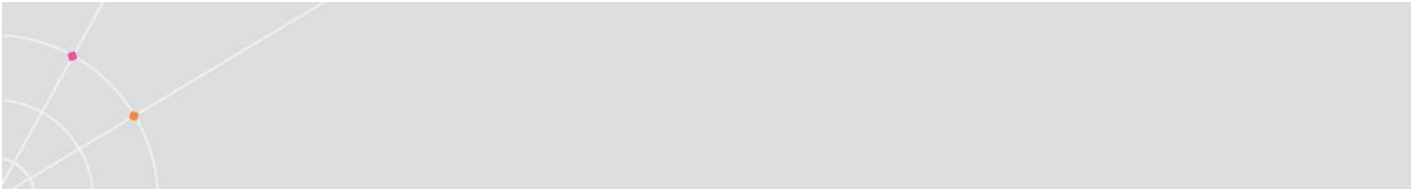


Ericom AccessNowTM

HTML5 RDP Client

Administrator's Manual

Version 2.0



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 properly 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.

Copyright © 1999-2012 Ericom® Software.

Ericom is a registered trademark and AccessNow is a trademark, of Ericom® Software. Other company brands, products and service names, are trademarks or registered trademarks of their respective holders.

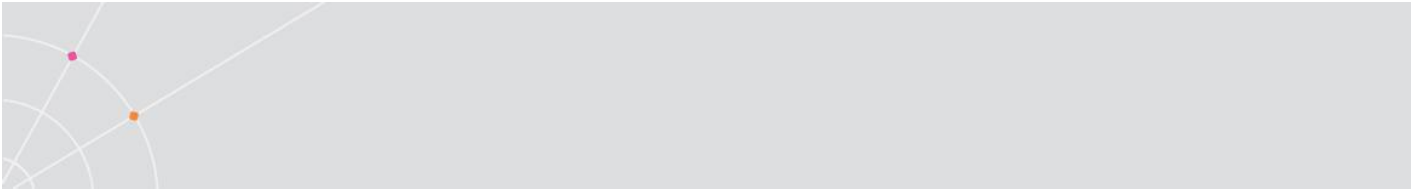
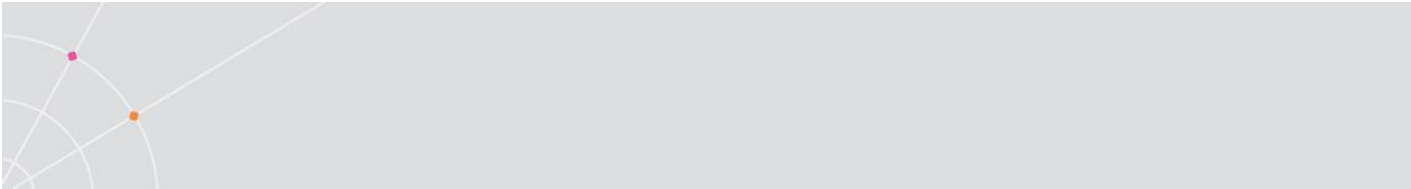


Table of Contents

LEGAL NOTICE	2
ABOUT THIS DOCUMENT	5
1. OVERVIEW.....	6
Architecture	6
RDP Compression and Acceleration	7
What's New in 2.0	8
Getting Started in 5 Minutes	8
2. INSTALLATION.....	10
Pre-requisites	10
AccessNow Server.....	12
AccessNow Web Component	18
Secure Connections.....	19
3. USER ACCESS	20
Supported Browsers	20
Connection Web Page	20
Connecting to a Desktop.....	23
Connecting to an Application	24
Connecting to an Application in Kiosk Mode	25
Clipboard Support	25
File Transfer	27
Printing	29
Supported RDP Shortcut Keys	30
URL Redirection.....	30
Ending a Session	31
Configuring Firefox and Opera browsers.....	31
Browser Extension Conflicts	32
4. GOOGLE CHROMEBOOKS	33
Chromebook Keyboard	33
5. TABLET AND SMARTPHONES	35
6. HTTPS MODE	36
7. ADVANCED CONFIGURATION	37
Static Configuration of <i>Config.js</i>	37
Passing URL Query Strings	37
Define Configuration Groups	38
Passing Cookies	39



Settings Precedence	39
Settings Table	39
Sample HTML - Passing Cookies into AccessNow	43
8. ACCESSNOW SERVER FOR LINUX	46
Pre-requisites	46
Installation	46
Usage	47
9. JUNIPER SSL VPN CONFIGURATION	48
Adding an AccessNow connection to Juniper	48
Web Proxy (no download required)	49
Network Connect	50
JSAM and WSAM	50
10. LOAD BALANCERS	52
11. TECHNICAL SUPPORT	54
TSAgent Update	54
Requesting Support	54
ABOUT ERICOM	55



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.



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

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 server*) that is installed on, or next to the RDP hosts
- c. (Optional) Ericom Secure Gateway enables access from outside the organization

This diagram illustrates 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 is displayed in the web 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.
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

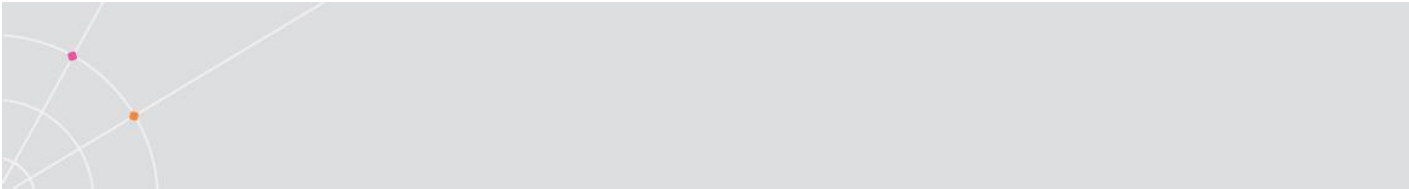


Image compression compresses images before transmitting them to the browser for rendering. The level of compression is dependent on the acceleration/quality level selected by the user (a default value can be configured by the administrator).

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.

What's New in 2.0

- Printing: print files from the RDP session to the local printer
- Print as PDF: save print output from the RDP session to the local device as PDF files
- File Transfer: transfer files between local and remote sessions
- Support for tablets and smartphones (devices with virtual keyboards)
- URL Redirection (open URL's using local browser)
- HTTPS mode (support for SSL VPN and proxies that do not support WebSockets)
- Microsoft Internet Explorer 9 support without requiring Google Chrome Frame

Getting Started in 5 Minutes

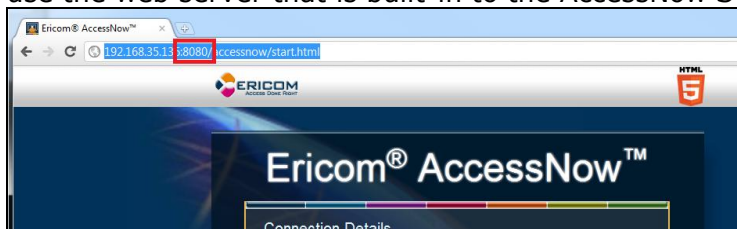
Ericom AccessNow is a feature rich and flexible application. The manual covers all available features in detail to help customers best configure AccessNow to fit their environment.

The AccessNow application is very quick and easy to install. The basic installation will take approximately five minutes and will make a Windows RDP host (server or workstation) accessible from a Google Chrome web browser, Google Chromebook, Mozilla Firefox 8, and Apple Safari 5 web browser. Here are the steps to install and use AccessNow in five minutes:

- 1) Download the Ericom AccessNow Server MSI installer (EricomAccessNowServer.msi) from the Ericom website (since download speeds vary, the time to download the MSI is not counted in the five minutes)

- 2) Run the MSI installer and click *Next* through all the dialog boxes and then *Finish* at the last one
- 3) Configure (or disable) the Windows Firewall for use with AccessNow.
 - a. Go to the Windows *Control Panel* and open *Windows Firewall*
 - b. Click "Allow Program or Feature ..."
 - c. Click "Allow another program ..."
 - d. Click *Browse* and navigate to <drive>:\Program Files (x86)\Ericom Software\Ericom AccessNow Server\AccessNowServer32.exe
 - e. Click *Add* and then *OK*
- 4) Once the AccessNow Server is installed, it is ready for use. The AccessNow Server contains a built-in web server to allow users to connect its URL: <https://machineaddress:8080/accessnow/start.html>

The AccessNow port must be specified in the URL to tell the browser to use the web server that is built-in to the AccessNow Server service.



- 5) Once the AccessNow web page appears, click the *Connect* button. The empty fields will automatically use the address of the server specified in the URL. Enter the user credentials if desired and it will be passed to the RDP session.



- 6) The connection dialog will appear momentarily while the web browser connects to the RDP host where the AccessNow Server is installed.



2. INSTALLATION

Pre-requisites

The *AccessNow Server* is compatible with all released versions of Windows from XP on up. It also supports all these versions of Windows as RDP hosts. In general, it is recommended to install the *AccessNow Server* on the RDP host itself. The *AccessNow Server* is highly efficient, and will have little or no impact on the RDP host's performance and scalability.

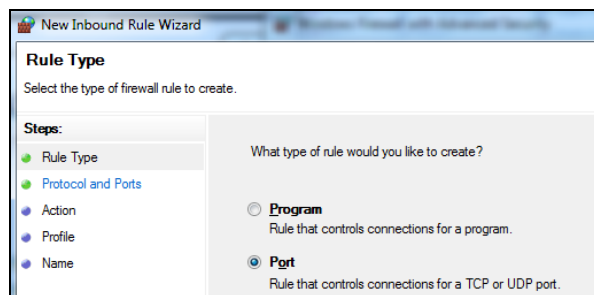
The *AccessNow Web Component* must be installed on a web server. The *AccessNow Server* includes a built in web server along with the *AccessNow* web component.

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

Configure Firewalls

By default, the client (browser) connects to the *AccessNow Server* using port 8080 for both encrypted and unencrypted WebSocket communication. This port number can be changed using the *AccessNow Server Configuration* utility. In order to enable direct connection from the client to the *AccessNow Server* (without using the Gateway), the server must be directly accessible from the client using that port. If the *AccessNow Server* is not installed on the RDP host then the RDP host must be directly accessible from it over the RDP port (default=3389).

If the Windows firewall is enabled on the same computer where the *AccessNow Server* is installed, make sure to configure it to enable the *AccessNow* client connection. On 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 port: *8080*

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

All local ports

Specific local ports:

Example: 80, 443, 5000-5010

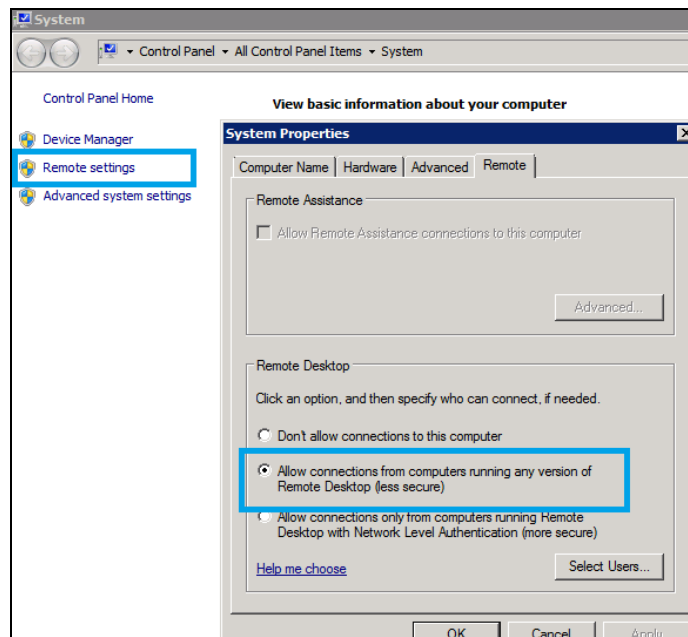
Click *Next* and select *Allow the connection*

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...*

Bind Service to All Network Interfaces

In a virtual network environment - it is recommended to bind the AccessNow Server to use all virtual network interfaces, rather than just one virtual NIC. Always ensure that the network interface(s) that AccessNow Server is using is accessible by the desired group of end-users.

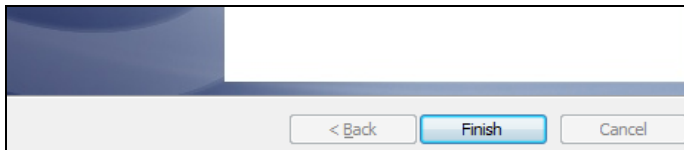
AccessNow Server

Ericom AccessNow Server is the server-side service that translates RDP into WebSocket communication. The AccessNow Server may be installed on the RDP host or on a dedicated system to serve as a proxy. It is strongly recommended to install the AccessNow Server on the RDP host to achieve the best performance and to use certain features such as File Transfer.

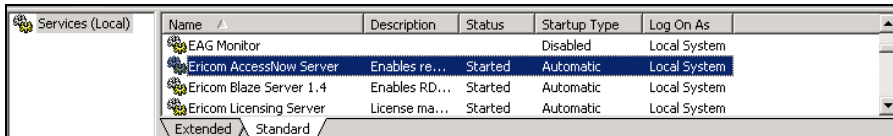
The AccessNow client interface, running inside the browser, connects to this service using WebSockets directly or through the Ericom Secure Gateway.

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 systems. At the end of the process click *Finish*:



The *Ericom AccessNow Server* runs as a service, and can be started and stopped from the Windows Services Manager:

A screenshot of the Windows Services Manager. The 'Services (Local)' tree is expanded. The 'Ericom AccessNow Server' service is selected and highlighted. The table below shows the details of the service.

Name	Description	Status	Startup Type	Log On As
EAG Monitor			Disabled	Local System
Ericom AccessNow Server	Enables re...	Started	Automatic	Local System
Ericom Blaze Server 1.4	Enables RD...	Started	Automatic	Local System
Ericom Licensing Server	License ma...	Started	Automatic	Local System

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), the client will not be able to connect to that host. Make sure to configure firewalls and proxies between the end-point devices and the server-side component to allow communication using port 8080, or use Ericom Secure Gateway.

NOTE AccessNow Server cannot be installed on systems where the hostname contains non-English characters.

AccessNow Server Configuration

The Server Configuration console presents a series of tabs that allow the administrator to configure various settings for the server service. The Configuration console only works on systems with Microsoft Internet Explorer 7 or later. The console may not operate properly if IE6 is installed.

NOTE When installing AccessNow Server on a Terminal Server, it is recommended to hide the *Server Configuration* application from end users to prevent unexpected changes to the server's settings.

General

This page provides functions to restart and stop the AccessNow Server service. For certain configuration changes, a service restart is required. This page also displays the number of active AccessNow sessions connected to this system.

IMPORTANT: Whenever the AccessNow Server service is restarted, all sessions on the server will be disconnected.



Licensing

This page displays licensing information for the AccessNow Server. The *Connected to licensing server* field indicates the license server that is currently in use.

When sharing a pool of licenses across multiple AccessNow Servers, create a centralized license server to distribute the licenses.

By default, AccessNow Server uses DNS lookup to locate the Licensing Server. The DNS entries used are *ericom-license-server.<domain-name>* or *_ericom-license-server._tcp.<domain-name>*. If the DNS entries do not exist, the AccessNow server attempts to connect to a Licensing Server that is running on the same computer as itself.

The other option is to explicitly specify the address of the Licensing Server in the AccessNow Server Configuration under *Licensing server address*. After changing the Licensing Server address restart the AccessNow Server service using the *Service* tab.

The license server communicates over port 8888 by default.

General | Licensing | Performance | Communication | Acceleration | Security | Logging | Advanced

Information | Activation

AccessNow		AccessNow_VMwareView	
License type:	Concurrent Users	License type:	Concurrent Users
License duration:	Grace (6 days left)	License duration:	Grace (6 days left)

Connected to licensing server: <offline>

Use DNS lookup
 Licensing server address:

Changing this setting may take effect only after the AccessNow Server service is restarted.

Specify the address - domain name or IP address - of the centralized Licensing Server. An empty value instructs AccessNow to locate the Licensing server using DNS lookup. If DNS lookup does not succeed, the locally installed Licensing server will be used.

Manage Licensing Service on localhost

If no valid license is found, AccessNow Server will continue to run if the grace period has not expired. Once the grace period expires, AccessNow Server will not allow user sessions.

Licensing Activation

Click on *Licensing | Activation* to enter the serial number and activation key into the product's configuration. To activate an installation from an evaluation, send the "key to send to Ericom" along with the serial number to supportusa@ericom.com for processing. An activation key will be returned. Once the activation key is entered, click on the *Activate License* button. The AccessNow Server does not have to be restarted for the license to take effect.

NOTE AccessNow and AccessNow for VMware View are licensed separately. To select the mode to activate, click on the *Client type* drop down menu

General | Licensing | Performance | Communication | Acceleration | Security | Logging | Advanced

Information | Activation

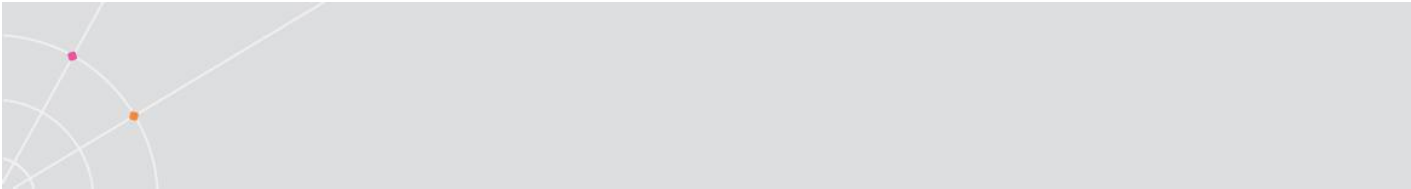
Client type: AccessNow

License Description:
 License Status: Valid
 License Type: Concurrent Users
 Counting Mode: Permanent
 Expiration Date: Never Expires
 Number of Licenses: 20

If you have received a serial number from Ericom, please enter it into the field below before clicking the "Email to Ericom" button.

Serial Number:
 Key to send to Ericom:
 Key received from Ericom:

Copy the key received from Ericom Software into the form and click the "Activate License" button to activate the software license.



Performance

This page displays current performance statistics related to AccessNow connections.

Communication

This page provides functions to change the AccessNow listening port and the address of the host running RDP.

When using an AccessNow listening port other than the default (8080), the port number must be explicitly specified in the client address field (i.e., 192.168.1.1:5678)

The RDP host address is used when the destination system is not the system running AccessNow Server. In this scenario, the AccessNow server is acting as a proxy between the end user and the destination RDP host system. This type of configuration is not optimal as it requires an additional network hop.

Changes to both settings require a service restart (see Service page).

General | Licensing | Performance | **Communication** | Acceleration | Security | Logging | Advanced

AccessNow port number:

Changing this setting will take effect only after the AccessNow Server service is restarted.

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

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

RDP host address:

Changing this setting will take effect only after the AccessNow Server service is restarted.

Specifies the address - domain name or IP address - of the RDP host for which AccessNow acceleration is used. Best performance is achieved when the AccessNow Server is installed on the RDP host itself. In that case the address *localhost* should be used.

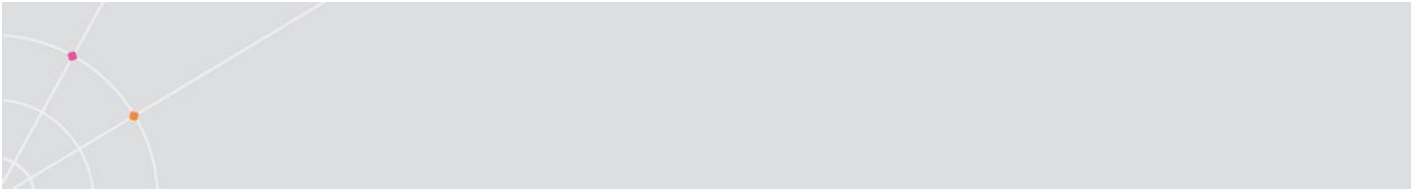
When connecting to *localhost* AccessNow Server will automatically determine the RDP port by retrieving that value from the system. When connecting to any address other than *localhost*, AccessNow Server will connect to the default RDP port, which is port 3389. To specify a different port use the format: *address.port-number*

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

Acceleration

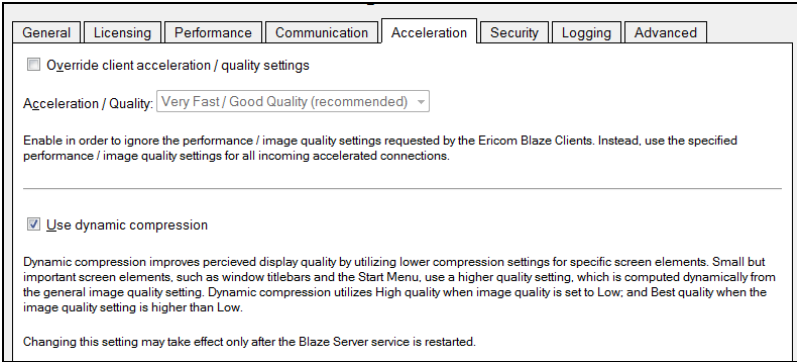
This page provides functions to force the Acceleration/Quality level and disable dynamic compression. When the *Override client acceleration / quality settings* checkbox is checked all sessions will use the configured setting. All client settings will be ignored. When checking or unchecking this setting,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

Dynamic Compression identifies small graphical objects on the screen (such as toolbar icons, taskbar icons, Start Menu icons, etc.) and compresses them using high *quality* when the *Quality* setting is set to *Low*; and at the best quality when



the *Quality* setting is higher than *Low*. All other graphical objects are compressed at the selected quality. This provides the visual impression of a high quality remote desktop session.

By default, this feature is enabled. To disable, uncheck the “Use dynamic compression” box.



Security

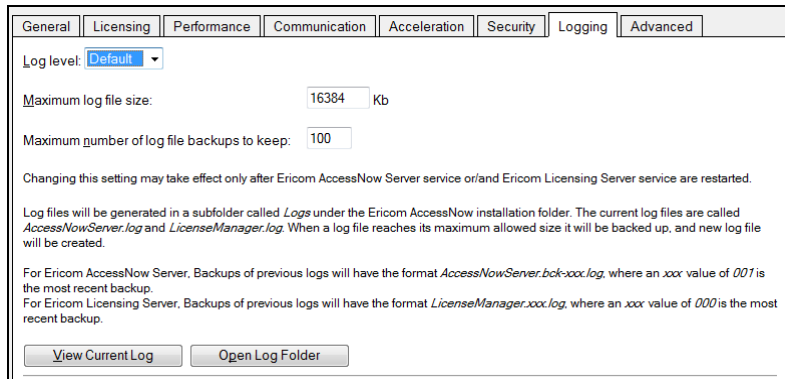
This page configures the AccessNow security settings.



Ericom AccessNow provides integrated *128-bit SSL* encryption. For best performance, set the host’s RDP Security Encryption level to Low and change the *Encrypt AccessNow communication* to *Always*. Using this configuration, Ericom AccessNow SSL encryption will be used instead of the RDP encryption.

Logging

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



Advanced (For Administrator Use Only)

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

Open Registry – opens the Registry editor and displays the location where the Ericom AccessNow Registry keys are stored.

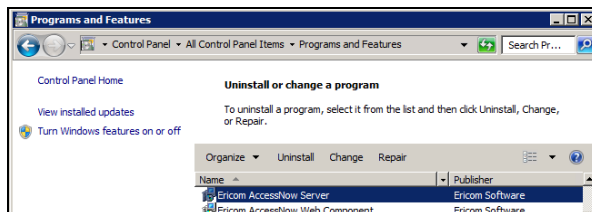
Export Settings – exports the AccessNow Server Registry key to the user's home folder (i.e., My Documents).

Import Settings – imports previously saved AccessNow Server Registry settings.

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

Uninstalling AccessNow Server

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

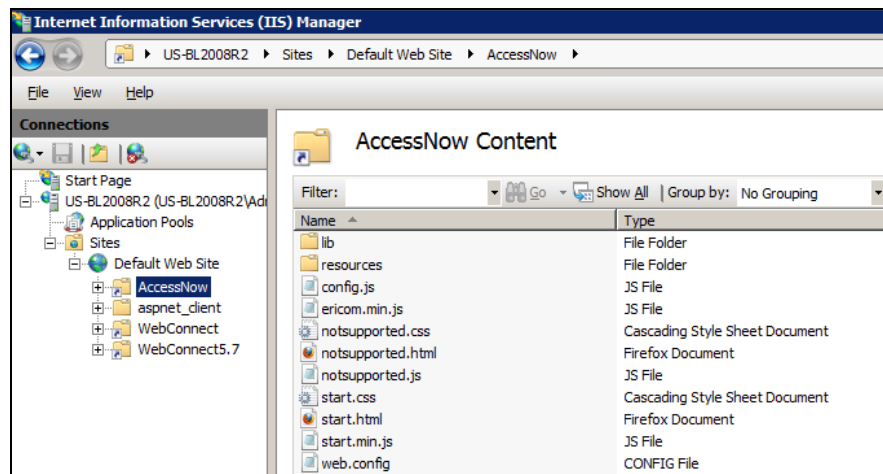
Installation with AccessNow Server

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

<drive letter>:\Program Files\Ericom Software\Ericom AccessNow Server\WebServer\AccessNow

Installation on Microsoft IIS web server

The web server 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: <http://webserver/accessnow> or <http://webserver/accessnow/start.html>

For example: <http://rdpdemo.ericom.com/accessnow>

Installation on web server

The web server 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.

Modifying the logo image

The AccessNow start page is comprised of a group of images. Any of the standard images may be edited and replaced with a custom image. For example, to replace the Ericom logo, open the *ericom.jpg* file using an image editor (i.e. MS Paint) and paste in the desired custom image. It is recommended to keep the new image as close to the same dimensions as the original image. Default *ericom.jpg* image:



Secure Connections

Secured WebSocket communication to remote desktops

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

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

Chrome OS, Safari 5.x, and Firefox will not allow connections using self-signed certificate. In order to provide connectivity from these browsers, the Ericom Secure Gateway along with a trusted certificate must be used.

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 Ericom Secure Gateway is installed with a self-signed certificate by default, but supports trusted certificates as well. Please read the *Ericom Secure Gateway Administrator's Manual* for full instructions on how to install and configure it for use with Ericom AccessNow.

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 and higher, Apple Safari 5 and higher, Firefox 4 and higher, Microsoft IE 10 (BETA), IE 9 with Google Chrome Frame installed and Opera. For Firefox 4/5 and Opera, WebSocket support must be enabled in the browser configuration. Firefox 6 does not require any configuration change.

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 reduce its CPU and memory utilization.

Connection Web Page

When the user navigates to the URL, a login form will be displayed.

Ericom® AccessNow™

Connection Details

Ericom AccessNow Server:

RDP Host:

User name:

Password:

Remember password

Domain:

Enable SSL encryption for remote session

Compression and Acceleration

Acceleration / Quality:

Screen resolution:

Keyboard locale:

Copyright© 2012, Ericom® Software. All rights reserved.

The user must enter the connection parameters to the target RDP host and press the *Connect* button to initiate the connection.

Connection Details	
<i>Ericom AccessNow Server</i>	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.
<i>RDP Host</i>	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.
<i>User name</i>	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.
<i>Password</i>	Corresponding password for the user name. For security reasons, this value should not be saved for future connections. When using Ericom Secure Gateway this field is mandatory. Otherwise this field is optional – when not specified then user will be prompted for credentials by the RDP host.
<i>Remember Password</i>	When this setting is checked, the password that is entered for the current session will be saved for the next session. When this setting is unchecked, the password that is entered for the current session will <i>not</i> be saved for the next session.
<i>Domain</i>	The user's domain if it is not specified in the user name.
<i>SSL encryption for desktop session</i>	When checked, the client utilizes SSL encrypted WebSocket communication to the AccessNow Server.
<i>RDP compression and acceleration</i>	When checked, enables lossy image compression for the session. Degree of quality loss / acceleration can be specified using drop down list.
<i>Acceleration Quality</i>	Controls the degree of acceleration that is enabled in the session. Faster acceleration will result lower quality images.

<i>Screen resolution</i>	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.
<i>Keyboard Locale</i>	Selects the keyboard region to be used in the AccessNow session
<i>About</i> button	Displays the version number of the AccessNow client.
<i>Advanced</i> button	Configures the Secure Gateway and Application Launch setting.
<i>Connect</i> button	Starts the connection based on the entered parameters. When the user clicks the <i>Connect</i> button, all configured settings are saved for future sessions.
<i>Reset</i> button	Clears all values that are saved and entered into the form and resets them to the defaults.

Advanced Settings

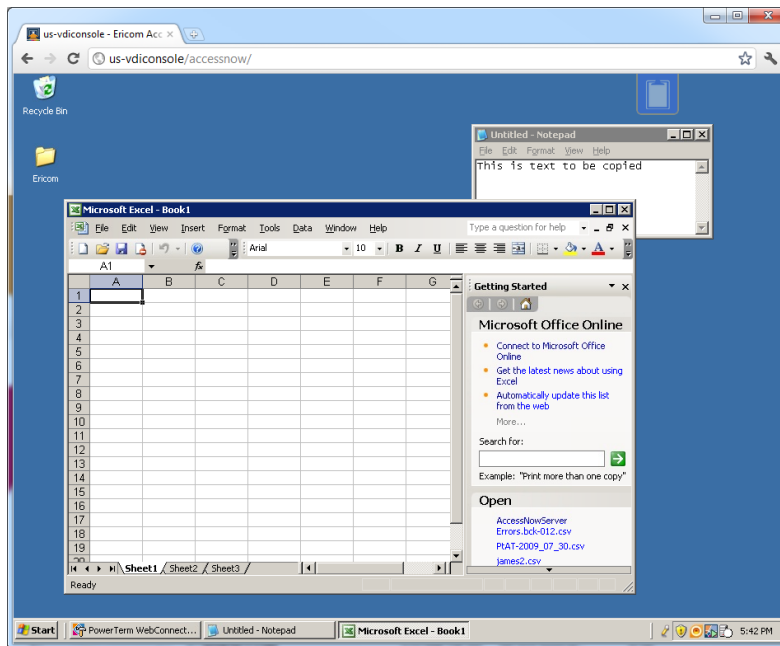
Click the *Advanced* button to set additional settings for the connection.

<i>Use Secure Gateway</i>	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).
<i>Remote Audio Playback</i>	Configure where the session's sound will play at: local computer, remote computer, or do not play.
<i>Keyboard scan-codes</i>	Enables scan codes. Certain applications use scan codes and will require this setting to be enabled.
<i>Start program on connection</i>	Select this to only launch the specified application upon connection to the RDP host. The remote desktop will not be displayed.
<i>Open links on client (URL Redirection)</i>	Will open URL links launched in the RDP session to open using the local browser.

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.

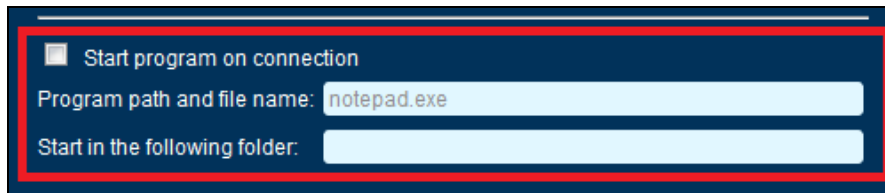


While it is connected AccessNow intercepts mouse button and keyboard events, and transmits them to the RDP host. As a result, various keyboard keys and mouse buttons that are usually handled by the browser, will behave differently. For example, clicking the F5 button usually causes the browser to reload 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.

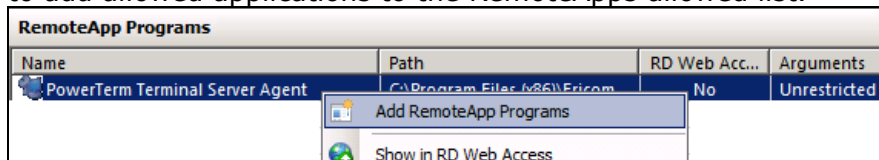
Clicking the Back, Forward or Reload browser buttons will cause AccessNow to display a message asking the user if he/she wishes to leave the current page. If the users decides to proceed, the remote session will be disconnected.

Connecting to 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.



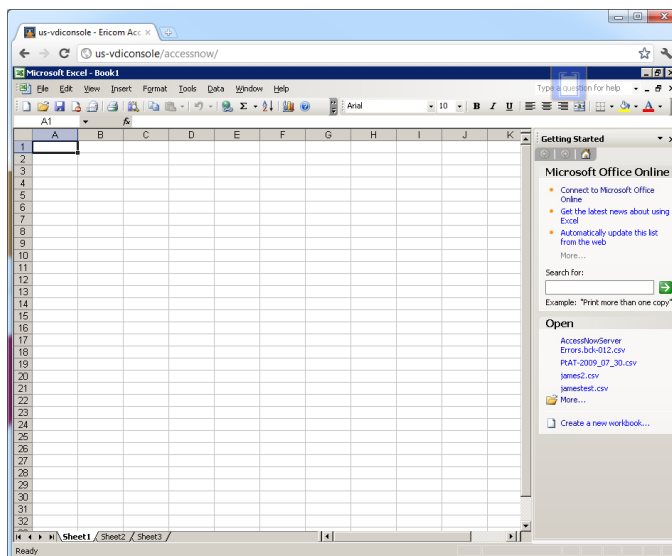
On Windows 2008 Terminal Services and Remote Desktop Services remember to add allowed applications to the RemoteApps allowed list.



Name	Path	RD Web Acc...	Arguments
PowerTerm Terminal Server Agent	C:\Program Files (x86)\Ericom...	No	Unrestricted

Remote applications only work when connecting to Terminal Servers. Microsoft blocks this functionality when connecting to Windows workstation operating systems (i.e. Windows 7).

Open applications cannot be minimized. Users can close the application by clicking on the X button. After the user closes the application, the session will be automatically terminated in approximately three seconds.





Connecting to an Application in Kiosk Mode

Applications may be displayed in a kiosk mode such that it will cover the entire monitor (in multi-monitor configurations only the primary monitor is covered). To create a kiosk mode application using AccessNow and Google Chrome, perform the following:

- 1) Configure AccessNow to launch an application in "Full Screen" mode:
Edit the *config.js* file. Uncomment then modify the following parameters:
autostart: true, // sets the session to auto start
address: "rdphost_address" // sets the address of the RDP host
remoteapplicationmode: true, // sets the session to use application mode
alternate_shell:
"C:\\Program Files\\Ericom Software\\My App.exe", // sets the application path
Other parameters may also be modified as desired.
- 2) Create a shortcut to the Chrome browser (chrome.exe). Edit the shortcut properties to launch chrome.exe in kiosk mode with the URL to AccessNow:
chrome.exe -kiosk <http://accessnowserver/accessnow/start.html>

The shortcut may be placed in the system's *Startup* folder to launch it each time the system is started.

Clipboard Support

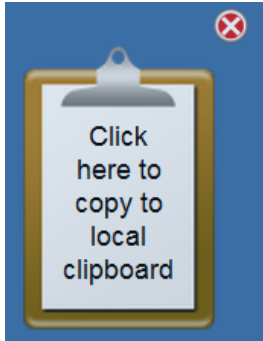
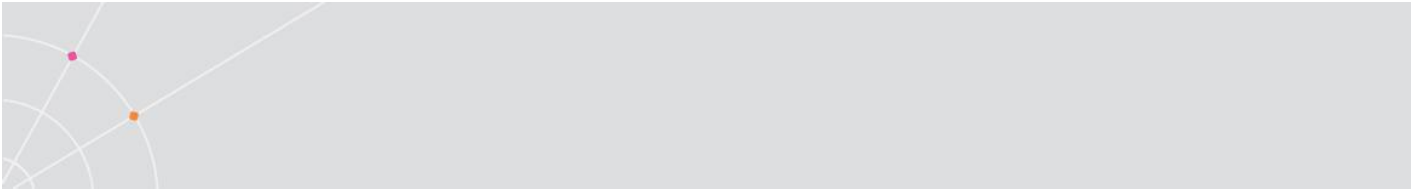
Ericom AccessNow provides the ability to copy and paste text between the local device and the remote RDP session using a built-in clipboard.

Clipboard redirection functionality is limited to only text content in the current version.

Copy Text from Remote to Local

Steps to copy text from the AccessNow remote session to the local desktop:

- 1) In the remote selection perform a copy function (i.e. CTRL-C) on the desired text.
- 2) The following image will be displayed on the right-hand side of the browser window:



- 3) Click on the image – if the browser supports Adobe Flash, the text is immediately copied into the local clipboard. If the browser does not support Flash a dialog will be displayed containing the text so that you can copy it manually.
- 4) Click the red **X** to cancel the Copy operation. The image will disappear automatically after 15 seconds.
- 5) Once the data is copied to the local clipboard, execute a *Paste* operation (i.e. CTRL-V) to paste the text to the local application.

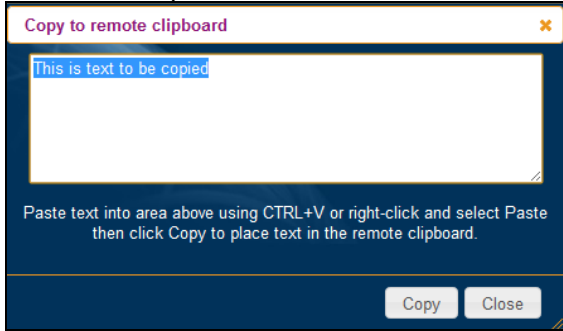
Copy Text from Local to Remote

Steps to copy text from the local desktop to the remote AccessNow session:

- 1) From the local application, perform a copy function on the desired text.
- 2) Click on the Copy icon.



- 3) Paste the copied text into the AccessNow clipboard



- 4) Click the *Copy* button
- 5) Once the data is copied to the remote clipboard, execute a *Paste* operation to paste the text to the remote application in the AccessNow session.

File Transfer

Ericom AccessNow provides the ability to transfer files between the local device and the remote RDP session. When downloading files ensure that the AccessNow service has permission to read the desired files. When uploading files, ensure that the AccessNow service has permission to write files to the desired location.

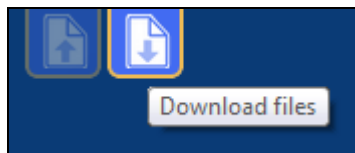
File names with Unicode characters may not be supported.

File upload may not work with Microsoft Internet Explorer 9 (MS IE9) natively. Install Chrome Frame to use files transfer with MS IE9.

Download files from Remote to Local

There are two methods to download files from the remote AccessNow session to the local device.

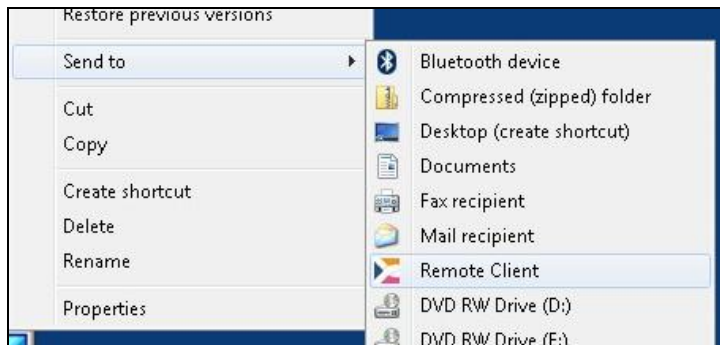
Method 1: Press the *Download* button at the upper right hand corner of the AccessNow session.



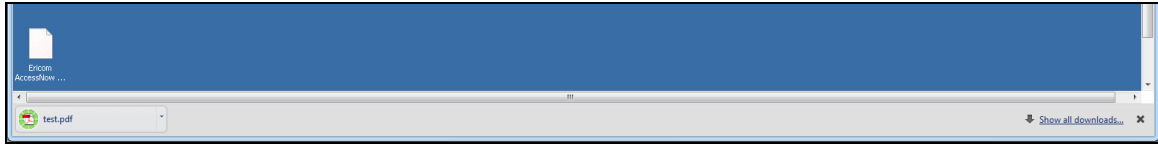
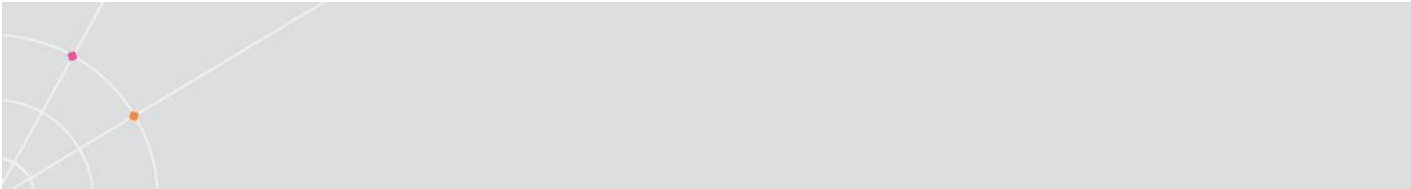
The *Open* dialog will then appear so that the user can select the desired file(s) to download.



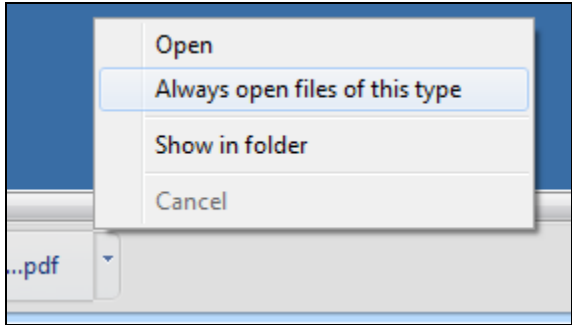
Method 2: Right click on the desired file(s) and select *Send To* and *Remote Client*.



After using either download method - the selected files will be downloaded to the browser's configured *Downloads* folder.



Open the *Downloads* folder to view the file. The method to display the *Downloads* will vary depending on the browser being used. The *Downloads* folder location will also vary based on the path that is configured in the browser.



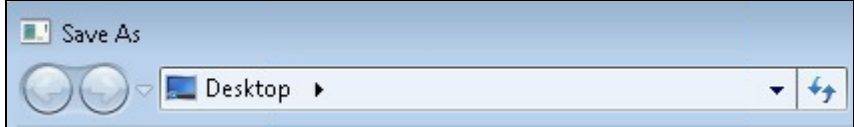
Upload files from Local to Remote

There are two methods to upload files from the local device to the remote AccessNow session.

Method 1: Press the *Upload* button at the upper right hand corner of the AccessNow session.



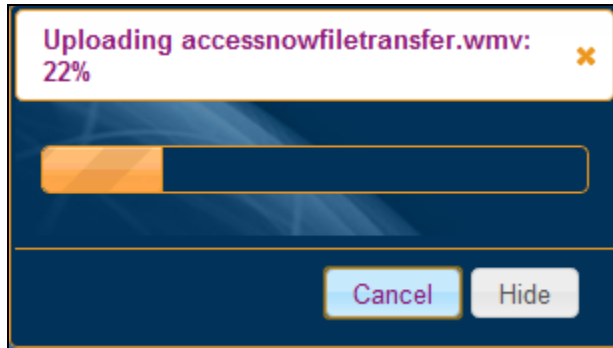
The *Save As* dialog will then appear for the user can select the desired file(s) to upload.



Method 2: Drag the desired file(s) from the local device over the browser where the AccessNow session is running.



After using either upload method - the selected files will be uploaded to the selected folder. A file transfer progress dialog box will appear.



NOTE Apple Safari browser only supports uploading one file at a time, and not multiple files in one operation. This may be resolved in a future version of AccessNow.

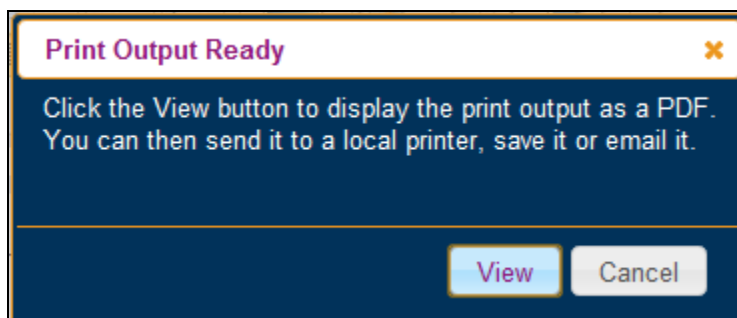
Printing

The Ericom AccessNow printer is added to the remote RDP session upon connection. The AccessNow printer will appear as an available printer while the session is active.

To print to the AccessNow printer, the user simply selects the desired printer when prompted at the Print dialog window.



Once the print operation is executed, AccessNow will send the print output to the local web browser. A ready status dialog will appear when the print output is ready for viewing and printing with the web browser.



When the user presses the *View* button to see the print output, the contents will be displayed in a new browser tab using a one-time use URL. This URL should not be bookmarked for future use.

Sample printout URL:

```
/accessnow/Ericom/FileTransfer/Print/P1/%7B7903DDCA-A91F-4A7E-8985-E6E216551921%7D?address=192.168.35.199&port=8080&secured=true
```

Once the print output is displayed, it can be sent to the device's local printer or saved as a local PDF file using the web browser.

NOTE If the AccessNow printer is not appearing as an available printer verify that the user has permissions to add a printer to the session.

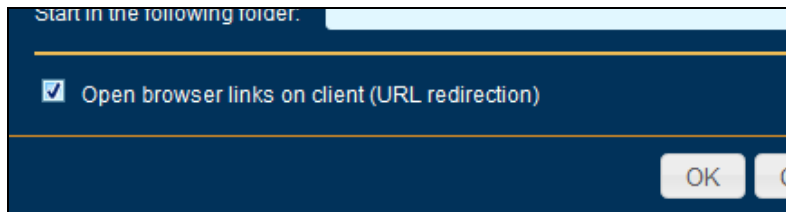
Supported RDP Shortcut Keys

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

URL Redirection

URL Redirection allows URL links that are selected (clicked) on the remote RDP desktop to be opened using the local web browser. This enables redirected websites to use the local resources rather than remote resources to achieve better performance. URL's should only be redirected when the local device has access to the website. If the URL is only viewable from the RDP session, then it should not be redirected.

To enable URL redirection, click on the AccessNow Advanced button and check Open browser links on client:



During a session where URL redirection is enabled, if a user launches a URL, a prompt will be displayed to ask the user where to launch the URL from:



On Client – Opens the URL on the local device in a new browser tab

On Server – Opens the URL in the remote RDP session

Cancel – Cancels the request

Ending a Session

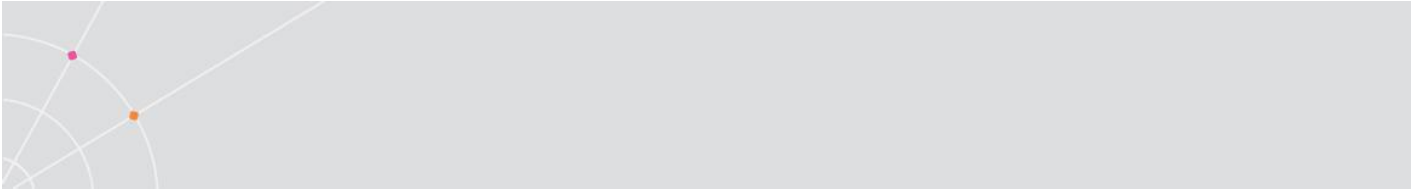
After the user logs out or disconnects, a "Session ended" message appears. The browser returns to the connection dialog after the user clicks *OK*.



No trace of the session will remain on the device once it is ended. For additional security, close the browser tab or window that previously ran the AccessNow session.

Configuring Firefox and Opera browsers

Older versions of Firefox and Opera browsers disable WebSocket by default. It is recommended to upgrade such browsers to newer versions that have WebSockets enabled upon installation. If older versions of these browsers



must be supported, WebSocket must be enabled on these browsers to use Ericom AccessNow.

Enabling WebSocket for Firefox (earlier than version 6)

1. Type **about:config** in the Location bar
2. If a warning is displayed, click button to proceed
3. In the Filter 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

NOTE Opera browser does not support the changing of the cursor type, so a generic browser cursor will always be used
--

Browser Extension Conflicts

Browser extensions and toolbars may inject JavaScript code into web pages. This can adversely impact the behavior of certain web pages. If AccessNow is not working properly - try disabling or uninstalling any active browser extensions or toolbars. Restart the web browser after uninstalling or disabling an extension to ensure that it is no longer active.

4. 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 <i>one</i> finger
Mouse Right-click	Click the Chromebook trackpad with <i>two</i> fingers
Scrolling a document or website	Drag <i>two</i> fingers on the Chromebook trackpad up or down to scroll
Configure Chromebook	Enter into the address field: <i>chrome://settings</i>

Most Chromebook shortcut key combinations (i.e. CTRL+T to open a new tab) are supported during an active AccessNow session. Configured Modifier keys are also supported within the AccessNow session.

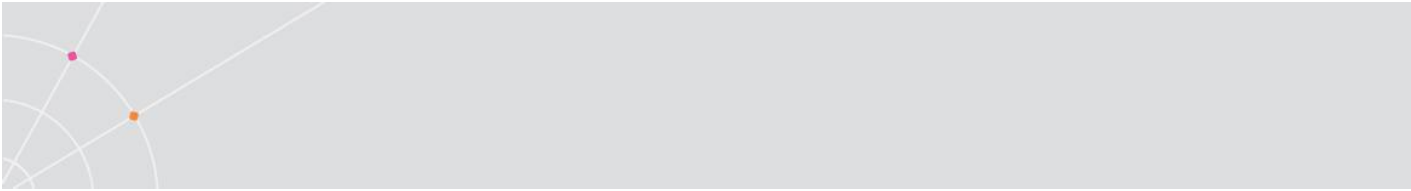
Chromebook Keyboard

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

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

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

Command	Key combination
F1	CTRL+1
F2, ...	CTRL+2, ...



ALT+TAB	ALT+`
ALT+SHIFT+TAB	ALT+SHIFT+`
CTRL+Home	CTRL+ATL+Left
CTRL+End	CTRL+ALT+Right



5. TABLET AND SMARTPHONES

Ericom AccessNow will operate on any tablet or smartphone device if used with an HTML5 browser (i.e. iPad Safari).

The following table provides tips on using AccessNow from a tablet or smartphone device where a physical keyboard and mouse is not available. Functionality will vary across different devices and certain commands may not be available.

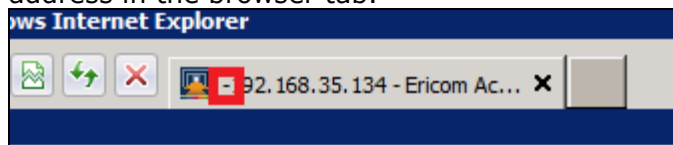
- Single Tap performs a left click.
- Single long Tap performs a right-click.
- Tap + Hold + Drag performs a select then drag/scroll function.
- Double Tap, or tapping once with two fingers, performs double-click.
- Tap with three fingers sends Back command to a remote browser.
- Swipe down with three fingers is Page Up.
- Swipe up with three fingers is Page Down.
- Drag left or right with three fingers performs a left arrow and right arrow respectively.
- Tap the keyboard icon (upper right-hand corner of window) to open/close the virtual keyboard.
- Currently there is no support for clipboard and file transfer on tablets and smartphones.
- Swipe and pinch gestures will apply to the AccessNow session (i.e. zoom in with pinch in).
- (iOS only) When saving an AccessNow icon to the iOS desktop, the shortcut will open the AccessNow session full-screen mode. The browser's toolbar will be hidden and there will be more remote desktop area available.

6. HTTPS MODE

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

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

- 1) Install the AccessNow Server on the desired RDP Hosts.
- 2) Install the Ericom Secure Gateway (this does not necessarily have to be on the RDP Host or AccessNow Server). The Ericom Secure Gateway must be installed on a server that is accessible by the target end-user group(s).
- 3) To connect to the AccessNow server using HTTPS - enter the AccessNow URL of the *Secure Gateway* (the Secure Gateway includes the AccessNow web component) <https://<securegatewayaddress>/accessnow/start.html>
- 4) Enter the parameters for the target AccessNow Server in the start.html page.
- 5) Upon connection, if HTTPS mode is active a '-' symbol will prefix the address in the browser tab.



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



7. ADVANCED CONFIGURATION

Ericom AccessNow provides flexible ways to set predefined values and accept custom values that are passed to it. These values can either be displayed in the AccessNow start page or trigger an automatic connection without allowing the user to change any settings (for an example of this, visit Ericom AccessNow online demo at <http://demo.ericomaccessnow.com>).

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

Static Configuration of *Config.js*

An administrator can modify configuration settings for AccessNow by editing the **config.js** file that is installed as part of the AccessNow web component. 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:

name: value,

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

Refer to the *Settings Table* for a description of each setting.

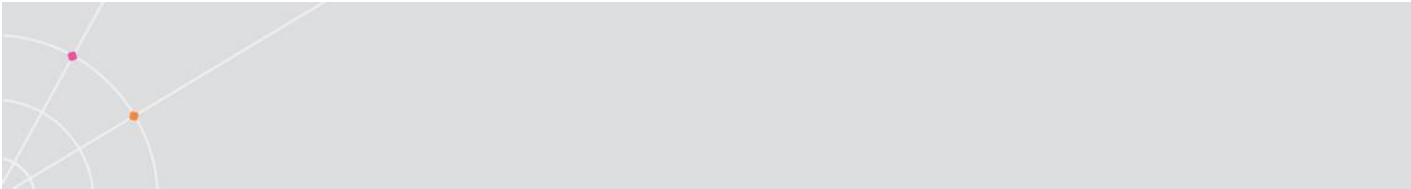
NOTE Backup the original *config.js* file before saving any changes. This will ensure easy rollback to the original configuration.

Passing URL Query Strings

AccessNow supports the ability to pass custom settings as parameters in the URL. For example, the following URL will instruct AccessNow to just launch the Notepad application from the RDP host, rather than display the entire remote desktop:

http://app.ericomaccessnow.com?remoteapplicationmode=true&alternate_shell=Notepad.exe

To start a URL parameter string add the '?' character to the end of the URL.



Separate each parameter using the '&' character.

If a value contains special characters that cannot be placed in a URL, such as the space key, these character must be represented using an escape string. For example, the space character is encoded as %20.

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
remoteapplicationmode=	(true, false) Launches just the specified application
alternate_shell=	(string) Path the application when using application mode (i.e. Notepad.exe)

NOTE Passing parameters in the URL is very simple and easy to use, but is inappropriate for passing sensitive data such as user credentials. For secure transmission of AccessNow parameter values, use browser cookies.

Define Configuration Groups

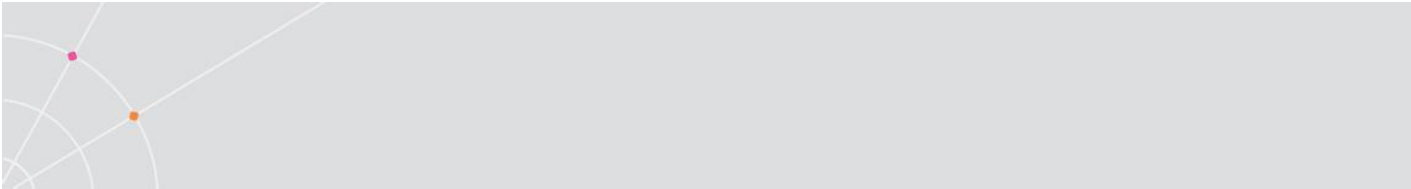
All users share the configuration settings defined in the config.js configuration files. It is possible to specify special settings that will override the general settings for certain groups of users. Multiple configuration groups can be defined in the configuration file.

For example, if the *Marketing* group will have clipboard redirection disabled. Change config.js as follows:

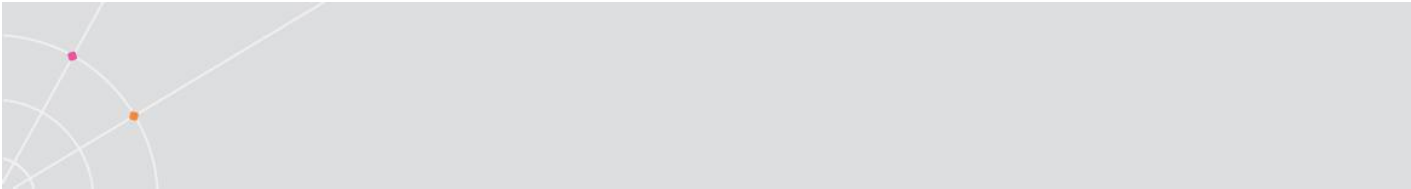
```
var defaults = {  
  ...  
  "Marketing": {  
    clipboardSupport: false  
  }  
};
```

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

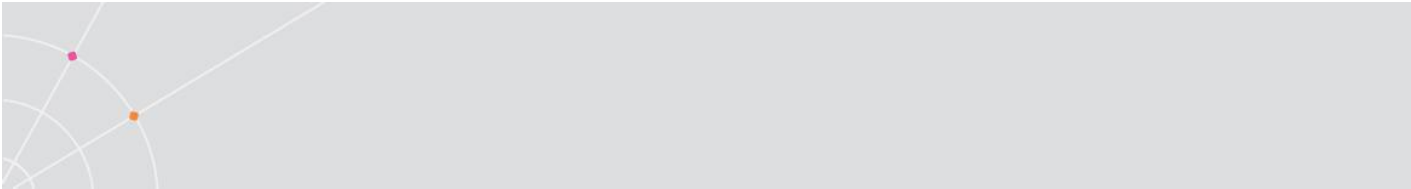
<http://www.accessnow.com/accessnow/start.html?settings=Marketing>



overrideSaved	false (default), settings that the user changes are preserved between sessions and override values set in config.js. Change to true for config.js to override preserved settings.
autostart	Set to true to force the AccessNow sessions to connect automatically without allowing the user to specify settings.
Hidden	<p>A comma- or space-separated list of field names as they appear in config.js. For example "username,password,domain". The listed fields will be hidden so that the user will not be able to modify them.</p> <p>To hide a button, such as the Advanced button, prefix the button text with the word show. For example, "showAdvanced,showAbout" <i>hides</i> both the Advanced and About buttons.</p>
settings (URL parameter only)	Name of a Configuration Group to be used
wsport	<p>The default WebSocket port that will be used by the client. The value specified in the file (8080 by default) will be used for both encrypted and unencrypted WebSocket communication. The user can override this value by explicitly specifying a port address in the client UI.</p> <p>For backward compatibility with older versions of AccessNow server, this behavior can be modified. If singlePort is set to false then the port value specified is only for encrypted communication. The value specified in the file plus one (8081 by default) will be used for unencrypted WebSocket communication.</p>
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.
specialkeys	Enables support for special RDP key combination commands, such as CTRL+ALT+END which starts the Windows NT Security dialog box (similar to local CTRL+ALT+DEL). See http://support.microsoft.com/kb/186624 for the list of key combinations.
chromeKeys	true (default) support special ChromeOS keys combinations
showDownload	true displays a link in the connection dialog to download the AccessNow Server installer.
clipboardSupport	true (default) enables clipboard functionality; false disables it
clipboardTimeoutSeconds	The delay duration before the clipboard image automatically fades out
clipboardUseFlash	true (default) uses Flash when available for one-click copy into local clipboard
clipboardKey	Key to open clipboard paste dialog, set to false to disable
console	false (default) set true to enable RDP console mode
settingsURL	URL of the connection settings file
endURL	URL to open to after the AccessNow session has ended (# value closes window). If there is a prefix with the symbol ^ then this sets the value of window.location instead of top.location. This is useful when the AccessNow session is embedded in a frame. For example "^http://www.ericom.com"
address	address of AccessNow server
full_address	address of RDP host
username	Username to pass into the AccessNow session
password	Password to pass into the AccessNow session



	(entered as clear text in config.js file)
domain	Domain to pass into the AccessNow session
remember	false (default) determines whether the user's password will be saved in the AccessNow page for future use. Set to true to enable password saving (not recommended for kiosk usage).
encryption	false determines if encryption will be enabled from the AccessNow client to the server
blaze_acceleration	true determines if RDP acceleration will be used
blaze_image_quality	Sets the quality level using a numeric For example: 40 (fair quality), 75, 95 (best)
resolution	Sets the resolution size of the AccessNow session. The value set must be a valid option under the AccessNow <i>screen resolution</i> setting For example: "1024,768" "
use_gateway	false (default), set to true to use an Ericom Secure Gateway for remote access
gateway_address	Defines the address and port of the Ericom Secure Gateway For example: <i>secure.acme.com:4343</i>
remoteapplicationmode	false (default), set to true to use application-only mode to launch specific applications instead of a full desktop session.
alternate_shell	Defines the path to an application that will be launched instead of a full desktop session. When using a backslash, it must be prefixed with another backslash. When using double quotes as part of a string, the entire string must be denoted using single quotes (and vice versa). Here is an example of a path using backslashes and double quotes: "C:\\Program Files\\notepad.exe" For more information on JavaScript language string syntax rules, read: http://en.wikipedia.org/wiki/JavaScript_syntax

	#String
shell_working_directory	Sets the working directory for the application defined in the <i>alternate_shell</i> parameter.
useScancodes	false (default), set to true when using certain applications that send characters as scancodes (i.e. VMware vSphere Client, Ericom Blaze Client, any application where you may have issues typing text).
leaveMessage	The message displayed to the user after he/she navigates away from an active session

These settings only take effect after the user starts a new session.

NOTE In some cases the local browser must be closed and reopened before changes take effect.

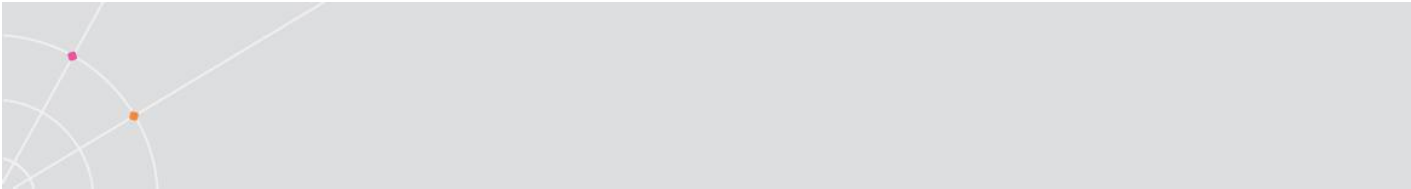
Sample HTML - Passing Cookies into AccessNow

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<script>
<!--
function createCookie() {
    var address = document.forms['cookieform'].address.value;
    var fulladdress = document.forms['cookieform'].fulladdress.value;
    var username = document.forms['cookieform'].username.value;
    var password = document.forms['cookieform'].password.value;
    var domain = document.forms['cookieform'].domain.value;
    document.cookie = "EAN_autostart=true; expires=0; path=/";
    document.cookie = "EAN_address="+address+"; expires=0; path=/";
    document.cookie = "EAN_full_address="+fulladdress+"; expires=0; path=/";
    document.cookie = "EAN_username="+username+"; expires=0; path=/";
    document.cookie = "EAN_password="+password+"; expires=0; path=/";
    document.cookie = "EAN_domain="+domain+"; expires=0; path=/";
}
function testCookie() {
    document.cookie = "EAN_autostart=true; expires=0; path=/";
    document.cookie = "EAN_address=Rdpdemo.ericom.com; expires=0; path=/";
```

```

document.cookie = "EAN_full_address=Rdpdemo.ericom.com; expires=0; path="/";
document.cookie = "EAN_username=demo; expires=0; path="/";
document.cookie = "EAN_password=demo; expires=0; path="/";
//document.cookie = "EAN_domain=; expires=0; path="/";
}
function readCookie(name) {
    var nameEQ = name + "=";
    var ca = document.cookie.split(';');
    for(var i=0;i < ca.length;i++) {
        var c = ca[i];
        while (c.charAt(0)==' ') c = c.substring(1,c.length);
        if (c.indexOf(nameEQ) == 0) {
            alert( c.substring(nameEQ.length,c.length));
        }
    }
}
// -->
</script>
</head>
<body>
<form name="cookieform" action="#"><p>
address: <input name="address"><br/>
RDP Host: <input name="fulladdress"><br/>
Username: <input name="username"><br/>
Password: <input name="password"><br/>
Domain: <input name="domain"><br/>
</p></form>
<a href="javascript:createCookie()">Set Cookie</a><br/>
<br/>
-----<br/>
<a href="javascript:testCookie()">Test Data</a><br/>
<br/>
<!--
-----<br/>
<a href="javascript:readCookie('EAN_address')">Read address</a><br/>
<br/>
<a href="javascript:readCookie('EAN_full_address')">Read full address</a><br/>
<br/>

```



```
<a href="javascript:readCookie('EAN_autostart')">Read autostart</a><br/>
<br/>
<a href="javascript:readCookie('EAN_username')">Read user</a><br/>
<br/>
<a href="javascript:readCookie('EAN_password')">Read pass</a><br/>
<br/>
<a href="javascript:readCookie('EAN_domain')">Read domain</a><br/>
<br/>
-->
-----<br/>
<br/>
<a href="/accessnow/start.html">Launch</a>
</body>
</html>
```

8. ACCESSNOW SERVER FOR LINUX

Pre-requisites

xRDP must be installed, configured, and operational on the Linux RDP host. Use the Ericom Blaze Client (in non-accelerated mode) to verify connectivity to the host with xRDP.

Ericom AccessNow Server for Linux only supports IPv4 addresses.

SSL connections can only be established from Google Chrome and Chromium based browsers

Installation

Two installers are available:

- Rpm version for most Linux distributions such as Red Hat / Fedora / SUSE.
 - Deb version for Debian based Linux distributions such as Ubuntu.
- 1) Download the installer to the Linux desktop where AccessNow Server will be installed.
 - 2) To install the RPM package run: `rpm -i AccessNowServer_1.3-0_i386.rpm`
 - 3) To install the DEB package do one of the following:
 - a. Double click on the installation file. Use the *Package Installer* to install the application.
 - b. Run the command: `dpkg -i AccessNowServer_1.3-0_i386.deb`
 - 4) Once the installation is completed a folder named *Ericom-AccessNow-Server* will be created under the */opt* folder. The executable file *AccessNowServer* is located here.
 - 5) To install AccessNow as a service, run the command:
`./AccessNowServer -install`
 - 6) To run AccessNow as an executable, run the command:
`./AccessNowServer -exec`
 - 7) Once AccessNow is running, it will listen on three ports:
 - a. 8080 (for SSL connections)
 - b. 8081 and 8082 (for non-SSL connections)

Usage

- 1) The AccessNow web client page must have the scan codes setting enabled. Open the *Config.js* file and change the setting *useScancodes*: **true**
- 2) Using an HTML5 compatible web browser, navigate to the AccessNow client URL and enter the parameters to connect to the Linux desktop running Ericom AccessNow Server.
- 3) For SSL enabled connections, the port does not have to be specified.
- 4) For non-SSL enabled connections, the port must be specified as part of the address. For example: 192.168.1.1:8081



The screenshot displays the Ericom AccessNow client interface. At the top, the logo "Ericom® AccessNow™" is visible. Below it, a section titled "Connection Details" contains several input fields and checkboxes. The "Ericom AccessNow Server:" field contains the text "192.168.1.:8081", with the port number "8081" highlighted by a red box. The "User name:" field contains "administrator". The "Password:" field contains "password on host". The "Domain:" field contains "domain on host". At the bottom of the form, there are two checkboxes: "Enable SSL encryption for remote session" (which is unchecked and highlighted by a red box) and "RDP Compression and Acceleration" (which is checked).

- 5) Once the parameters are entered into the client page, click *Connect* to start the AccessNow session.

9. JUNIPER SSL VPN CONFIGURATION

Ericom AccessNow is compatible with most SSL VPN's. It has been tested with Juniper's SA SSL VPN's and the configuration is documented in this section. Configuration with other third-party SSL VPN appliances will be similar to the procedures described here (difference are mostly in terminology).

Adding an AccessNow connection to Juniper

AccessNow links are published in the Juniper's web interface as *web* applications. To publish a new AccessNow connection, go to the Juniper Admin page and do the following:

- 1) Go to Resource Profiles | Web | *New Web Application Resource Profile*

The screenshot shows the 'New Web Application Resource Profile' configuration page. The 'Type' is set to 'Custom'. The 'Name' is 'My Server and AccessNow'. The 'Base URL' is 'http://myserver.test.local/accessnow/start.htm'. The 'Autopolicies' section is expanded to show 'Autopolicy: Web Access Control'. Below this, there is a table with columns for 'Resource', 'Action', and 'Add'. The table contains one entry: 'http://myserver.test.local:80/accessnow/*' with 'Allow' action.

Resource	Action	Add
http://myserver.test.local:80/accessnow/*	Allow	

- 2) Enter the AccessNow URL in the *Base URL* field. Click Save
- 3) Assign all desired user groups in the *Roles* screen.
- 4) Enter the desired label for the connection in the *Bookmarks* tab

The screenshot shows the 'My Server and AccessNow' configuration page with the 'Bookmarks' tab selected. A message states: 'The bookmark below has been automatically created and added to the selected roles for this profile. Add can be created as part of this profile by selecting "New bookmark". If you don't want all roles to receive delete it below, or modify the bookmark's list of roles. To modify the order in which bookmarks appear to the Roles page.' Below the message are buttons for 'New Bookmark...', 'Duplicate', and 'Delete...'. A table shows the bookmark details:

Bookmark	Used by role(s)
My Server and AccessNow http://myserver.test.local/accessnow/start.html	All selected roles

Web Proxy (no download required)

To use Juniper to access applications and desktops on an RDP host without having to download any client components - use Ericom AccessNow in HTTPS Mode (see HTTPS Mode chapter in this guide). This configuration allows devices that do not accept client downloads (such as Google Chromebooks and kiosk stations) to securely access RDP resources using a Juniper SSL VPN. Follow these instructions to use Ericom AccessNow through the web proxy:

- 1) In the Juniper Administration console go to *Users | Resource Profiles | Web*
- 2) Click on *New Profile*
- 3) Enter the *Name* of the AccessNow connection that the users should see
- 4) Enter the Gateway's AccessNow URL address as the *Base URL*

Web Application Resource Profiles >

New Web Application Resource Profile

Type: * Custom

Name: * AccessNow Connection to RDP Host

Description:

Base URL: * https://GWaddress.com/accessnow/start.html

- 5) Go to *Autopolicy: Web Access Control*
- 6) Edit the automatically entered address and delete the subfolder "accessnow".
Instead of <https://GWaddress.com:443/accessnow/> the correct resource is <https://GWaddress.com:443/>
- 7) Click *Save and Continue*
- 8) At the *Roles* dialog add all roles that should have access to the AccessNow link and click *Save Changes*
- 9) When the user logs into Juniper - the AccessNow link will be displayed under the Web bookmarks section (i.e. AccessNow Connection to RDP Host). Simply click on the link to connect to an application or desktop published with AccessNow.

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

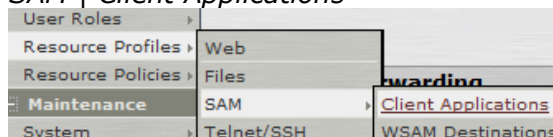
Network Connect

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

JSAM and WSAM

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

- 1) Publish a JSAM Client Application Profile by going to *Resource Profiles | SAM | Client Applications*



- 2) Click *New Profile* and enter the parameters:
 - a. Type: *JSAM*
 - b. Application: *Custom*
 - c. Name: <enter desired label here>
 - d. Servers Name: <enter address of AccessNow Server>
 - e. Server Port: <enter AccessNow port # (default is 8080)>
 - f. Client Loopback IP: Juniper's aliased address for the AccessNow Server (Important note: this address must be entered as the AccessNow address for Juniper users).
 - g. Client Port: Juniper's aliased port for the AccessNow Server (Important note: this port must be entered as the AccessNow port for Juniper users). The default port 8080 may be used here if it does not create a port conflict.
 - h. Click *Save and Continue*
 - i. Select the *Roles* that will have access to this JSAM application
 - j. Click *Save Changes* and now this application is ready for use.

Client Application Resource Profiles >
AccessNow Connection

Resource Roles

Type: * JSAM
 Application: * Custom
 Name: * AccessNow Connection
 Description:

JSAM Port Forwarding

JSAM secures traffic destined for the following server(s). It listens for this traffic on a local loopback address, which you can also specify (valid loopback addresses are 127.0.0.1 or 127.0.10.x and higher). JSAM will automatically choose and configure the client loopback addresses if you leave them blank. If you leave the Client Port blank, JSAM will use the Server Port for that server.

Servers:

Server Name *	Server Port *	Client Loopback IP	Client Port
myserver.test.local	8080	127.0.10.99	8080

Create an access control policy allowing SAM access to these servers
 Allow JSAM to dynamically select an available port if the specified client port is in use

Auto-starting JSAM or WSAM upon login

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



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

- 1) Click on User Roles | <select desired Role> | *General*
- 2) Verify that the *Secure Application Manager* is checked and click on Options
- 3) Check the *Auto-launch Secure Access Manager option*:

General Web Files SAM Telnet/SSH Terminal Services Meetings Network Connect

Applications Options

Windows SAM Java SAM

Secure Application Manager options

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

Auto-allow application servers
 Use auto-allow to automatically add WSAM allowed servers and JSAM application servers to the [SAM_access.co](#) does not apply to any user-configured applications.

Windows SAM Options

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

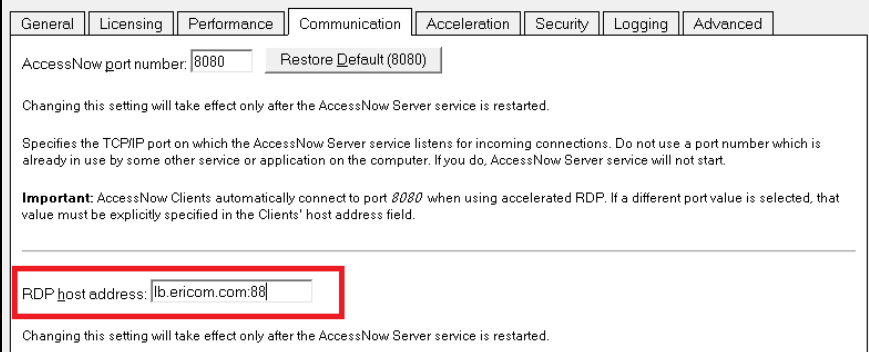
10. LOAD BALANCERS

Larger application and desktop hosted deployments will require multiple RDP host servers. The Ericom PowerTerm WebConnect connection broker may be used to handle larger loads and evenly distribute users across a large base of Terminal Servers. Third-party Terminal Server aware load balancers (i.e. Microsoft Windows 2008 R2 Remote Desktop Connection Broker or 2X Load Balancer) may also be used.

Configuration

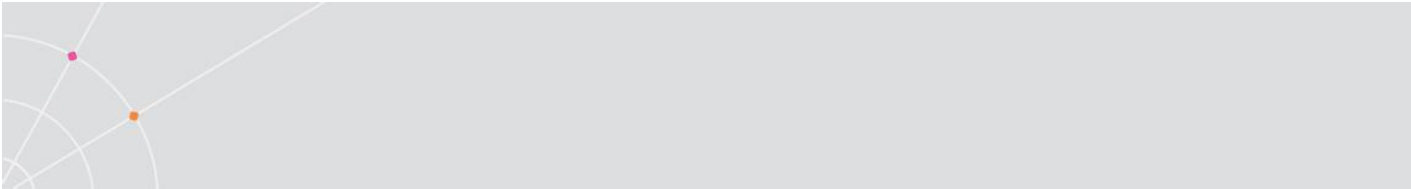
When using a software based load balancer (i.e., Remote Desktop Connection Broker) that runs on a Windows operating system (2003 and higher), the Ericom AccessNow Server may be installed on the same machine. For all others load balancers, install Ericom AccessNow on a separate machine.

Ericom AccessNow Server must be configured to connect to the load balancer's address and port. This is performed by using the Ericom AccessNow Server Configuration Tool. Go to *Communication* and enter the load balancer's *address:port#* in the *RDP host address* field. When AccessNow Server is installed on the same Windows machine as the load balancer use *localhost:port#*.

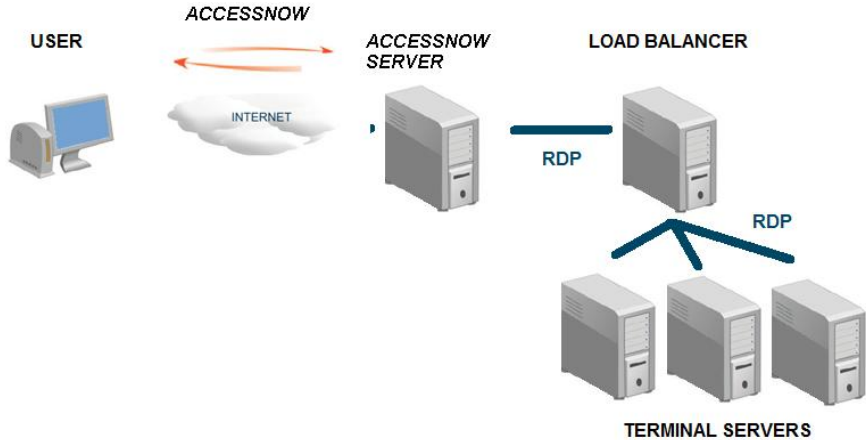


The screenshot shows the 'Communication' tab of the Ericom AccessNow Server Configuration Tool. The 'AccessNow port number' is set to 8080. Below it, there is a note: 'Changing this setting will take effect only after the AccessNow Server service is restarted.' and a description: 'Specifies the TCP/IP port on which the AccessNow Server service listens for incoming connections. Do not use a port number which is already in use by some other service or application on the computer. If you do, AccessNow Server service will not start.' An **Important** note states: 'AccessNow Clients automatically connect to port 8080 when using accelerated RDP. If a different port value is selected, that value must be explicitly specified in the Clients' host address field.' The 'RDP host address' field is highlighted with a red box and contains the value 'lb.ericom.com:88'. Below this field, another note states: 'Changing this setting will take effect only after the AccessNow Server service is restarted.'

Configure AccessNow client web page (or config.js file) to connect to the address of the AccessNow Server. The AccessNow Server will then forward the communication to the load balancer. In this environment, the connection between the AccessNow Server, load balancer, and RDP hosts must be in very close proximity, with minimal latency, to ensure good performance.



This diagram illustrates how Ericom AccessNow works with a load balancer:

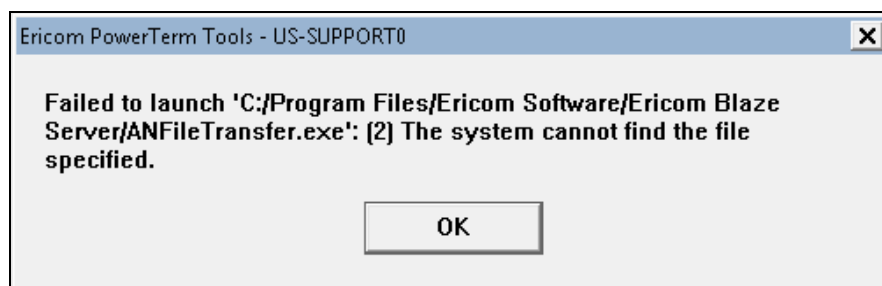


The system running Ericom AccessNow Server must be equipped with enough memory to handle the total number of active users.

11. TECHNICAL SUPPORT

TSAgent Update

Ericom AccessNow incorporates the latest Ericom TSAgent technology. If AccessNow is installed on systems where Ericom Blaze Server and PowerTerm WebConnect TSAgent are also installed – the following error may appear when the end-user performs a file transfer operation.



To resolve this issue, copy two files from the AccessNow Server directory to that of Blaze Server and TSAgent. The two files are:

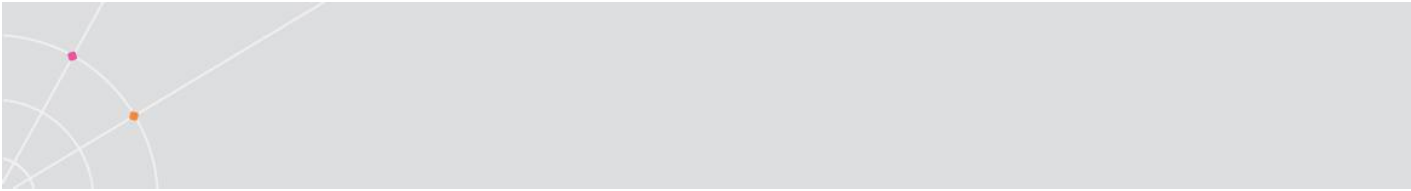
- Pptsagent.exe
- ANFileTransfer.exe

It is advisable to back up the existing pptsagent.exe file(s) before overwriting them.

Requesting Support

To request technical support from Ericom Software, email SUPPORT@ERICOM.COM and provide the following information:

- Which version of Ericom AccessNow are you using (see About)?
- What type of system/operating system are you connecting to (host)? Is it 32 or 64 bit? Is RDP enabled?
- What type of system/operating system are you connecting from (client)? Is it 32 or 64 bit?
- Is port 8080 enabled on the host (is the firewall configured with an exception)?
- What error messages are being displayed?
- How many people/machines/hosts are having this problem (one, all, etc)?



ABOUT ERICOM

Ericom Software is a leading global provider of Application Access, Virtualization and RDP Acceleration Solutions. Since 1993, Ericom has been helping users access enterprise mission-critical applications running on a broad range of Microsoft Windows Terminal Servers, Virtual Desktops, legacy hosts and other systems. Ericom has offices in the United States, United Kingdom and EMEA. 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 about Ericom and its products, please visit <http://www.ericom.com>

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

Ericom Software Inc.
231 Herbert Avenue, Bldg. #4
Closter, NJ 07624 USA
Tel +1 (201) 767 2210
Fax +1 (201) 767 2205
Toll-free 1 (888) 769 7876
Email info@ericom.com

Western Europe

Ericom Software (UK) Ltd.
11a Victoria Square
Droitwich, Worcestershire
WR9 8DE United Kingdom
Tel +44 (0) 845 644 3597
Fax +44 (0) 845 644 3598
Email info@ericom.co.uk

International

Ericom Software Ltd.
8 Hamarpeh Street
Har Hotzvim Technology Park
Jerusalem 91450 Israel
Tel +972 (2) 591 1700
Fax +972 (2) 571 4737
Email info@ericom.com