Ericom® AccessNow for VMware View™

HTML5 Access for VMware View Desktops

Administrator's Manual

Version 3.3

Legal Notice

This manual is subject to the following conditions and restrictions:

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

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

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.

AN_VVAdminMan20140514

Table of Contents

ABOUT THIS DOCUMENT

This manual provides instructions on how to install and use *Ericom AccessNow for VMware View* to access virtual desktops managed by the VMware View connection broker, from within HTML5 compatible web browsers. Follow the instructions in this manual and start enjoying the benefits of Ericom AccessNow for VMware View within minutes!

This manual includes the following information:

- Overview of Ericom AccessNow for VMware View Client
- 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
- Basic 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.
- 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.
- AJAX – Asynchronous JavaScript And XML is a mechanism that enables web applications to communicate with server using XML over HTTP/HTTPS.

1. OVERVIEW

Ericom AccessNow for VMware View provides end-users with remote access to virtual desktops managed by the VMware View connection broker from any HTML5 compatible web browser. Any browser that supports HTML5 WebSocket and Canvas can be used to launch the client, and enables users to view virtual desktops from within the browser window itself. This provides the following benefits:

- Access virtual desktops 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 ChromeOS
- Same look-and-feel and functionality on any platform that has a HTML5 compatible browser
- No need to perform software updates on end-point devices
- Remote virtual desktop can be seamlessly integrated with other web-based applications and portals
- Supports RSA SecurID two-factor authentication (via VMware View)

Architecture

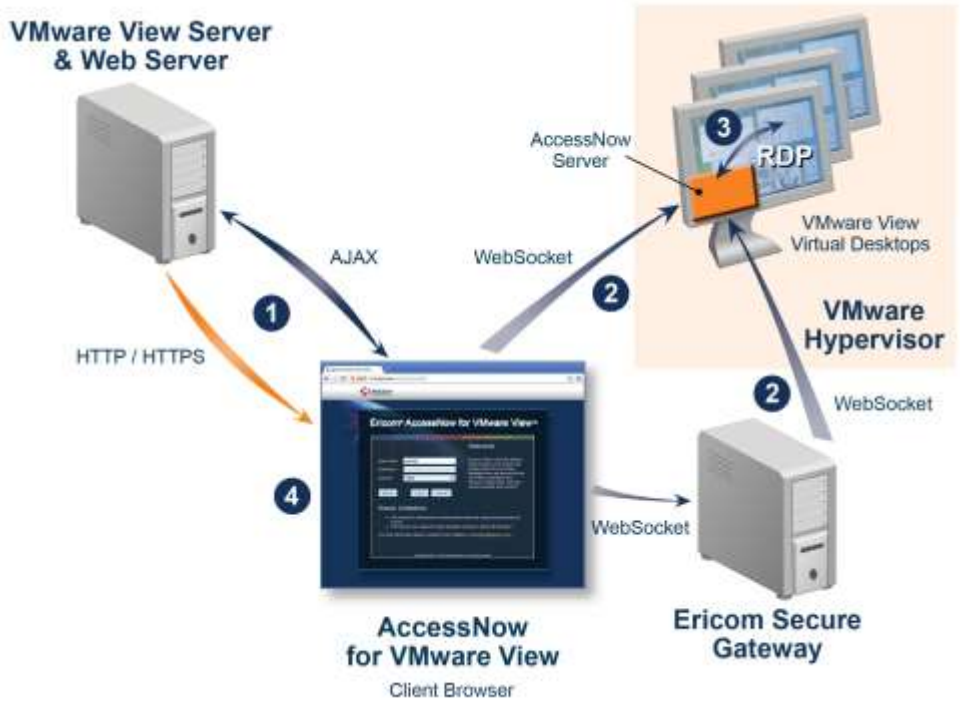
Ericom AccessNow for VMware View is comprised of three installable components:

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

b. Access 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 the components of the Ericom AccessNow for VMware View and their interaction:



1. *The user initiates the process by directing the browser to the **view.html** page that is hosted on the web server, which is also the VMware View server. This page is displayed in the browser using HTTP/HTTPS. The browser then communicates with the VMware View server using AJAX (XML over HTTP/HTTPS).*
2. *After receiving the connection information for the selected virtual desktop, the browser opens a WebSocket connection to the Ericom Access Server Service running on the virtual desktop itself.*
    a. *If the optional Ericom Secure Gateway is used, the AccessNow browser session will connect through it using secure WebSockets.*
3. *The Ericom Access Server Service translates the WebSocket to and from RDP, thus establishing a connection from the browser to the virtual desktop itself.*
4. *The browser then displays the content of the virtual desktop.*

RDP Compression and Acceleration

The Ericom AccessNow for VMware View 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 client for rendering. The level of compression is dependent on the acceleration/quality level selected by the user.

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. 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. ERICOM ACCESS SERVER

Ericom Access Server provides AccessNow HTML5 access and Blaze RDP compression and acceleration features. All features are enabled during the trial period, and each feature can be unlocked using an activation key after the trial period ends. The host may be any Windows system that has RDP access enabled, such as a Windows Terminal Server or a Windows workstation. The Access Server uses a customizable port – by default this is port number *8080*. Port *3399* is also enabled for backward compatibility with installations using older versions of Blaze.

NOTE	Ericom Access Server 3.x is not be backward compatible with previous versions Blaze: 2.x and earlier. If you are using an earlier version of Blaze, please upgrade all Blaze client and server components to the same version.

The Access Server may be installed on the RDP host or on a dedicated system to serve as a proxy. It is recommended to install the Access Server on the RDP host itself. Some features such as AccessNow file transfer may only available when the Access Server is installed on the RDP host itself. The Access Server has a small footprint and will have minimal impact on the RDP host's performance and scalability.

Ericom Access Server Requirements

- Windows operating system
- Incoming RDP connections enabled on the Host OS (e.g. Terminal Server)
- 80 MB of free Hard-Disk space
- MMX and SSE2 capable CPU
- Firewalls are configured for Access Server traffic 8080 (or 3399) port

The Access Server should be installed on *each* server / host that requires accelerated or HTML5 access. Terminal Servers only require one installation to accelerate all user sessions. Each workstation / desktop (physical or virtual) requires an installation. It is possible to include Access Server as part an image that will be deployed using Microsoft® Sysprep or Symantec® Ghost.

Bind Service to All Network Interfaces

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

Host Firewall Configuration

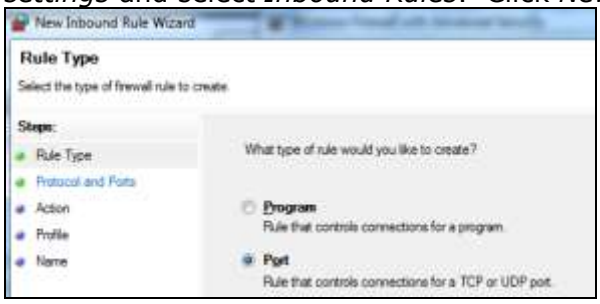
Make sure to allow traffic communication from the end-user device to the Ericom Access Server host. Firewall configuration may be necessary.

On Windows operating systems, ensure that the Windows Firewall is configured to allow traffic to the Access Server port (by default 8080). This port value may be changed using the Access Server Configuration utility.

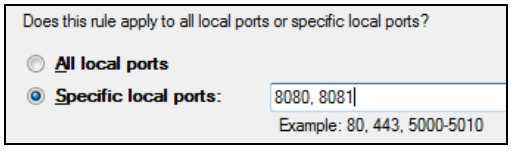
NOTE	Disable the Windows Firewall temporarily to troubleshoot any connectivity issues. If the connection is only successful with the firewall disabled, then there may be a rule that is blocking the Access Server port.

To add a rule to allow the Ericom port, perform the following (instructions based on Windows 7/2008 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*



- 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*.

Port Forwarding Configuration

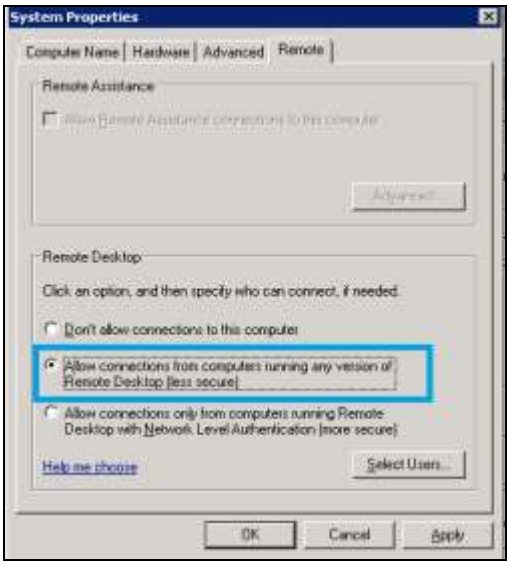
When configuring a firewall for port forwarding to an RDP host that has Access Server installed on it, make sure that it is directed to the Access Server port (default: 8080). Do not forward to port 3389 (default RDP port).

If a custom port is being used, configure the firewall to forward to the port value configured under the Communication page.

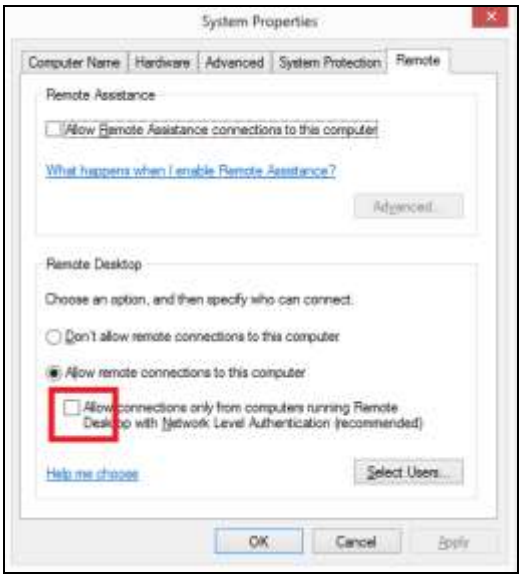
Disable NLA on RDP Host

Access Server currently does not support NLA. Please disable NLA on RDP hosts running Access Server, otherwise AccessNow and Blaze connections will fail (a message showing "initializing remote session" will appear and then the session will be disconnected immediately).

On Windows 7 and 2008 or higher - in the Windows System | Remote | Properties tab, select "Allow connections from computers running any version of Remote Desktop":

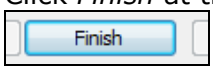


On Windows 8 and 2012 or higher - in the Windows *System* | *Remote* | *Properties* tab, make sure that the NLA checkbox is unchecked:

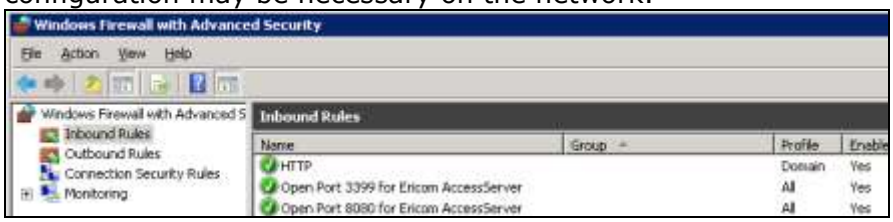


Installing Ericom Access Server

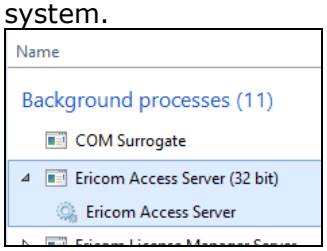
- Run *EricomAccessServer.msi* and follow the instructions of the installation wizard.
- Review and accept the License Agreement.
- Click *Install* (if prompted, accept the security elevation request). Click *Finish* at the last screen to complete the installation



- Verify that the Access Server port is available and accessible to the host system. Access Server will automatically add the necessary rules to Windows firewall, however additional firewall configuration may be necessary on the network.



- Once installed, the Access Server will run as a service on the system.



  - The service is configured to run automatically on system startup.
  - If the service is stopped or is unable to listen on its default ports (8080), the client will not be able to connect to that host. Verify that there are no other applications using the same port.
  - On Windows XP, a system restart (reboot) may be required after installing the Ericom Access Server.

Access Server can be automatically and silently installed using a management application such as Microsoft System Center.

- To perform a silent install run: msiexec /I "**EricomAccessServer.msi**" /q
- **EricomAccessServer.msi** represents a valid path to the .msi file
- On Windows Vista, 7, 8, Windows Server 2008, and 2012 this command may need to be performed with elevated Administrator credentials.
- Run MSIEXEC without any parameters to view the help dialog.

NOTE	Access Server may not be compatible with certain systems where the hostname contains non-English characters.

Using Ericom Access Server

To modify Access Server settings: Go to *Start* | *Programs* | *Ericom Software* | *Access Server Configuration.* On systems that do not have a Start menu, the GUI may be launched using the command line:

<drive>:\Program Files (x86)\Ericom Software\Ericom Access Server\ServerConfiguration.hta

NOTE	Access Server is used by **both** the AccessNow HTML5 and Blaze RDP Acceleration products.

Access Server Configuration

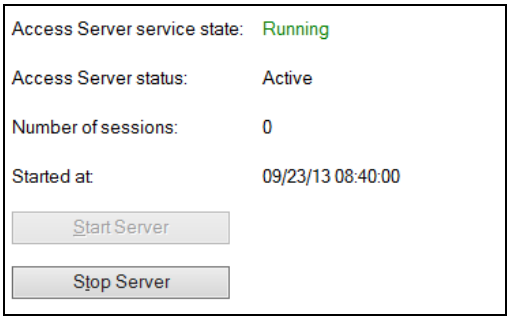
The *Server Configuration* console presents a series of tabs that allow the administrator to configure various settings for the server service. The Configuration console only works on systems with Microsoft Internet Explorer 7 or later (the console will not launch on systems with IE6 installed).

HINT	When installing Access Server on a Terminal Server, it is recommended to hide the Server Configuration application from end users to prevent unexpected changes to the configuration settings.

General

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

STOP	When the Access Server service is restarted, all AccessNow and Blaze sessions on the server will be disconnected.



Licensing Information

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

NOTE	In a production VDI or Terminal Server environment, the licensing server must be **centralized** on a robust system. See the section on Central Server Configuration for additional details.

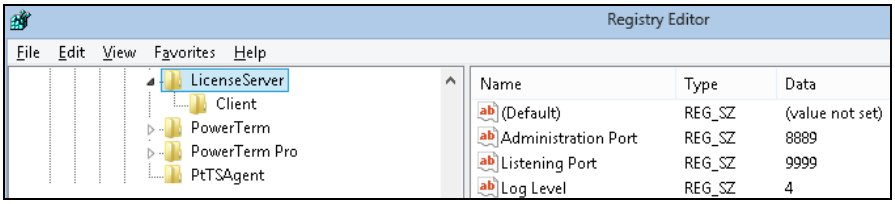
By default, Access Server uses DNS lookup to locate the Licensing Server. The DNS entries used are *ericom-license-server.<domain-name>* or *_ericom-license-server._tcp.<domain-name>*. If the DNS entries do not exist, the Access Server attempts to connect to a Licensing Server that is running on the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

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

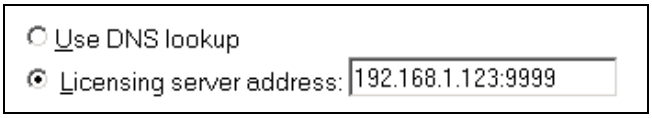
If no valid license is found, Access Server will continue to run if the grace period has not expired. Once the grace period expires, Access Server will not allow user sessions. A "grace period" lasts up to 10 days within a 30 day period.

Changing the License Server Port

The license server communicates over port *8888* by default. If there is another application on the same system already listening on port 8888, the license server port value may be changed in the Registry. Use the Registry Editor and navigate to HKLM | SOFTWARE | (WOW6432Node) | Ericom Software | LicenseServer | *ListeningPort*



In the example above, the port has been changed to 9999. Once the value is set, restart the *Ericom Licensing Server* service. For each Access Server that will be connecting to the central license server on a custom port, the custom port value must be specified after the address with a colon. For example:

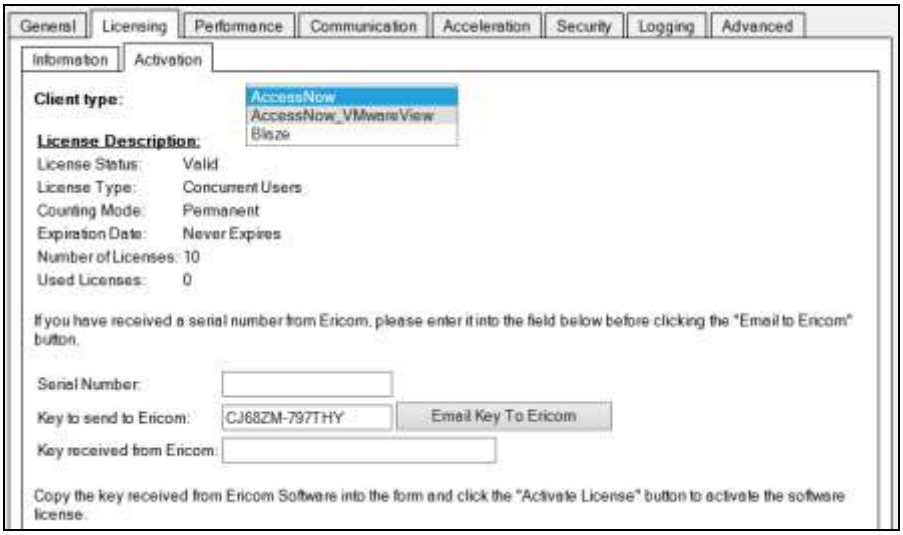


Licensing Activation

Click on: *Licensing* | *Activation* to enter the serial number and activation key into the product's configuration.

To activate an installation from an evaluation, select the desired *Client type* and then send the "*key to send to Ericom*", along with the serial number, to Ericom for processing. An activation key will be returned. Once the activation key is entered, click on the *Activate License* button. The Access Server does not have to be restarted for the license to take effect.

To extend an evaluation, send the "key to send to Ericom" to an Ericom sales representative for processing. A standard two week extension key will be returned once the request is approved.



Performance

This page displays current Server performance statistics.

Communication

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

When using a listening port other than the default (8080), the port number must be explicitly specified in the *Access Server* address or the Blaze Client *Computer* field (e.g., rdpdemo.ericom.com:22).

AccessNow web client: 

Blaze Client: 

The RDP host address is used when the destination system is not the system running Access Server. In this scenario, the Access Server is acting as a *gateway* proxy between the end user and the destination host system. This

type of configuration is not recommended as it may adversely impact AccessNow and Blaze performance.

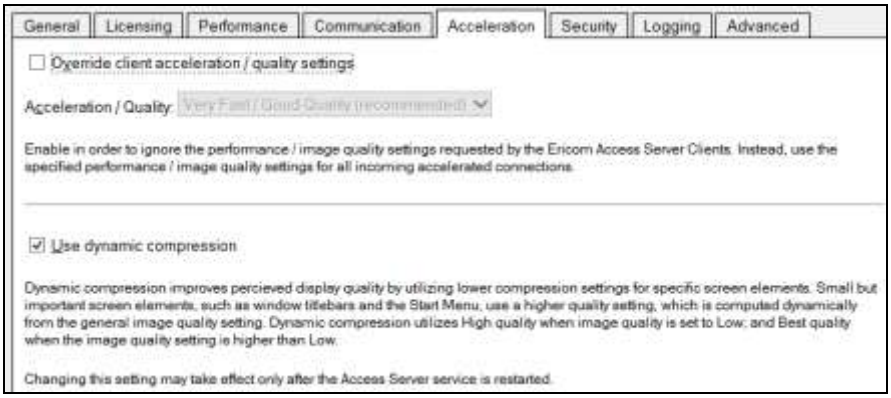
Changes to both settings require a service restart (under General tab).

When running Access 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, and 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 compress them using *High* quality when the Blaze Quality setting is *Low*; and at *Best* quality when the Blaze Quality setting is higher than Low. All other graphical objects are compressed at the chosen 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 Access Server security settings.

Ericom Access provides integrated *128-bit SSL* encryption. For better performance, set the host's RDP Security Encryption level to Low and change the *Encrypt Access Server communication* to *Always*. Using this configuration, Ericom SSL encryption will be used instead of the RDP encryption. See the *Ericom Optimization* chapter in this document for more details.

To use a custom or trusted certificate, enter the thumbprint ID into the *Certificate Thumbprint* field and click the *Apply* button. The certificate's

properties will be displayed in the GUI, represented by the black boxes in the image above. Restart the service to apply the changes.

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

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 Access Server settings that are stored in the system's Registry.

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

Import Settings – imports previously saved Registry settings.

Advanced Configuration – Launches regedit.exe and opens the Access Server registry keys. By default, only settings that are changed from the default value are saved into the Registry.

Extended Session Scripting

This product extends Windows built-in scripting capabilities on the RDP host. This mechanism adds an additional layer of functionality to run certain commands when sessions start or end, and when they are connected or disconnected.

Post-Startup Login script (_login)

Create a file named *_login* with the appropriate extension, for example a script file called _login.vbs or an executable called _login.exe, and place this in a folder named *scripts* under the Access Server installation folder. If this folder does not exist, create it. This script will execute when a new session starts, after the TS/RDS session processes the *Startup* folder.

Pre-Startup Login script (__login)

Similar to _login, __login is executed at session startup, but it is executed before the TS/RDS session processes the *Startup* folder.

Session connection script (_connect)

Create a file named *_connect* with the appropriate extension, and place this in a folder called *scripts* under the Access Server installation folder. If this folder does not exist, create it. This script will execute upon connection into an existing TS/RDS session.

Session disconnection script (_disconnect)

Create a file named *_disconnect* with the appropriate extension, and place this in a folder called *scripts* under the Access Server installation folder. If this folder does not exist, create it. This script will execute upon disconnection from a TS/RDS session.

Sample VB Script to create a new file

```
Set objFileToWrite =
CreateObject("Scripting.FileSystemObject").OpenTextFile
("newfile.txt",2,true)
objFileToWrite.WriteLine("hello world")
objFileToWrite.Close
```

3. LICENSING OVERVIEW

Evaluation (Demo) Period

Each Access Server installation includes a Licensing Server that is installed on the same device. By default, the license server includes an evaluation period of 30 days. During this period, the Licensing Server allows up to 50 Concurrent User licenses. The evaluation period can be extended by contacting an Ericom sales representative.

Licensing Modes

The Ericom License Server service manages licensing for Ericom AccessNow and Blaze. Any connection made with an Ericom Blaze Client or AccessNow HTML5 requires an Ericom license. A single licensing server can manage licensing for multiple Ericom Access Servers.

There are two modes of licensing:

Concurrent User – Ericom licenses are counted based on the number of active users that are currently connected to all the Access Servers utilizing the same Licensing Server. In this licensing mode:

- There is no licensing limit on the number of Ericom sessions that the same user can open concurrently on a single client device. Only one license will be consumed regardless of the number of sessions the user opens on the device.
- The same user opening Ericom sessions concurrently from several devices will consume the same number of licenses as the number of devices used.`
- Several users using the same device (i.e. using Fast User Switching) will take the same number of licenses as the number of users that have active Ericom sessions

Named User – Ericom licenses are counted based on the number of names registered that *have ever* connected to any Access Servers utilizing the same Licensing Server. In this licensing mode:

- A license is allocated for a name when it is first used by any user
- The license is automatically released after a period of 14 days during which the name has not been used for running Blaze Clients

at all. A license allocated to a name cannot be released prior to the end of the 14 day period

- The Access Server must be installed on the RDP host (as the TSagent is also required for this method). If the Access Server is used as a Gateway, then only the Concurrent license will be available.

Central Server Configuration

The Access Server can be configured to use a remote Licensing Server so that a single pool of licenses may be shared among multiple Access Servers.

For example, a 10 user license would be activated once on a central server. All Access Servers on the network would then be directed to use the pool of licenses on the central server. Ericom recommends that in an environment with more than two RDP hosts (Remote Desktop Servers, Terminal Servers, VDI, etc.) that a dedicated server be made available to host the licenses to prevent disruptions and conflicts. Guidelines for the central license server are as follows:

- The central license server must be hosted on a server that is highly available so that it can distribute licenses.
- In a VDI environment, do not install the license server on a cloned desktop or the gold image template. It should be installed on a static machine that does not experience system changes.
- In a TS/RDS environment with two or more servers, avoid installing the license server on the Terminal Server if possible.
- Minimize the amount of reboots and disruptions on the server. Apply updates only during off-peak times.

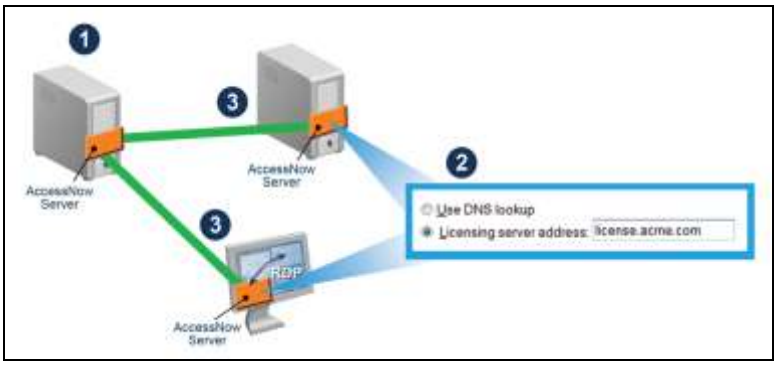
When no valid license is found, Access Server will continue to run if the grace period has not expired. Once the grace period expires, Access Server will not allow user sessions. A "grace period" lasts up to 10 days within a 30 day period. When there is an issue with the license server, it should be rectified before the grace period expires.

Implementation

Step 1: Install Access Server on the desired system and activate it (using the *Licensing* | *Activation* tab). Although Access Server will be running, the main role of this installation is to create a central license server. Enable the incoming port 8888 on the Windows firewall of this system. Verify that this port is available over the network between the central license server and the any Access Servers that will connect to it.

Step 2: Configure all Access Servers to use the central license server address for licensing. There are two methods to configure the address of the central license server, see the next section for details.

Step 3: Once the Access Server service starts, it will connect to the configured central license server to obtain a license when an Ericom AccessNow or Blaze session is established.



There are three methods to use a central license server:

Use DNS Lookup

When using this setting, Access Server will always attempt to find a centralized Licensing Server before using the local one that was installed along with it. If a central license server is found and used, the local one will be ignored. When the Ericom Access Server service starts, it looks for the central licensing server address (IP or DNS name) in the following order.

1) **DNS-SRV** Entry
Access Server will look for the Licensing Server address in a DNS-SRV entry: *_ericom-license-server._tcp.<domain>*
For example, *_ericom-license-server._tcp.ericom.local*

2) **DNS** Entry
If the DNS-SRV record does not exist, Access Server will look for the Licensing Server address in a DNS entry: *ericom-license-server.<domain>*
For example, *ericom-license-server.ericom.local*

3) Localhost
If the DNS entry does not exist, the locally installed Licensing Server will be used (i.e. localhost will be used as the address of the Licensing Server).

Manual Entry

Licensing server address

The administrator may also explicitly specify the license server that will be used at the Licensing page in the Access Server Configuration application.

4. ACCESSNOW WEB CLIENT

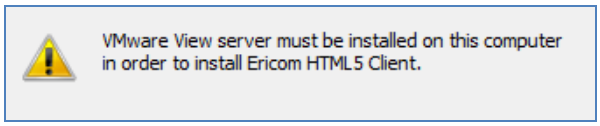
The web component contains the resources that are used by the web browser to display an interface for users to use to connect to their remote application or desktop. These resources include HTML pages, JavaScript and CSS files and graphic images. Review the chapter on *Advanced Configuration* to modify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

Installing the AccessNow for VMware View Web Client Component

The AccessNow web-server component provides the user interface to connect from a HTML5 compatible browser. The web-server component must be installed on the VMware View broker server (where its Apache web server is running).

The web-server component is provided as a MSI installer named **EricomAccessNowforVMwareView.msi or EricomAccessNowforVMwareView64.msi**. Launch the installer on the server running VMware View.

If an attempt is made to install on a machine without VMware View, and error will be displayed.



The installer will place the web-server components to the root folder of the web server on the VMware View server. On 32-bit (x86) Windows the default location will be:
C:\Program Files\VMware\VMware View\Server\broker\webapps\ROOT

This will create a folder called "ericom" under the ROOT folder that contains all the web resources. Ensure that the proper permissions are set such that users may view the files and folders.

5. HTML5 User Access

With Ericom AccessNow for VMware View, users can access virtual desktops from HTML5 compatible web browsers. To start a session users must navigate to *view.html* which is installed in the ericom folder on the web server. For example, if the VMware View server / web server is located at address www.vmwareview.com then users need to launch the URL: https://www.vmwareview.com/ericom/view.html

By default VMware View servers are configured for secure access, which requires HTTPS. If the VMware View server is configured for unsecured access, use HTTP instead.

Ericom AccessNow for VMware View communicates with the VMware View Connection Broker directly using the standard VMware View protocol. The client supports both encrypted and unencrypted communication.

Supported Browsers

Google Chrome 11 and higher, Apple Safari 5 and higher (version 5 requires ESG), Firefox 4 and higher, Microsoft IE 11, 10, and 9 (version 9 requires ESG) and Opera. For Firefox 4/5 and Opera WebSocket support must be enabled in the browser configuration. Firefox 6 and higher 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 significantly reduce its CPU and memory utilization.

Web Page Login

The functionality of the Ericom AccessNow for VMware View interface is similar to the standard VMware View client.

When the user initially navigates to the URL, he or she may be presented with a disclaimer message which must be accepted in order to proceed. This message is sent by the VMware View server.

After clicking OK, a login form will be displayed and the user must provide the credentials for *VMware View*. Only username/password/domain is currently supported for authentication. Press the *Login* button to authenticate the user.

After a successful login, the user will be presented with the list of virtual desktops. Select the desired desktop to configure its parameters.

NOTE The list of virtual desktop displayed to users in the browser is filtered to only display virtual desktops that support RDP access. However, the list is not filtered to display only virtual desktops that contain the server-side Ericom Access Server. If users try to connect to virtual desktops that do not have a server-side component - the connection will fail.

The user can specify connection settings independently for each virtual desktop. These settings are saved between sessions, and can also be hidden from the end users (see Advanced Configuration chapter).

Field	**Description**
SSL encryption for desktop session	When checked, the client utilizes encrypted WebSocket communication to the virtual desktop.
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	Controls the degree of acceleration that is enabled in the session. Faster acceleration will result lower quality

Quality	images.
Screen resolution	Size of the desktop for the session. The browser window will not be resized. If the remote desktop is larger than the browser window then scrollbars will be displayed. Select "fit to browser window" 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.

Advanced Settings

Field	**Description**
Keyboard locale	Choose desired language
Keyboard scan-codes	Enables scan codes. Certain applications use scan codes and will require this setting to be enabled.
Use Client Time Zone	Check this box to enable local time zone redirection (the remote session will use the time of the user's "local" system.
Use Secure Gateway	Select this to use the Ericom Secure Gateway to connect to the RDP host.
Gateway Address	Enter the address and port for the Ericom Secure Gateway(s) in this field. To specify a custom port, add a ':' and the port number to the address (i.e., gateway.com:4343). If no port value is specified, 443 with be used by default.

	Multiple ESG's can be specified for failover. Separate each address with a comma (,) or semicolon (;). An asterisk (*) will shuffle the items after it. For example, if the following is specified: aaa;*;bbb:4433;ccc:4343 ESG aaa on port 443 is used to initially connect. If aaa is unavailable, then bbb:4433 is used followed by ccc:4343 OR ccc:4343 followed by bbb:4433.
Open links on client (URL Redirection)	Will open URL links launched in the RDP session to open using the local browser.

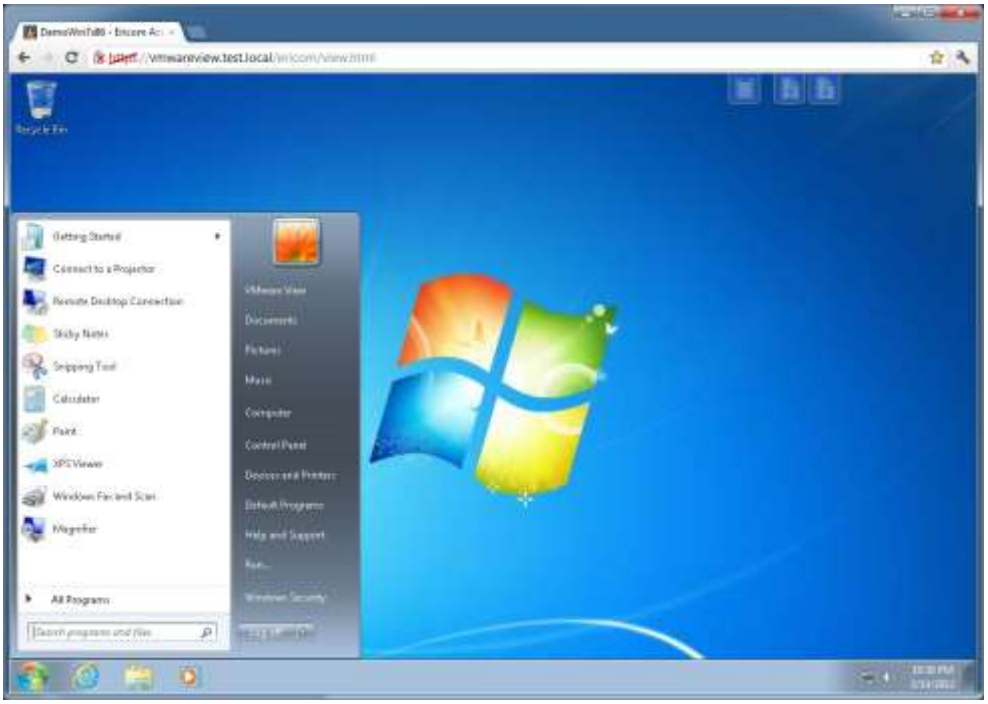
Idle Timeout

If the VMware View connection broker has an idle timeout set, and the user has not clicked *Connect* within this period of time, a timeout message will appear and the user will be logged off.

Connecting to the desktop

When the user clicks the *Connect* button, all configured settings are saved for future sessions.

After selecting the desired desktop and successfully connecting to the virtual desktop, the content of the virtual desktop will be displayed within the browser window. Keyboard and mouse input are transmitted from the browser back to the virtual desktop.



Special Key Handling

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. Other function keys, such as the Windows *Start* key will not be transmitted to the AccessNow session, but handled by the local system.

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 from the RDP session (not logged off).

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

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.

NOTE When using *Internet Explorer (MSIE) 10*, the Clipboard feature is integrated, so there are no AccessNow clipboard icons. Simply copy and paste text between the local device and AccessNow session using the traditional copy/paste commands (i.e. CTRL+C and CTRL+V).

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 Access Server service has permission to read the desired files. When uploading files, ensure that the Access Server service has permission to write files to the desired location.

- File transfer with local and mapped drives are supported.

- If the Access Server detects that the File Transfer feature cannot be used in the session, the icons will be automatically hidden.
- 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.
- File transfer functionality requires that the Access Server be installed on the RDP host; do not use Access Server as a gateway.

Download files from Remote to Local

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

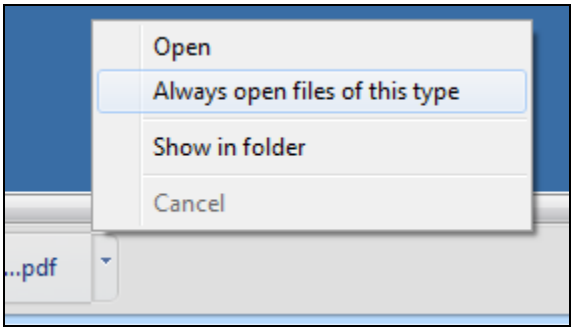
Method 1: Press the *Download* button at the upper right hand corner of the AccessNow session.

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.

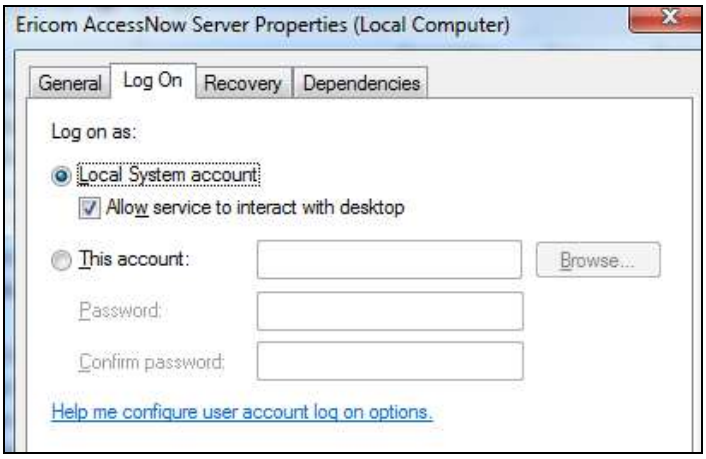
Built-in Universal Printing

Ericom AccessNow includes a built-in universal printer for redirecting remote print jobs to the local web browser. Once the print job is received by the web browser, it can be saved or printed.

NOTE	The built-in AccessNow Universal Printer driver users a generic driver and may not work in certain scenarios. The print output may also differ than that of one from a native driver.

Requirements

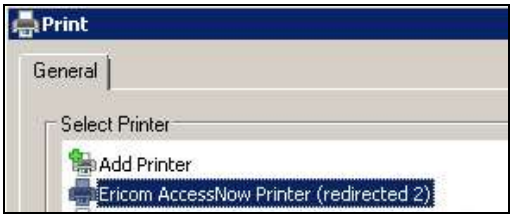
In order for the AccessNow Printer to be added to the remote sessions, the Access Server Service must have rights to add a printer to the session. In most cases the *Local System* account has sufficient rights. If it does not, go the *Access Server Properties* and enter a user account that has the rights.



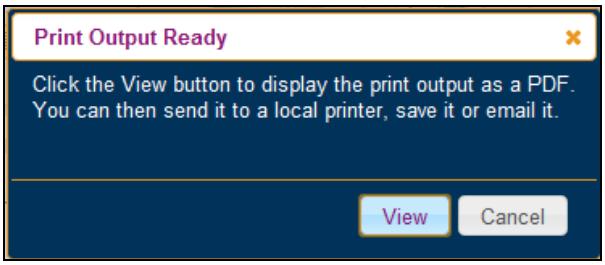
Usage

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 it 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:

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. The web browser may have shortcut buttons for both functions. Here is an example from Chrome:

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.

Using AccessNow Printer on Windows 8 and 2012

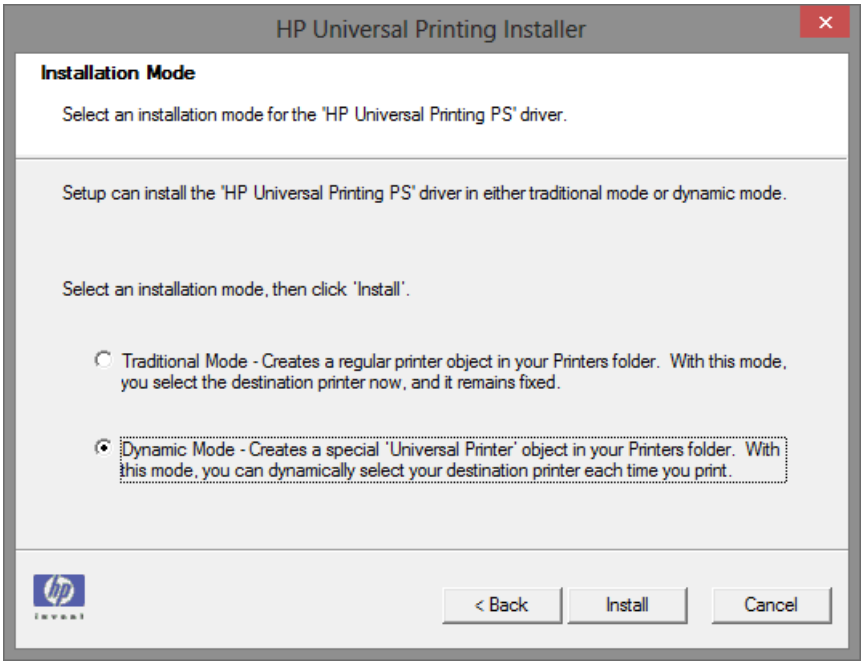
Windows 8 and 2012 do not include the necessary built-in drivers to support the AccessNow Printer. This functionality can be added by installing the HP Universal Postscript (PS) Printing Driver. Download the appropriate driver from the HP website:

For Win2012: ftp://ftp.hp.com/pub/softlib/software12/COL40842/ds-99376-6/upd-ps-x64-5.6.5.15717.exe

For Win 8 32 bit: ftp://ftp.hp.com/pub/softlib/software12/COL40842/ds-99375-6/upd-ps-x32-5.6.5.15717.exe

For Win 8 64 bit: ftp://ftp.hp.com/pub/softlib/software12/COL40842/ds-99376-6/upd-ps-x64-5.6.5.15717.exe

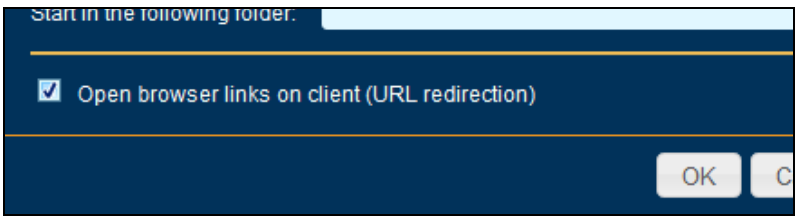
During the installation, when prompted for the *Installation Mode*, choose *Dynamic Mode*. Use default settings for all other selections.



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

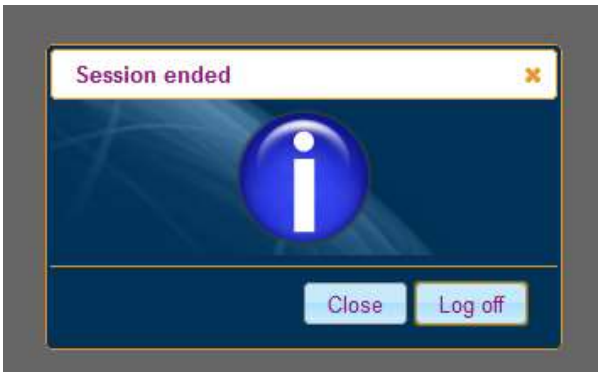
Cancel – Cancels the request

Ending the session

When the user logs out or disconnects the desktop session, the browser will display a *Session ended* dialog with two options:

Close – the session will be closed and the user will be brought back to the desktop selection list. The user is not logged off from VMware View.

Log off – the session will be closed and the user is logged off from VMware View.



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.

Session Idle Auto-logoff

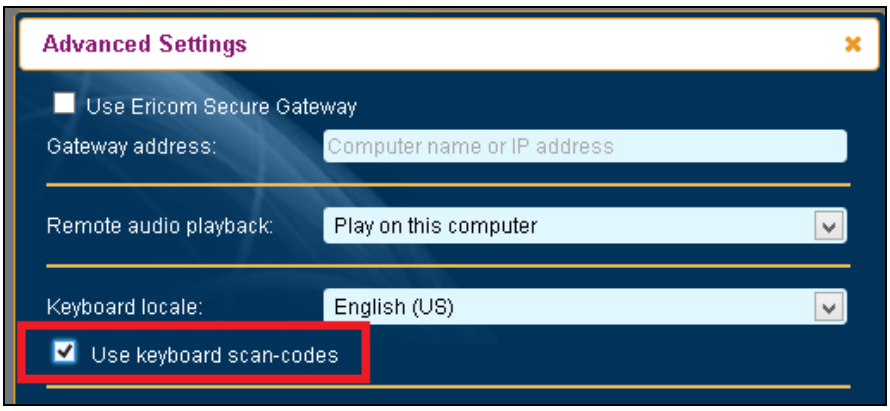
Remote desktop sessions are explicitly logged off using the *Log Off* option in the remote desktop's *Start Menu*.

Application sessions are logged off when the application is closed. In some cases the session is not closed immediately or is non-responsive. AccessNow includes an auto-logoff feature where if nothing is displayed on the screen for a specified duration of time, the session will be automatically logged off. The default value is three (3) seconds, this value may be changed by editing the *blaze.txt* file in *Resources* folder and adding the line:
RDP_LogoffDelaySeconds:i:*n* *(n* is the duration, default = 3.)

Fixing Typing Issues (Enable Scan code Input)

In some cases while typing within an AccessNow session the keyboard input will be incorrect or missing in certain applications. The affected applications may require scan-code input rather than Unicode (which is the default). To enable scan-code input, click on the AccessNow web page's *Advanced* button.

Then check the "Use keyboard scan-codes" setting, click *OK*, and test.



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*

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

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. ADVANCED CONFIGURATION

Ericom AccessNow provides flexible ways to set predefined values and accept custom values that are passed to it. 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 *Settings.js*

An administrator can modify configuration settings for AccessNow by editing the **settings.js** file that is installed as part of the AccessNow for VMware View 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.

Passing Credentials using Form POST

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

The Ericom Secure Gateway is required in order to use form POST with AccessNow. Please refer to the Ericom Secure Gateway manual for detailed instructions.

Passing Cookies

Ericom AccessNow cookies uses the same settings as the settings.js file, but with an additional **EAN_** prefix. For example, the *gateway_address* setting is

set using the cookie *EAN_gateway_address*. Ericom AccessNow erases the cookies immediately after reading them.

When using cookies, remember to perform the following:

- Use HTTPS to encrypt the cookies so that they can contain sensitive data, such as user credentials.
- Set the *Secure* option to the cookies to ensure that they are never transmitted over unencrypted communication.
- Do not use *HttpOnly* cookies because Ericom AccessNow requires JavaScript access to the cookie values.
- Use the *Path* option to limit addresses to which cookies might be sent from (Ericom AccessNow cookies should not be sent to any host-side address.)
- Use Session cookies that expire as soon as the session ends and/or specify a very short expiration duration.

Settings Precedence

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

Lowest Precedence **Highest Precedence**

settings.js | *saved settings from previous session* | *cookies*

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

If the setting *overrideSaved* is set to *true* in *settings.js*, any settings predefined in the settings.js file will override previously used settings. Precedence order:

Lowest Precedence **Highest Precedence**

saved settings from previous session | *settings.js* | *cookies*

Settings Table

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

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

Setting Value	Description
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 previously used settings.
onlyHTTPS	By default, AccessNow first attempts to connect using WebSockets. If the Ericom Secure Gateway is used with AccessNow, the connection will fall back to HTTPS when WebSockets is not available. If this setting is **true**, HTTPS is used immediately.
noHTTPS	By default, AccessNow first attempts to connect using WebSockets. If the Ericom Secure Gateway is used with AccessNow, the connection will fall back to HTTPS when WebSockets is not available. If this setting is **true**, only WebSockets will be used and HTTPS fallback will be disabled.
autostart	Set to **true** to force the AccessNow start.html page to connect automatically upon access.
hidden	A comma- or space-separated list of field names as they appear in config.js. For example "username,password,domain". The listed fields will be hidden so that the user will not be able to modify them. To hide a button, such as the Advanced button, prefix the button text with the word **show**. For example, "showAdvanced,showAbout" *hides* both the Advanced and About buttons. "locale" hides the "Display Language field". All hidden variables ignore previously saved settings.
settings (URL parameter only)	Name of a Configuration Group to be used
wsport	The default WebSocket port that will be used

	by the client. The value specified in the file (8080 by default) will be used for both encrypted and unencrypted WebSocket communication. If the Access Server port is changed, this value must also be updated manually. When no port is entered in the *Access Server* value of the *start.html* page, this port value will be used. The user can provide a different value by explicitly specifying the port value after the Access Server address.
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. The following are not supported: Alt+Delete and CTRL+ALT+MINUS SIGN (-)
chromeKeys	**true** (default) support special ChromeOS keys combinations
showDownload	**true** displays a link in the connection dialog to download the Access 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 Access 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 *screen resolution* 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: secure.acme.com:4343
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 *alternate_shell* parameter.
useScancodes	No longer in use, see convert_unicode_to_scancode
convert_unicode_to_scancode	**false** (default), set to **true** when using certain applications that send characters as scancodes (i.e. VMware vSphere Client, Ericom Blaze Client, any application where you may have issues typing text). This setting will generate scancodes based on the selected locale.
leaveMessage	The message displayed to the user after he/she navigates away from an active session

printing	**true**, enables the printing feature (default) false, disables the printing feature
fileDownload	**true**, enables the ability to download files (default) false, disables the download feature For Full Screen use "screen"
fileUpload	**true**, enables the ability to upload files (default) false, disables the upload feature
audiomode	**0**, enables audio redirection (default) 1, play audio on remote computer 2, disables audio redirection
name	Defines a custom string for the connection name. By default, the *RDP Host address* is used.
minSendInterval	Specifies the minimum duration between mouse position messages sent from the client when the mouse button is pressed. Units is milliseconds
use_client_timezone	**true** (default) enables local time zone redirection; false disables it

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

Passing Credentials using Form POST

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

The Ericom Secure Gateway is required in order to use form POST with AccessNow. Please refer to the Ericom Secure Gateway manual for detailed instructions.

Embedding AccessNow in an iframe

To embed AccessNow within a third-party web page using the iframe mechanism, simply place an iframe tag within the containing page, and have the iframe's SRC attribute reference the AccessNow URL.

For example:

```
<body>
    <h1>Embedded AccessNow</h1>
    <iframe src="http://127.0.0.1/ericom/view.html" style="width:1024px;
height:768px"></iframe>
</body>
```

When the AccessNow session ends, it can be configured to send the browser to a specified URL using the *endURL* setting.

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

AccessNow File Transfer API

AccessNow includes a file transfer mechanism that can support advanced functionality. The file transfer executable, *ANFileTransfer.exe* includes three features to provide enhanced integration with third-party applications.

After enabling any of the three features explained in this section, users with active sessions need to logoff and back on in order to use the feature.

Initiate a download of a file

Within an AccessNow session, launch: ANFileTransfer.exe *file-path*

ANFileTransfer.exe is located in the AccessNow installation folder, e.g. C:\Program Files (x86)\Ericom Software\Ericom Access Server. This folder is added to the system path during installation.

The complete path is also available in the registry under: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\ANFileTransfer.exe*. This allows the executable to be launched directly using ShellExecute.

Here is an example of a use case:

An application always creates an output file in *c:* named *test.csv*. Since the file will always be in the same location, a shortcut may be created to simplify the download process.

Launch "*ANFileTransfer.exe c:\test.csv*" and test.csv will be downloaded in one step, rather than three (initiate download, select file, click OK). This operation may also be called from a third-party application to automate the download process of an output file.

NOTE	The download destination cannot be configured ahead of time. The downloaded file will be placed in a folder specified by the web browser.

Specify upload folder

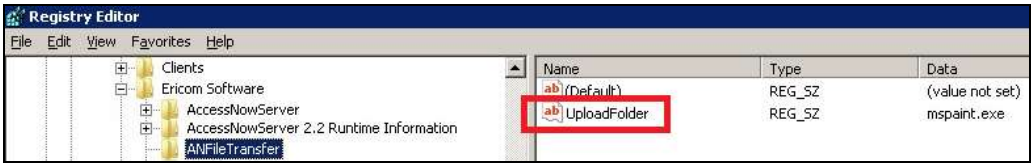
Instead of displaying a dialog to the user, uploaded files will always be placed directly into a pre-configured folder (files with the same name will be overwritten with the latest version).

The folder path is specified using a registry setting. It will be read from either HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER with HKEY_CURRENT_USER taking precedence. Before configuring the upload folder path, verify that users have write access to the specified location.

On a 32-bit system the paths are:
HKEY_LOCAL_MACHINE\SOFTWARE\Ericom Software\ANFileTransfer, REG_SZ value UploadFolder
HKEY_CURRENT_USER\SOFTWARE\Ericom Software\ANFileTransfer, REG_SZ value UploadFolder

On 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ericom Software\ANFileTransfer, REG_SZ value UploadFolder
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Ericom Software\ANFileTransfer, REG_SZ value UploadFolder

NOTE	These registry keys may not have been installed with the application. If they are missing, simply add them to the Registry.



Here is an example of a use case:

All uploaded files should go to the user's home directory. Set *UploadFolder* to the path or drive of the home directory (e.g. U:\). When users upload files with AccessNow, they will not be prompted for the upload path and all files will be placed in the specified location. It is best practice to hide and prevent access to drives that contain critical system files (e.g. C:\).

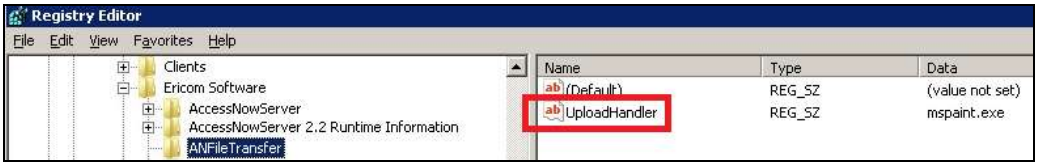
Specify executable that is launched with every uploaded file

An executable can be defined to launch with every uploaded file, with the file path as the command-line argument.

The executable is specified using a registry setting. It will be read from either HKEY_LOCAL_MACHINE or HKEY_CURRENT_USER with HKEY_CURRENT_USER taking precedence.

On a 32-bit system the paths are:
HKEY_LOCAL_MACHINE\SOFTWARE\Ericom Software\ANFileTransfer, REG_SZ value UploadHandler
HKEY_CURRENT_USER\SOFTWARE\Ericom Software\ANFileTransfer, REG_SZ value UploadHandler

On 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ericom Software\ANFileTransfer, REG_SZ value UploadHandler
HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Ericom Software\ANFileTransfer, REG_SZ value UploadHandler



Here is an example of a use case:

Only Microsoft Paint is published to the end user. Set the *UploadHandler* to the path of the published application and this application will be automatically launched each time a file is uploaded. The uploaded file will be used as the parameter for the application so it will be opened automatically (if it is a valid file for the specified application).

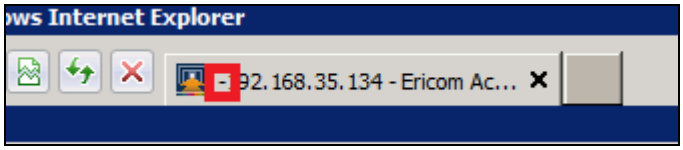
NOTE	This feature specifies a single handler application and will not verify that the application is able to properly open a file passed to it. If multiple file types need to be supported, use this feature to execute a script that checks file types, and then launches the appropriate application for each type.

7. 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 Access Server on the desired RDP Hosts.
2) Install the Ericom Secure Gateway (this does not necessarily have to be on the RDP Host or Access 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 Access 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 Access 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.

Forcing HTTP Mode

AccessNow connections may be forced to use HTTPS mode for all connections. To enable HTTPS-only mode, configure the following setting in the *settings.js* file: *onlyHTTPS:* ***true,***

In the default *settings.js* file, this line is commented out; simply delete the comments "//", save the file, and all future AccessNow connections will use this setting (the end-user's browser's cache may need to be cleared as well).

8. TECHNICAL SUPPORT

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.

AccessNow Printing with Foreign Languages

When using the AccessNow Printer with content containing foreign characters, the resulting PDF file may show incorrect characters instead.

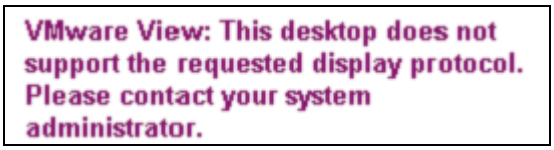
The fix for this issue is to add the entry **ps2pdf mode:i:0** to *blaze.txt*.

The blaze.txt file is located under the *resources* folder of the AccessNow web component. In an Access Server installation, this is located at *Access Server | WebServer | AccessNow | resources.*

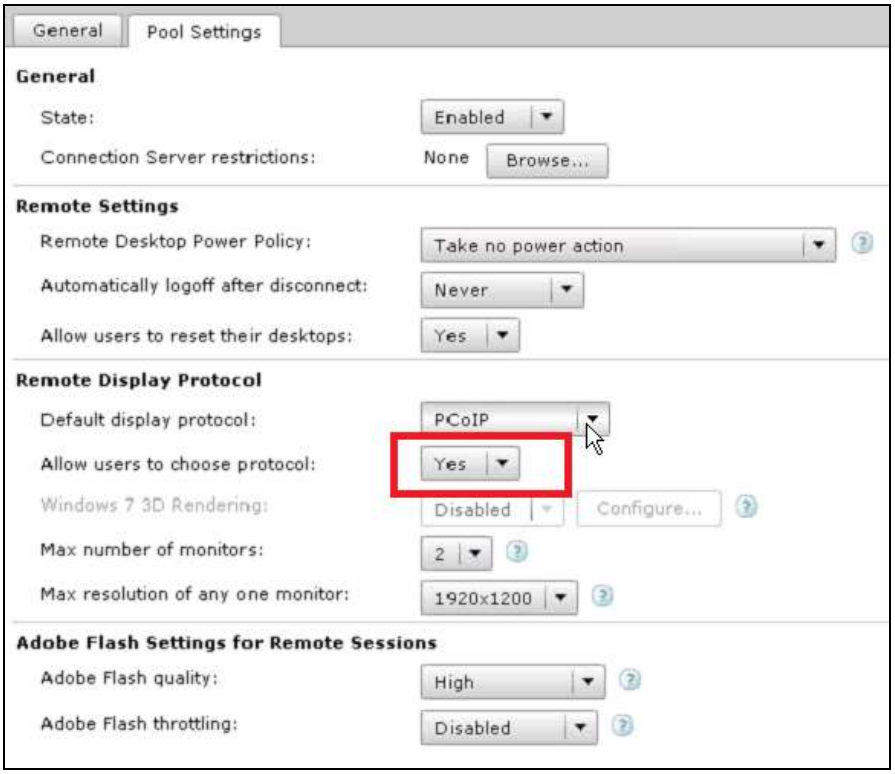
Examples	Correct	Incorrect
Korean		
Russian		

RDP is the Only Supported Display Protocol

This desktop does not support the requested display protocol



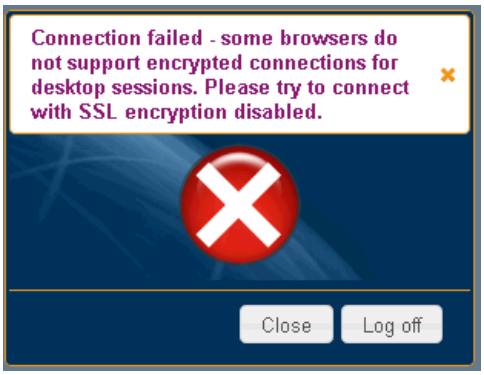
Resolution: The VMware View broker is configured to only allow the PCoIP protocol. This is not supported by AccessNow - configure VMware View to allow RDP connections.



HTTPS and SSL Encryption

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

Error: Connection Failed – do not support encrypted connections



Resolution: If the user sees an error message similar to this, the web server on the VMware View Server may require a trusted certificate.

Right Click on Mac

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

Copy Remote Text Displays Dialog

If Flash is missing or disabled in the web browser, the following *Copy* dialog will appear when content is copied from the remote session and then the user clicks on the Clipboard icon. Simply copy the text from this dialog and paste.

Demo Site to Verify Connectivity

If a user is having trouble connecting to the AccessNow environment that has been installed – ask the user to connect to the Ericom demo site on the Internet using this URL: http://demo.ericomaccessnow.com/

If the demo site appears, then the browser is compatible with AccessNow. This demo site communicates over port 443 using the Ericom Secure Gateway and a trusted certificate. If it works for the user, verify the following:

- AccessNow port between the user's browser and the AccessNow environment is available. The default port is 8080.
- A trusted certificate may be required for the Ericom Secure Gateway or the Access Server.

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)?
- Which version of VMware View are you using?

- 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 users. 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