

**Ericom AccessToGo™**

**Ericom Connect® Client**

**Ericom Blaze™ Client**

**Ericom PowerTerm™ WebConnect Client**

**Version 9.2**

**User Manual**

## Legal Notice

This manual is subject to the following conditions and restrictions:

This Manual provides documentation for Ericom Connect Client, Ericom (PowerTerm) WebConnect Client, Ericom Blaze Client and Ericom AccessToGo.

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

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.

AccessToGoUG20190531JL

Copyright © 1999-2019 Ericom® Software.

Ericom and PowerTerm are registered trademarks, and AccessToGo and Blaze are trademarks, of Ericom Software. Other company brands, products and service names, are trademarks or registered trademarks of their respective holders.

## Table of Contents

|  |           |
|--|-----------|
| <b>LEGAL NOTICE.....</b>                           | <b>2</b>  |
| <b>ABOUT THIS DOCUMENT.....</b>                    | <b>7</b>  |
| <b>1. OVERVIEW.....</b>                            | <b>8</b>  |
| <b>ARCHITECTURE.....</b>                           | <b>8</b>  |
| <b>BLAZE RDP COMPRESSION AND ACCELERATION.....</b> | <b>10</b> |
| <b>2. GETTING STARTED.....</b>                     | <b>11</b> |
| <b>PRE-REQUISITES.....</b>                         | <b>11</b> |
| <b>DEVICE REQUIREMENTS.....</b>                    | <b>11</b> |
| <b>DOWNLOADING ACCESSTOGO.....</b>                 | <b>11</b> |
| <b>CONNECTION LIST.....</b>                        | <b>12</b> |
| <b>CONNECTION OPTIONS.....</b>                     | <b>13</b> |
| <b>ONLINE HELP.....</b>                            | <b>14</b> |
| <b>CREATING A NEW CONNECTION.....</b>              | <b>14</b> |
| <b>CONNECTION PARAMETERS.....</b>                  | <b>14</b> |
| <b>DISCONNECTING AND EXITING.....</b>              | <b>16</b> |
| <b>CONFIGURING ERICOM SECURE GATEWAY.....</b>      | <b>16</b> |
| <b>3. USING ACCESSTOGO.....</b>                    | <b>18</b> |

|  |           |
|--|-----------|
| <b>ACCESSTOGO TOOLBAR .....</b>                            | <b>18</b> |
| <b>USING THE FINGER AS MOUSE .....</b>                     | <b>19</b> |
| <b>USING THE ON-SCREEN MOUSE .....</b>                     | <b>19</b> |
| <b>USING THE ON-SCREEN TOUCHPAD MOUSE .....</b>            | <b>20</b> |
| <b>USING THE KEYBOARD TOOLBAR.....</b>                     | <b>21</b> |
| <b>USING THE ON-SCREEN KEYBOARD .....</b>                  | <b>22</b> |
| <b>USING THE ON-SCREEN FUNCTION KEYBOARD.....</b>          | <b>22</b> |
| <b>USING REMOTE SESSION PPI RESOLUTION.....</b>            | <b>23</b> |
| <b>COPY AND PASTE OF TEXT BETWEEN DEVICE AND HOST.....</b> | <b>23</b> |
| <b>USING PHYSICAL KEYBOARDS AND MICE.....</b>              | <b>24</b> |
| <b>USING THE TABLET FUNCTION BAR.....</b>                  | <b>25</b> |
| <b>USING THE EXTENDED MENU .....</b>                       | <b>26</b> |
| <b>USING THE TABLET SPLIT KEYBOARD .....</b>               | <b>28</b> |
| <b>AUTO-DISPLAY KEYBOARD AND POSITION ON TEXT .....</b>    | <b>28</b> |
| <b>MULTI-TOUCH.....</b>                                    | <b>29</b> |
| <b>4. CONNECT TO DESKTOP .....</b>                         | <b>30</b> |
| <b>AUTO ROTATE RESIZE.....</b>                             | <b>31</b> |
| <b>5. CONNECT TO AN APPLICATION .....</b>                  | <b>32</b> |

|  |           |
|--|-----------|
| <b>6. CONFIGURE REMOTE ACCESS .....</b>                    | <b>34</b> |
| <b>7. CONFIGURE MANAGED BROKER ACCESS.....</b>             | <b>35</b> |
| <b>USING THE USER INTERFACE.....</b>                       | <b>35</b> |
| <b>SUPPORT FOR TWO-FACTOR AUTHENTICATION .....</b>         | <b>37</b> |
| <b>MANAGED PERMISSIONS .....</b>                           | <b>37</b> |
| <b>8. SETTINGS .....</b>                                   | <b>38</b> |
| <b>APPEARANCE .....</b>                                    | <b>38</b> |
| <b>LANGUAGE AND KEYBOARD.....</b>                          | <b>38</b> |
| <b>CONNECTION .....</b>                                    | <b>39</b> |
| <b>ABOUT.....</b>  | <b>39</b> |
| <b>GESTURES.....</b>                                       | <b>40</b> |
| <b>REMOTE DESKTOP SESSION PPI (PIXEL'S PER INCH) .....</b> | <b>41</b> |
| <b>9. URL SCHEMES .....</b>                                | <b>43</b> |
| <b>CREATING .RDP OR .BLAZE FILES.....</b>                  | <b>43</b> |
| <b>ADD MIME TYPE TO WEB SERVER.....</b>                    | <b>44</b> |
| <b>CONFIGURATION FILE PARAMETER DEFINITIONS .....</b>      | <b>45</b> |
| <b>LAUNCHING APPLICATIONS WITH URL SCHEME.....</b>         | <b>50</b> |
| <b>BLOCKING SCREENSHOTS VIA URL SCHEME (ANDROID).....</b>  | <b>51</b> |

|   |           |
|---|-----------|
| <b>NOTIFYING AN APPLICATION OF SCREENSHOT (IOS) .....</b> | <b>51</b> |
| <b>10. TECHNICAL SUPPORT .....</b>                        | <b>53</b> |
| <b>RELEASE NOTES .....</b>                                | <b>53</b> |
| <b>VERIFY CONNECTIVITY .....</b>                          | <b>53</b> |
| <b>NOT COMPATIBLE WITH CHROMEBOOKS .....</b>              | <b>54</b> |
| <b>URL SCHEME IS NOT WORKING .....</b>                    | <b>54</b> |
| <b>DISABLE RDP SSL .....</b>                              | <b>54</b> |
| <b>SSL CERTIFICATE ERROR WITH PTWC AND ESG .....</b>      | <b>54</b> |
| <b>TABLET MODE (TOP BAR) NOT AVAILABLE .....</b>          | <b>55</b> |
| <b>REQUESTING TECHNICAL SUPPORT .....</b>                 | <b>55</b> |
| <b>ABOUT ERICOM .....</b>                                 | <b>56</b> |

## ABOUT THIS DOCUMENT

This manual provides instructions on how to use Ericom Connect Client, Ericom WebConnect Client, Ericom Blaze Client and Ericom AccessToGo to connect to virtual desktops and Terminal Servers from compatible phone and tablet devices browsers.

This manual includes the following information:

- Overview of Ericom AccessToGo
- 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
- Familiarity of the device where AccessToGo will be installed

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 system that can be remotely accessed using Microsoft RDP, such as a Terminal Server (RDS Session Host) or Windows workstation with remote access enabled.
- SSL – Secure Sockets Layer is a cryptographic protocol that provides communications security over the Internet.

For more information about this product and other Ericom products, please visit the [Ericom website](http://www.ericom.com) (www.ericom.com).

# 1. OVERVIEW

Ericom *AccessToGo* provides end-users with remote access to Windows desktops and applications from any compatible phone or tablet device.

Ericom *Connect* and *WebConnect Client* uses the same engine and interface as *AccessToGo*, but is dedicated for managed broker access only. Please refer to sections related to *AccessToGo* usage and *Connect/WebConnect* configuration.

Ericom *Blaze Client* uses the same engine and interface as *AccessToGo*, but is dedicated for *Blaze* access only. Please refer to sections related to *AccessToGo* usage and *Blaze* configuration. Ericom *Blaze Client* requires *AccessServer* 7.3 and higher.

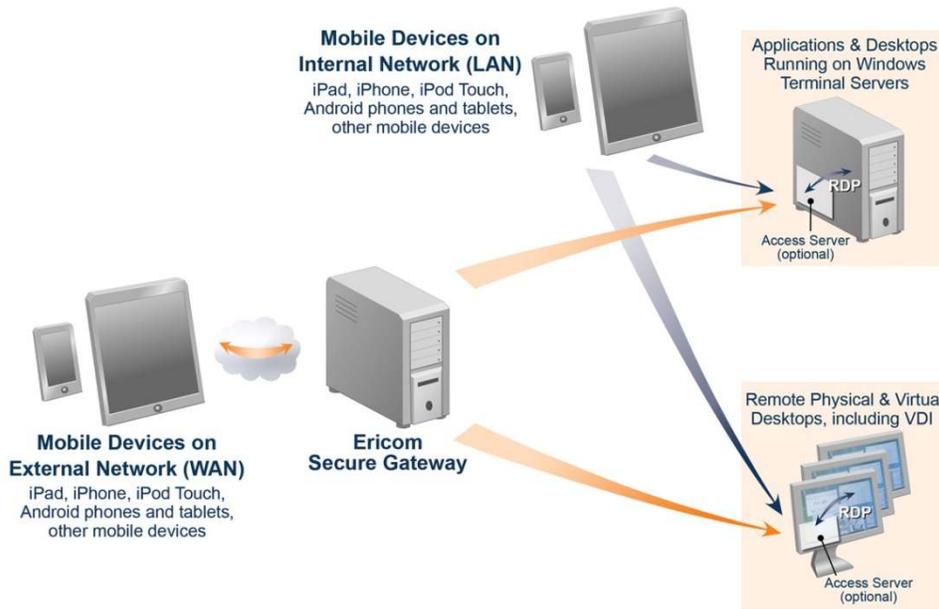
Email [mobile@ericom.com](mailto:mobile@ericom.com) with any questions or requests for technical support.

## Architecture

*Ericom AccessToGo* is comprised of three installable components:

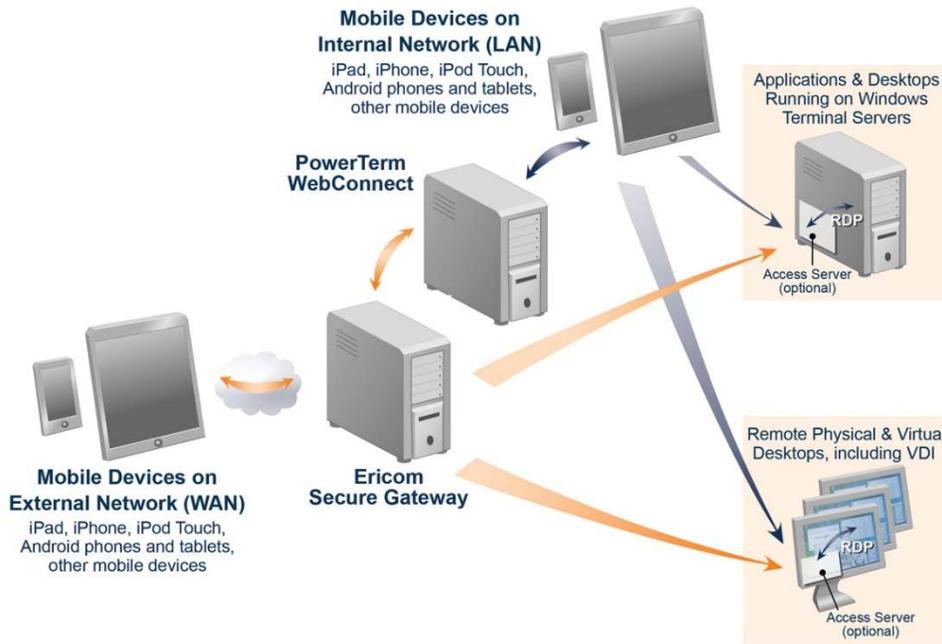
- a. Downloadable client
- b. (Optional) Access Server for RDP Acceleration and Compression
- c. (Optional) Secure Gateway Service that provides highly secure and encrypted remote access to desktops and applications

This diagram illustrates how the components of *AccessToGo* interact with each other. The orange arrows indicate remote connections and the blue arrows represent internal connections.



1. The end-user launches the Ericom AccessToGo client on a compatible mobile phone or tablet. Connection parameters are entered into the AccessToGo application.
2. AccessToGo initiates a RDP or Blaze connection to the desired RDP host.
  - a. If the optional Ericom Secure Gateway is used, the AccessToGo session will connect through it over a secure port (default 443).
3. If Blaze is enabled, the Access Server will accept the AccessToGo session and accelerate RDP (over port 8080 by default). If Blaze is not enabled, the AccessToGo session will be directly accepted by RDP (over port 3389 by default).

This diagram illustrates how the components of AccessToGo interact with each other and the Ericom Connect or PowerTerm WebConnect broker. The orange arrows indicate remote connections and the blue arrows represent internal connections.



## Blaze RDP Compression and Acceleration

Ericom AccessToGo contains Ericom's Blaze technology for RDP compression and acceleration. This technology enhances remote desktop performance over slow network connections. The accelerated sessions are also useful for viewing content that contain highly graphical images and animations.

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 (a default value can also be configured by the administrator).

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

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

## 2. GETTING STARTED

### Pre-requisites

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

- Verify with your network administrator that RDP connections are allowed to the target RDP host(s).
- Enable RDP on the target PC. Go to Control Panel | System | *Remote settings*. Under Remote Desktop select “*Allow connections from computers running any ...*”. NLA is not currently supported so do not select the third setting.
- Click on the Select Users button to add users that will be allowed to connect remotely. Click OK.
- Verify that the system’s Windows firewall allows incoming RDP connections (the default port is 3389). If Ericom protocols are being used, 8080 needs to be opened as well.

Configure the network or router firewall to allow incoming connections to the target PC over the RDP port.

### Device Requirements

AccessToGo requires at least 512 MB of RAM installed on the device. The following operating systems are supported in v9.2:

- Apple iOS 9, 10, 11, 12
- Android OS 6, 7, 8, 9

### Downloading AccessToGo

Go to the device’s marketplace (i.e. Google Play Store, Apple Appstore) and search for Ericom and select the desired app:

- AccessToGo
- Ericom Connect Client
- Ericom WebConnect Client
- Ericom Blaze Client

Once the application is downloaded an icon will appear in the device’s application list. Tap the icon to launch the application.

AccessToGo (includes RDP, Blaze, and PowerTerm WebConnect access):



Ericom Connect Client (includes Ericom Connect access only):



Ericom WebConnect Client (includes PowerTerm WebConnect access only):



Ericom Blaze Client (includes Ericom Blaze accelerated RDP access only):



## Connection List

When Ericom AccessToGo is launched, the Connection List is displayed. This is a list of all saved connections. Two sample connections to the Ericom Demo server located in the USA are included. One connection uses standard RDP, while the other uses Ericom's Blaze RDP acceleration to connect to the RDP host. If a new connection is created with the same name as an existing connection, it will automatically be renamed to avoid confusion.



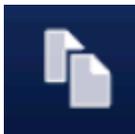
Press, tap, or click on the desired connection to launch it.

## Connection Options

Existing connections can be copied, edited, or deleted.

To apply an action to a connection press and hold on the desired connection until the action menu appears.



| Button  | Function | Description                             |
|---|----------|---|
|  | Connect  | Connect using the configured parameters |
|  | Edit     | Edit the existing connection parameters |
|  | Copy     | Copy the existing connection            |

|   |        |                        |
|---|--------|------------------------|
|  | Delete | Delete this connection |
|---|--------|------------------------|

## Online Help

To view the online AccessToGo manual - tap the *Online Help* button.



## Creating a New Connection

At the AccessToGo connection list screen, click on the *New Connection* button.



Several options will be available for selection. Choose the desired connection type and enter the connection parameters.

| Connection Type                 | Description  |
|---------------------------------|--|
| RDP (Free)                      | Connect to a RDP host with standard RDP. Make sure to enable RDP on the host   |
| Blaze                           | Requires AccessServer 7.3 or higher to be installed on the RDP host. Accelerates RDP screens showing graphics (movies, photos, etc.) over slow remote connections. For more information visit <a href="http://www.EricomBlaze.com">www.EricomBlaze.com</a> . |
| Ericom Connect                  | Connects to Ericom's Connect broker to access virtual applications and desktops  |
| PowerTerm WebConnect (VDI / TS) | Connects to PowerTerm WebConnect broker to access virtual applications and desktops  |

## Connection Parameters

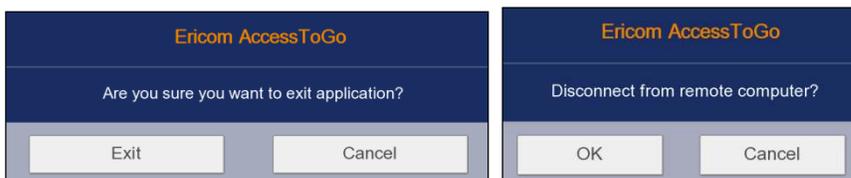
|                              |
|------------------------------|
| <b>Connection Parameters</b> |
|------------------------------|

|                                    |   |
|------------------------------------|---|
| <i>Connection Name</i>             | A customizable label for the connection being configured  |
| <i>Computer</i>                    | The address of the target system that has RDP enabled.  |
| <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.   |
| <i>User Ericom Secure Gateway</i>  | When enabled, AccessToGo will connect to the remote desktop using the specified Ericom Secure Gateway.  |
| <i>Ericom Secure Gateway</i>       | Configure and select the desired Ericom Secure Gateway for remote connectivity.   |
| <i>Blaze - RDP acceleration</i>    | When checked, enables lossy image compression for the session. Degree of quality loss / acceleration can be specified using the drop down list. Requires Access Server on the RDP host and activated license(s).  |
| <i>Acceleration Quality</i>        | Controls the degree of acceleration that is enabled in the session. Faster acceleration results in lower quality.   |
| <i>Desktop Size</i>                | <p>Size of the remote RDP desktop for the session. If the remote desktop is larger than the mobile device window, the user will have to scroll or zoom to see desktop areas that are not displayed. When <i>Automatic</i> is enabled, if the device is a tablet (screen size is 6 inches or larger), it will open the session in Full Screen. For non-tablet devices, the remote desktop size will be automatically determined by the application.</p> <p><b>IMPORTANT:</b> Refer to the <i>Advanced Feature</i> section on how to use the <b>PPI</b> feature to display the perfect resolution on your device!</p> |
| <i>Start Program on connection</i> | Enables application launch mode. On Terminal Server sessions, only the application will appear and the remote desktop will not be accessible. On workstation systems accepting RDP, the selected application will launch, but can be minimized to reveal the desktop.   |

|                             |  |
|-----------------------------|--|
| <i>Path/File Name</i>       | Specify the path to the application to be launched   |
| <i>Start Folder</i>         | Specify the start folder for the application   |
| <i>Color Depth</i>          | Sets the color depth of the session  |
| <i>Play sound on device</i> | <p>Enables audio for sessions where audio is available on the RDP host. To verify if audio is available, connect to the RDP host using mstsc.exe and verify that audio can be heard on a standard PC.</p> <p>Connections with limited bandwidth or high latency may not redirect audio perfectly. There may be distortion or choppiness.</p> |
| <i>Connection Speed</i>     | Set the Connection Speed of the network  |
| <i>Desktop Options</i>      | Configure RDP related desktop experience settings  |
| <i>Console Session</i>      | Check this setting to enable console session. This is equivalent to using the /console or /admin flag when using mstsc.exe.  |

## Disconnecting and Exiting

To disconnect an active session or exit the AccessToGo application on Android devices, press the device's *Back* button. A prompt will appear to confirm the disconnection or exit.



## Configuring Ericom Secure Gateway

The Secure Gateway is used for encrypted remote access from the AccessToGo application to the internal RDP hosts. The Secure Gateway is available for the following mode: RDP and Blaze. Ericom Connect and PowerTerm WebConnect connections will use the Secure Gateway as its address (when the ESG is configured to act as a reverse proxy for the PowerTerm WebConnect service).

The Secure Gateway is enabled in a Connection's *Options*.



- 1) Check *Use Ericom Secure Gateway* to enable the use of a Secure Gateway.
- 2) Then tap *Ericom Secure Gateway* to select configured Secure Gateways.
- 3) To add a new Secure Gateway, tap the *New Gateway* button and complete the required fields:

| Field           | Description  |
|-----------------|--|
| Server          | The address of the Secure Gateway server                       |
| Connection Port | The port value that the Secure Gateway service is listening on |
| User Name       | User name to authenticate into the Secure Gateway              |
| Password        | Corresponding password for the Secure Gateway                  |

- 4) Tap on the desired Secure Gateway to enable it.

**NOTE** The default gateway port is 443. If the Secure Gateway is listening on a custom port, make sure to enter the correct value for the *Connection Port* parameter.

### 3. USING ACESSTOGO

#### AccessToGo Toolbar

The AccessToGo toolbar is located at the bottom of the desktop or application once a session is established. To display the AccessToGo toolbar on *Android* based devices, press the Menu button on the device (usually the leftmost button).

To display the Toolbar upon connection, go to Settings and check Always



| Button  | Function                                      | Description  |
|---|---|--|
|   | On-screen mouse                               | Displays/Hides the on-screen mouse   |
|  | On-screen touchpad mouse                      | Display/Hides the on screen touchpad mouse   |
|  | Display On-screen keyboard                    | Displays the on-screen keyboard.   |
|  | Zoom In/Out                                   | Zoom In/Out of the screen  |
|  | Remote Mouse Mode<br><br>(Enabled by default) | When enabled, all mouse movements and gestures will be applied within the remote session. For example, the gesture to zoom out of the current display will be disabled. To scroll the local screen, tap and hold for half a second and then move the finger. |
|  | Scroll wheel mode                             | When this mode is enabled, sliding the finger up and down the screen will mimic the movements of a scroll wheel  |
|  | Extended Menu                                 | Displays additional functions, such as <i>Configure Gestures</i>   |

|   |   |   |
|---|---|---|
|  | Hide Toolbar – Down button  | When the Toolbar is displayed, this button will hide it   |
|  | Show Toolbar – Up button (Apple iOS only prior to version 9.x, Both editions have this starting at 9.x) | When the Toolbar is hidden, this button will display it. Starting in version 9.x this version is also available on Android. On older Android devices, pressing the physical Menu button will also to display the Toolbar. |
|  | Japanese Kanji/IME key  | When the Japanese locale is enabled, the Kanji/IME virtual key will appear.   |

## Using the Finger as Mouse

The user may use his or her finger to initiate mouse movements. The user taps an area on the screen, a click indicator will appear. The indicator will consist of a dot where the mouse click is executed upon in the session and a circle to represent the finger tap.

To execute a right-click, tap and hold the screen. Wait for the right click indicator to complete a circle and then release to complete the right click.

## Using the On-screen Mouse

The on-screen mouse provides convenient functions to interact with the remote session. Regardless of whether the mouse is enabled, the user may also use his or her finger to interact with the session.

| Operation   | Finger gesture    |
|-------------|-------------------|
| Left-click  | single tap        |
| Right-click | single tap + hold |

Full on-screen mouse icon:



When the On-screen mouse is enabled, the following functions are available.

| Icon  | Function                   | Description  |
|---|----------------------------|--|
|    | Mouse/Left click           | Tap this icon to execute a left click. Press and hold this icon to drag the mouse pointer around the screen.   |
|    | Pointer                    | This icon represents the mouse pointer   |
|    | Right click                | Tap this icon to right-click on the area where the mouse pointer is over   |
|   | Scroll wheel mode          | When this mode is enabled, sliding the finger up and down the screen will mimic the movements of a scroll wheel  |
|  | Remote Mouse Mode          | When enabled, all mouse movements and gestures will be applied within the remote session. For example, the gesture to zoom out of the current display will be disabled. To scroll the local screen, tap and hold for half a second and then move the finger. |
|  | Display On-screen keyboard | Displays the on-screen keyboard  |
|  | Close Mouse                | Hides the mouse  |

## Using the On-screen Touchpad Mouse

The Touchpad mouse allows the user to use the screen of the device as a touchpad mouse. When the Touchpad is enabled, the user can tap on any area on the screen to obtain control of the mouse. Simply slide the finger to move the mouse around the screen. The finger does not have to be directly over the mouse. Tap and hold the mouse to initiate a right-click. While Touchpad is enabled, the user can still perform zoom in and zoom out gestures on the screen.

Touchpad Mouse button:



## Using the Keyboard Toolbar

AccessToGo includes enhanced keyboard functionality. When the on-screen keyboard is enabled, the following operations are available.



| Icon  | Description   |
|---|---|
|    | Displays advanced keyboard keys: function keys, arrow keys, and key combinations (i.e. CTRL+ALT+DEL). Pressing this key will also toggle the advanced keys with the OS virtual keyboard.  |
|  | Simulates the ESC key   |
|  | Simulates the TAB key   |
|  | Simulates the pressing of the CTRL key - when activated the green light will turn bright  |
|  | Simulates the pressing of the ALT key - when activated the green light will turn bright. Pressing the ALT the first time will "hold" Hold the ALT key. Pressing the key again will "Tap" the ALT key.   |
|  | Simulates the pressing of the Windows key (displays the Windows Start menu)   |
|  | Displays the on-screen PC keyboard. The device's virtual keyboard is the default. The on-screen PC keyboard provides an enhanced user experience.<br><br>Pressing the button again while the keyboard is displayed will toggle between default OS keyboard and the AccessToGo keyboard. |
|  | Pressing this button will toggle through the languages that are enabled. To enable languages, go to <i>Settings   Select Preferred Keyboard Languages</i>   |



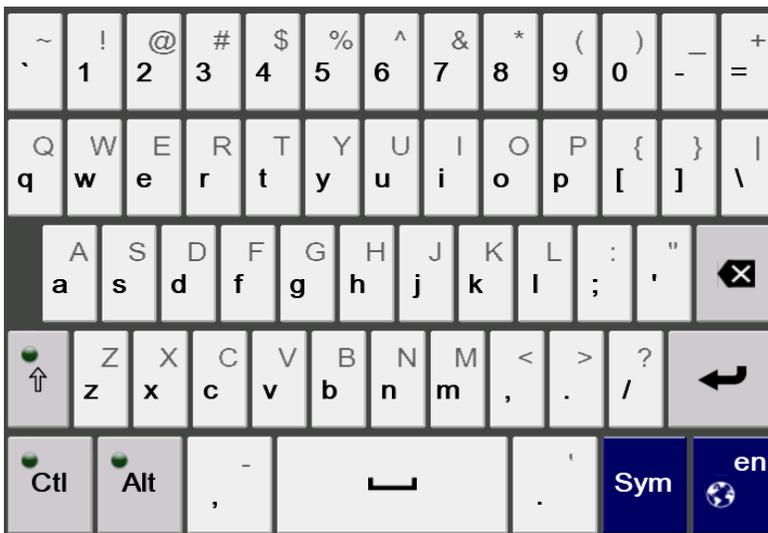
## Using the On-screen Keyboard

Pressing the On-Screen keyboard button will reveal the AccesToGo keyboard. The AccesToGo keyboard provides additional keys and features for an improved user experience when typing in Windows-based applications.

On-Screen keyboard button:



AccesToGo Keyboard:



## Using the On-screen Function Keyboard

Pressing the On-Screen Function keyboard button will reveal the AccesToGo function keyboard. The Function keyboard provides function keys, common Windows key combinations, and scrolling keys for an improved user experience when typing in Windows-based applications and desktops.

On-Screen function button:



AccessToGo Function Keyboard:

|        |                  |          |      |      |      |          |         |
|--------|------------------|----------|------|------|------|----------|---------|
| F1     | F2               | F3       | F4   | F5   | F6   | Ctrl+Tab | Ctrl+F4 |
| F7     | F8               | F9       | F10  | F11  | F12  | Alt+Tab  | Alt+F4  |
| Ctrl+Z | Ctrl+Alt         | Ctrl+Esc | Home | ▲    | PgUp | Del      |         |
| Ctrl+X | Ctrl+C           | Ctrl+V   | ◀    | Ins  | ▶    | ✖        |         |
| ↑      | Ctrl + Alt + Del | End      | ▼    | PgDn | ↶    |          |         |

## Using Remote Session PPI Resolution

With the increasing diversity of end-user devices and user preferences, it is ever more important to allow the user to work with the most comfortable resolution when launching a remote desktop or application.

By default, the **PPI** for devices with screen sizes less than 7 inches is 190; and the PPI for screen sizes 7 inches or greater is 170. These settings will provide the optimal usage based on the device’s screen size, however the user may also select a custom PPI value. Refer to the *Advanced Feature* section on how to use the PPI feature to display the perfect resolution on your device!

## Copy and Paste of text between device and host

AccessToGo includes text-only clipboard support for Copy and Paste functionality. The clipboard is enabled by default and may be disabled by going to *Setting* and unchecking *Enable Clipboard*.

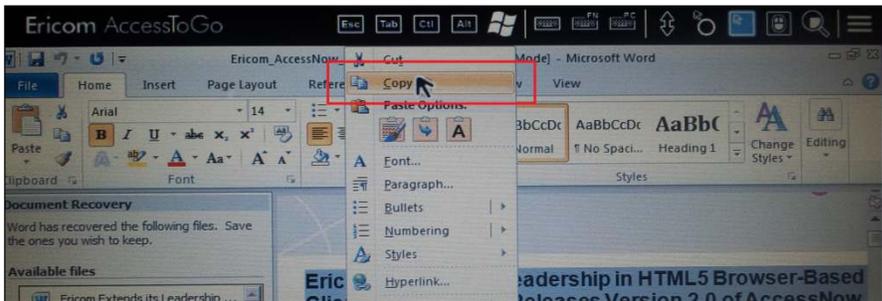
Enable Copy/Paste between device and host



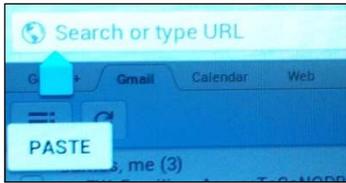
When this feature is enabled, copy and paste functionality is supported in both directions: copy/paste from local device to the AccessToGo session and vice versa.

Here is an example of a copy/paste operation from the remote AccessToGo session to the local device browser.

Perform a *Copy* operation from the remote AccessToGo session:



Once the desired text is copied to the clipboard, switch to the local application and initiate a *Paste* operation. The selected text will be copied over from the clipboard.



**NOTE** On certain devices, switching to the local application may end the AccessToGo session.

## Using Physical Keyboards and Mice

Physical input/output devices are handled by the operating system, and not directly by the applications. AccessToGo will accept input from physical keyboards and mice based on what is received from the operating system when such devices are used. Certain keys on a physical keyboard, such as the Right Shift, may not work properly because the operating system does not support it (and it will not work properly with *any* application on the device).

### Activating a Physical keyboard

Physical keyboards, such as a Bluetooth keyboard, may or may not work as soon as the session is established (varies based on the device). On devices where the keyboard does not work upon session connect, enable the AccessToGo Device Keyboard (tap button below) and then try typing.



**NOTE** When using a physical mouse, the right mouse button is only supported on devices running Android 4.0 and higher.

Bluetooth keyboards that have been tested on Android and Apple iOS devices:

HP Touchpad Bluetooth Keyboard, Microsoft Bluetooth Keyboard 6000

## Using the Tablet Function Bar

The Tablet Function bar (also known as the “Top” bar) displays popular keys (ESC, TAB, CTRL, ALT, Windows) and functions (such as display On-screen mouse) that may be used during any active session.

AccessToGo will detect whether the device is considered a tablet upon startup. A device where AccessToGo has more than 5.5 inches of display space will be classified as a tablet, and the Tablet Function bar will appear (by default) at the top of any active session.

The bar may be disabled by unchecking *Enable Top Bar* under *Settings*.



Tap and hold any button to view a brief description of its purpose.

| Button  | Function          | Description  |
|---|-------------------|--|
|  | Esc               | Escape key   |
|  | Tab               | Tab key  |
|  | Ctrl              | Control key  |
|  | Alt               | Alt key  |
|  | Windows key       | Executes the Windows key   |
|  | Device keyboard   | Displays/Hides the device keyboard for text input  |
|  | Function keyboard | Displays/Hides the function keyboard to perform special keys and combinations                          |
|  | PC keyboard       | Displays/Hides the PC keyboard for text input. This feature resembles a traditional PC keyboard layout |
|  | Scroll wheel mode | When this mode is enabled, sliding the finger up and down the screen will                              |

|   |                          |  |
|---|--------------------------|--|
|   |                          | mimic the movements of a scroll wheel. Moving or panning of the session display is not available.  |
|    | On screen floating mouse | Displays/Hides the on-screen mouse. Only actions applied by the floating mouse are applied inside the session. Moving or panning of the session display is available.  |
|    | On-screen Touchpad mouse | Display/Hides the on-screen Touchpad mouse. All mouse movements/gestures are applied within the remote session. Moving or panning of the session display is not available.   |
|   | Remote Mouse Mode        | When enabled, all mouse movements and gestures will be applied within the remote session. For example, the gesture to zoom out of the current display will be disabled. To scroll the local screen, tap and hold for half a second and then move the finger.<br><br>Moving or panning of the session display is not available. |
|  | Zoom In/Out              | Zoom In/Out of the screen  |
|  | Japanese Kanji/IME key   | When the Japanese locale is enabled, the Kanji/IME virtual key will appear.  |
|  | Extended Menu            | Displays a menu with additional AccessToGo functions   |

## Using the Extended Menu

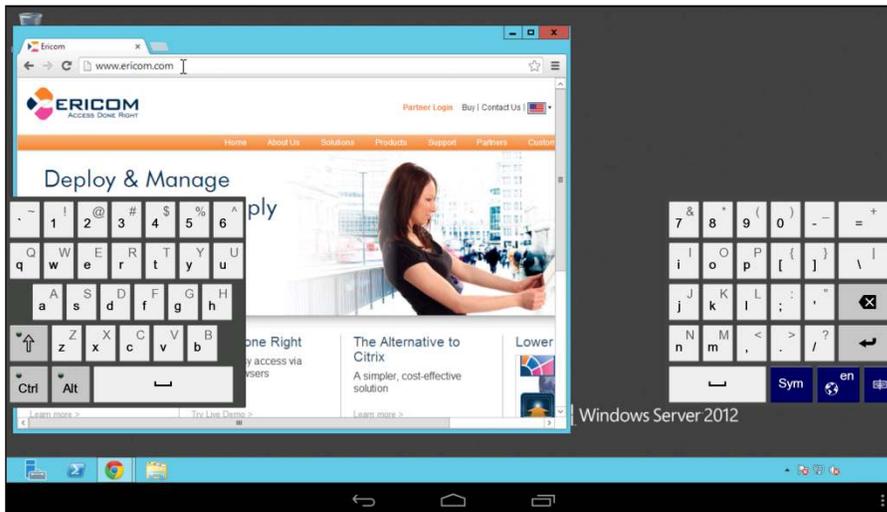


The Extended menu is accessible from the AccessToGo Toolbar and Tablet bar and provides additional functions described below.

|   |                         |   |
|---|-------------------------|---|
|  | Current Keyboard Locale | Displays the current keyboard locale language   |
|  | Configure Gestures      | Configure the desired functions for supported gestures  |
|  | Remote PPI              | Configure the PPI setting during an active session. Remote Session will automatically resize. |
|  | On-screen Help          | Displays the on-screen help dialog  |
|  | Exit Session            | Exits the current session and returns to the previous menu                                    |

## Using the Tablet Split Keyboard

AccessToGo includes the ability to use a Split PC Keyboard. This PC keyboard mode is designed to make the virtual keyboard more ergonomic so that the end-user can type with the thumb while holding the device.



### Disabling Split Keyboard

To disable the Split PC Keyboard and switch to full PC Keyboard mode, tap this button in the lower right:



### Auto-display Keyboard and Position on Text

AccessToGo will automatically display the built-in keyboard and position the display so the text field is visible for optimal usability. The keyboard will automatically close when the text field is no longer in focus. Certain applications are written in a manner where AccessToGo cannot detect the text field; as a result this feature will not work with such applications.

**NOTE** This operation is not applicable when *Split-keyboard* is enabled on tablets

## Disabling Auto-Keyboard and Position

Go to the *Settings* menu and *Language and Keyboard* and uncheck *Automatically show keyboard*.

## Multi-Touch

Multi-touch is an RDP feature supported in Windows 8 and Server 2012 and higher.

When multi-touch is enabled, the context related multi-finger gestures will be available in supported applications.

For example, when using Excel the user can use the two-finger gesture to zoom in on the Excel document without zooming in on the whole desktop.

The user may also use the swipe-up/down multi-finger gesture to scroll a page in a web browser without moving the entire desktop.

When connecting to a server that supports multi-touch, a short message is displayed on the screen notifying the user that multi-touch is available. When multi-touch is active, the session menu will have an option to enable/disable multi-touch mode.

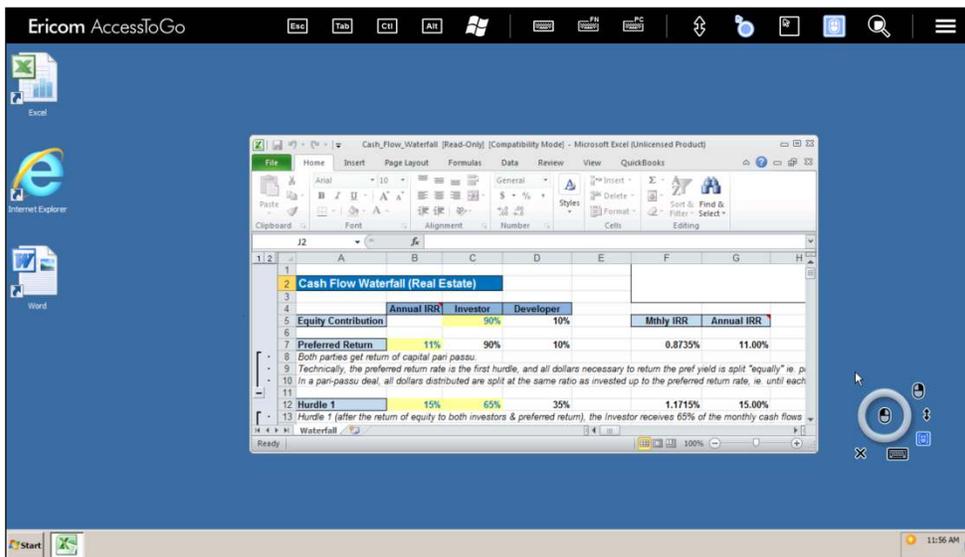
When using a gesture in multi-touch mode, the multi-touch icon will appear on the screen.



## 4. CONNECT TO DESKTOP

Once the connection parameters are configured, save the connection if desired. Press the *Connect* button to start the connection.

After a successful login, the user is connected to the desktop; the content of the virtual desktop is displayed within the browser window. AccessToGo intercepts mouse button and keyboard events, and transmits them to the RDP host. If the device is recognized as a tablet, the AccessToGo toolbar will be displayed at the top of the application as shown here:



To disconnect from an active session, press the device's *Back* button. A prompt will be displayed to confirm the disconnect request. A *Disconnect* command may also be initiated from the Windows *Start* menu.



To enable Blaze RDP acceleration access, the optional *Access Server* must be installed on the RDP host. The following RDP hosts are supported: Windows Vista, 7, 8, 10, 2008, 2008 R2, 2012, 2012R2 and 2016.

**NOTE** In order to use Blaze mode, AccessServer 7.3 or higher is required on the RDP host. If an older version of Blaze Server is installed, the connection will fall-back to the RDP protocol.

## Auto Rotate Resize

During a *Full Screen* session, AccessToGo can automatically resize the screen to support a new resolution when the device is reoriented (auto-rotate feature is enabled). To enable this feature, go to the application Settings and check the setting *In full Screen, resize on orientation change*.



## 5. CONNECT TO AN APPLICATION

To launch just an application rather than the full desktop configure the *Programs* parameters in the *Connection* parameters.

| <b>Programs Parameters</b>         |   |
|------------------------------------|---|
| <i>Start program on connection</i> | Configures the connection to launch just the specified program on the RDP host upon connection                |
| <i>Path and File Name</i>          | The path of the application to be launched from the RDP host. Make sure the application is properly installed |
| <i>Start Folder</i>                | The path to the working folder for the application  |

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

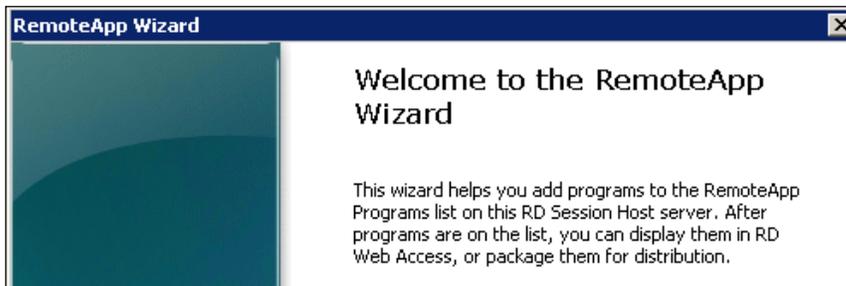


Remote applications only work when connecting to *Terminal Servers*. This functionality is not available on Windows workstation operating systems (i.e. Windows 7).

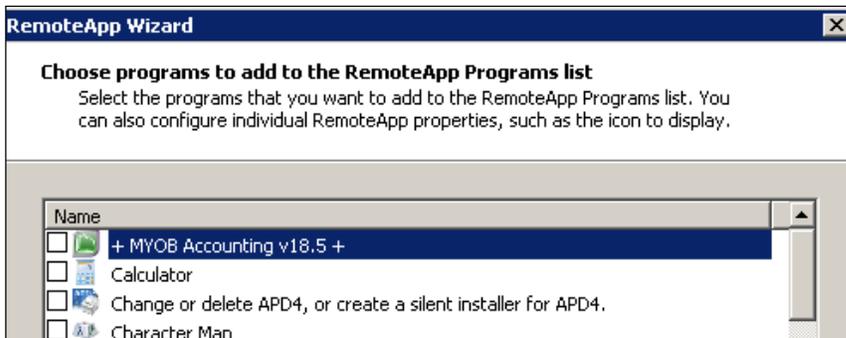
On Windows 2008 Terminal Servers (and 2008 R2RDS) RemoteApps must be enabled on the server. Applications that will be launched must be added to the *RemoteApps Programs* allowed list.

| RemoteApp Programs |  |               |              |  |
|--------------------|--|---------------|--------------|--|
| Name               | Path   | RD Web Acc... | Arguments    |  |
| Calculator         | C:\Windows\system32\calc.exe                               | Yes           | Disabled     |  |
| Paint              | C:\Windows\system32\mspaint.exe                            | Yes           | Disabled     |  |
| PowerTerm          | C:\Program Files\Microsoft Terminal Services\PowerTerm.exe | No            | Unrestricted |  |
| PowerTerm          | C:\Program Files\Microsoft Terminal Services\PowerTerm.exe | No            | Unrestricted |  |

Follow instructions for adding applications to RemoteApp:



Select desired applications that may be launched using TS/RDS:



After the desired application(s) have been added, test the connection using AccessToGo before distributing to end-users.

## 6. CONFIGURE REMOTE ACCESS

AccessToGo may be used as a remote access solution to any Windows based PC that supports RDP. Certain Windows operating systems do not support incoming RDP sessions (i.e. Windows 7 Home). Here are the steps required to implement a basic remote access connection:

- 1) Verify with your network administrator that remote RDP connections are allowed to the target PC. Some organizations prohibit RDP connections to their PC's.
- 2) Install AccessToGo on the end-user device (i.e. iPad).
- 3) Enable RDP on the target PC. Go to *Control Panel | System | Remote settings*. Under *Remote Desktop* select "Allow connections from computers running any ...". NLA is not currently supported so do not select the third setting.
- 4) Click on the *Select Users* button to add users that will be allowed to connect remotely. Click *OK*.
- 5) Verify that the PC's Windows firewall allows incoming RDP connections (the default port is 3389)
- 6) Configure the network or router firewall to allow incoming connections to the target PC over the RDP port.
- 7) Configure AccessToGo to connect to the address of the target PC. If the connection is being made remotely, point to the external address of the firewall/router that has been configured with the rule to port forward incoming connections to the target PC.
- 8) If the optional Access Server is used for RDP acceleration, note that the Blaze port is 8080.
- 9) If the optional Ericom Secure Gateway is used for remote connections, port 443 (rather than the RDP port) will be required on the network firewall. The Secure Gateway port value can be changed, see the documentation on the Ericom Secure Gateway for more information.

## 7. CONFIGURE MANAGED BROKER ACCESS

AccessToGo may be used to connect to an application or desktop hosted through an Ericom Connect or PowerTerm WebConnect connection broker. Here are the steps required to implement a remote access connection to a remote session:

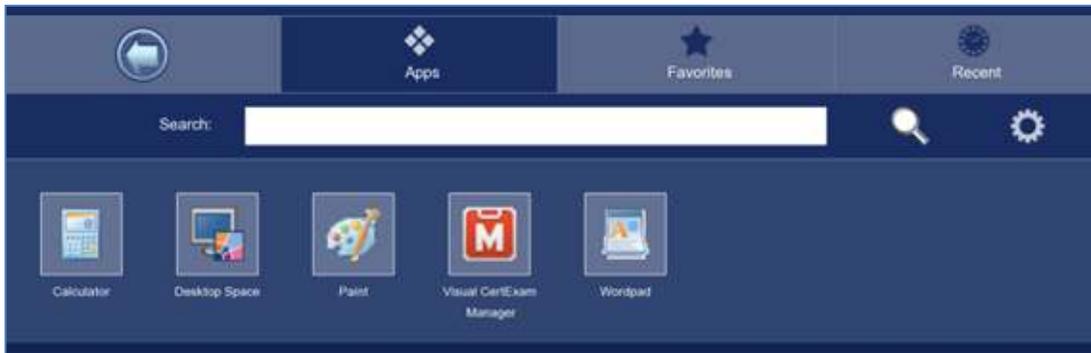
- 1) Verify with your network administrator that remote RDP connections are allowed to the target RDP host(s).
- 2) Enable RDP on the target PC. Go to *Control Panel | System | Remote settings*. Under *Remote Desktop* select "Allow connections from computers running any ...". NLA is not currently supported so do not select the third setting.
- 3) Click on the *Select Users* button to add users that will be allowed to connect remotely. Click *OK*.
- 4) Verify that the system's Windows firewall allows incoming RDP and/or Blaze connections (the default port is 3389 and 8080 respectively.)
- 5) Configure the network or router firewall to allow incoming connections to the target PC over the RDP port.
- 6) Install AccessToGo on the end-user device (i.e. iPad).
- 7) Configure AccessToGo to connect to the address of the Ericom Connect or WebConnect server. Explicitly specify the port if it is not 8011 for Connect or 4000 for WebConnect (i.e. 192.168.1.1:443).
- 8) If the optional Ericom Secure Gateway is used for remote connections, specify its external address and port 443 (rather than the PowerTerm WebConnect port). The Secure Gateway will act as a reverse proxy to the PowerTerm WebConnect server. The Secure Gateway port value can be changed (default is 443). See the Ericom Secure Gateway documentation for more information.
- 9) Configure the optional username and password that will be used to login to Ericom Connect or PowerTerm WebConnect.

**NOTE** To use the PowerTerm WebConnect "SmartInternal" setting, this environment variable must be set on the server:

*SmartInternalIsGateway* set to 1

### Using the User Interface

The Ericom Connect and WebConnect Connection interface will be displayed upon successful authentication into the brokered environment.



There are four tab options that the user can select:

| Function  | Description   |
|---|---|
|    | Log out   |
|   | Displays all assigned published applications and desktops   |
|  | Displays all assigned published applications and desktops marked as Favorite by the user  |
|  | Displays all assigned published applications and desktops that were recently launched.  |
|  | Access the Settings to configure AccessToGo features such as the Automatic PPI resize.  |
| Search:   | Enter a keyword in this field that will be used with the Search function. Tap the Search button to begin the search.  |
|  | <i>Search</i> for published connections that contact the keyword entered in the Search field. For example, entering "pa" will return results such as <b><i>Paint</i></b> , <b><i>Wordpad</i></b> , and <b><i>Space Game</i></b> . |
|  | If a keyword is entered in the <i>Search</i> field, this button will clear it.  |

Tap and hold a connection to display the option menu:



| Function  | Description                        |
|---|------------------------------------|
|  | Launch the connection              |
|  | Add connection to <i>Favorites</i> |

To search for a connection, enter a keyword into the *Search* field and tap the magnifying glass icon. A list of connections will be displayed based on the search.

## Support for Two-Factor Authentication

When connecting to an Ericom Connect or PowerTerm WebConnect 6.0 environment where two-factor authentication is enabled, a dialog will appear after the initial password login to request the second factor.



The user is able to enter a second authentication factor by typing it in or using the “Paste” function. Tap and hold the text field to see the Paste function, or press the Paste button to paste a string that has been copied to the clipboard.

If the second authentication is successful, the resource list will be displayed. If the authentication fails, the user may retry the authentication again.

## Managed Permissions

When using the Managed client, various settings that are defined in the AccessToGo application will be overridden by settings that are defined in the connection broker, i.e., Ericom Connect. For example, Copy/Paste between the device and host is configured in Ericom Connect, the local settings will not apply. An exception to this rule is the Desktop size/resolution. ATG settings always apply so the user can choose an optimal setting for the device.

Starting in version 9.x, passwords that are saved locally in the app will be removed if so configured in the Ericom Connect broker (Configuration | Settings | Secondary/Tenant Settings | Allow to Save Password).

## 8. SETTINGS

Click on the *Settings* button at the Connection List screen to configure AccessToGo application settings.



The available settings are organized into the following categories: *Appearance*, *Gestures*, *Language and Keyboard*, *Connection*, and *About*.

### Appearance

|   |   |
|---|---|
| Always Show Bottom bar                      | Displays the Toolbar at the bottom of the screen upon connection.   |
| In Full Screen Resize on Orientation change | If the device supports auto-rotate when the device is reoriented, AccessToGo will reconnect to the session to support the new resolution after the orientation change. This will only occur when the connection is in Full Screen mode. |
| Enable click animation                      | When checked, an animation will appear when the user performs a single click or double-click (long single tap) operation within an AccessToGo session.  |
| Remote Desktop PPI                          | See section on PPI  |
| Remote Mouse mode in Full Screen            | Enables remote mouse mode, unless the virtual keyboard is open (so the user can navigate around the screen).  |

### Language and keyboard

|                       |  |
|-----------------------|--|
| UI Language           | Changes the language of the AccessToGo application interface.                    |
| Default Keyboard type | Select between the keyboard layout of a native device keyboard or a PC keyboard. |
| PC Keyboard Language  | Select the languages of the PC keyboard that will be used with AccessToGo.       |

|                             |  |
|-----------------------------|--|
| Remote Keyboard Locale      | Select the region of the desired keyboard language locale. This should be set to the same language that is used on the remote RDP session.   |
| Use keyboard scan-codes     | Enables keyboard scan code mode. This setting must be enabled for certain operating systems and applications. Try enabling this setting if the user is unable to type within a desktop session or application. |
| Automatically show keyboard | Enable/disable the feature to automatically show the keyboard and position the text field when the focus is on a text field.   |

## Connection

|   |  |
|---|--|
| Enable Copy/Paste between device/host       | Enable/disable the feature to allow copy/paste between device and the host session.  |
| Reconnect                                   | Check this setting to enable session reconnect.  |
| PowerTerm WebConnect/Ericom Connect Timeout | If a session cannot be established to the connection broker during this timeout interval, AccessToGo will stop trying to connect. Applies to Ericom Connect as well. |
| Ask before disconnect                       | When checked, a confirmation prompt will appear when the user attempts to disconnect a session.  |

## About

|                 |   |
|-----------------|---|
| Product Version | Version number and build                          |
| What's New      | Displays a list of new features in this version   |
| Device          | Device ID   |
| OS Version      | Type and version of the operating system          |
| Reset Settings  | Restore application settings back to the defaults |
| Debug Logging   | Enable upon request by Ericom Technical Support   |

## Gestures

AccessToGo supports hand gestures to maximize user productivity. Any of the supported gestures may be configured to perform a certain operation.

To modify Gestures, go to the *Settings* menu and tap on *Configure Gestures*.



Tap on the *Edit* button to modify the desired *Gesture*.



The following images display the default Gestures configuration.

| 2 Fingers Gestures  | 3 Fingers Gestures   |
|---|--|
|  Swipe Up<br>Scroll Down                     |  Swipe Up<br>Page Up        |
|  Swipe Down<br>Scroll Up                     |  Swipe Down<br>Page Down    |
|  Swipe Left<br>Left Scrolling for MS Excel   |  Swipe Left<br>Alt + Tab    |
|  Swipe Right<br>Right Scrolling for MS Excel |  Swipe Right<br>Alt + Shift |
|  Tap<br>Toggle Functional Keyboard           |  Tap<br>Toggle Keyboard     |

Gestures may also be configured during an active session by opening the *Extended* menu and tapping *Configure Gestures*.

**NOTE** When opening AccessToGo 3.5 or later for the first time, a prompt may appear to select two-finger tap as the new Zoom feature. Click Yes to use the Zoom gesture



## Remote Desktop Session PPI (Pixel's Per Inch)

This Ericom patent pending feature lets the user choose the ideal PPI for their device. With the increasing diversity of end-user devices and user preferences, it is ever more important to allow the user to work with the most comfortable resolution when launching a remote application or desktop.

By default, the Recommended **PPI** for devices with screen sizes less than 7 inches is 190; and the PPI for screen sizes 7 inches or greater is 170. These settings will provide the optimal usage based on the device's screen size, however the user may also select a custom PPI value.



On devices with a lower resolution (e.g. 800x480) use a higher PPI to achieve more desktop space. The application or desktop will have a "zoomed-out" effect.

On devices with higher resolutions (e.g. 2560x1560) use a lower PPI to make the graphics and text more visible. The application or desktop will have a "zoomed-in" effect.

The default setting is 190 PPI.

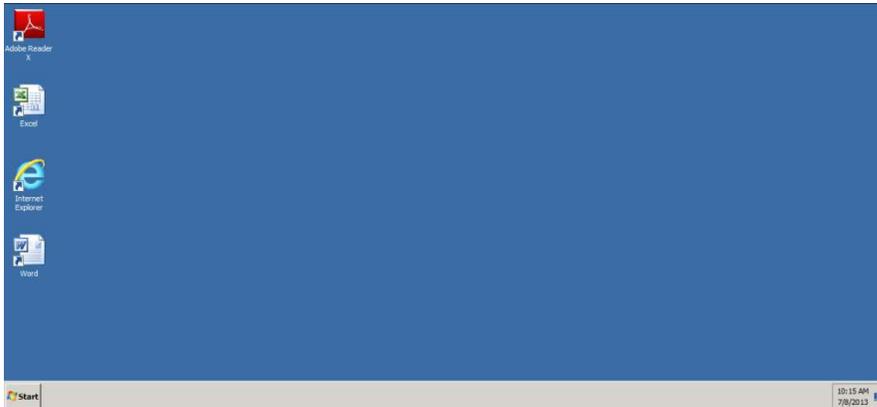
### Sample Screenshots

Test Device: Samsung 3S

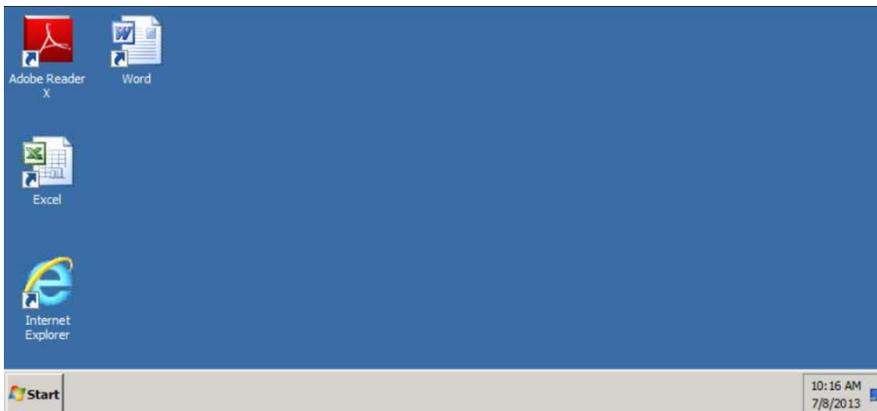
OS: Android

Native PPI: 304

When using the *Native* PPI, the remote desktop session will make use of the entire available resolution of the device. As seen in the first screenshot, the icon images and text may be too small for certain user's preferences.



In the second image, the PPI has been set to *190* so the icons and text are larger and easier to read. The session still makes use of the entire display area of the device; however, it uses fewer pixels per inch to display a lower resolution desktop.



## 9. URL SCHEMES

URL Schemes provides an easy method to launch preconfigured application and desktop sessions using AccessToGo. AccessToGo connections may be automatically launched by using the URL scheme "ericom" or "mrdp". For the full AccessToGo client use "ericom" as the URL scheme, and for sub-editions (Blaze, Connect, and WebConnect) use "mrdp". The syntax is the same for both.

When the user selects (or clicks) a .rdp or .blaze configuration file that is referenced by the URL scheme, AccessToGo will launch the session as configured in the settings file.

**NOTE** Clicking on a URL link while AccessToGo is already running will just switch to the AccessToGo application. In order to load the configuration defined in the link, AccessToGo must not be running when the URL is launched.

There are three methods to launch an AccessToGo session by using the URL scheme:

- 1) Using the URL scheme to launch a .rdp or .blaze file using HTTP/HTTPS (supported on iOS and Android).

Examples (replace "ericom" with "mrdp" if using a sub-edition):

```
<a href="ericom://http://www.test.com/myconnection.rdp">Connect to RDP Demo from WWW </a>
```

```
<a href="ericom://https://www.test.com/myconnection.blaze">Connect to Blaze Demo from WWW </a>
```

- 2) Using the URL scheme to launch a .rdp or .blaze file in the Ericom folder of the device (supported on Android only).

Example:

```
<a href="ericom://myconnection.rdp">Connect to RDP Demo from root folder </a>
```

- 3) Using the URL scheme to launch a .rdp or .blaze file from a subfolder on the device (supported on Android only).

Example:

```
<a href="ericom:///sdcard/myconnection.blaze">Connect to Blaze Demo from subfolder </a>
```

### Creating .rdp or .blaze files

The best method to create a .rdp or .blaze file for use with AccessToGo is to download the Ericom Blaze client from the Ericom website. Test the connection using the Blaze client, and then perform a *Save As* operation to save the settings into a configuration file. Refer

to the *Connection Parameter Definitions* table to manually configure any setting in the .rdp or .blaze file.

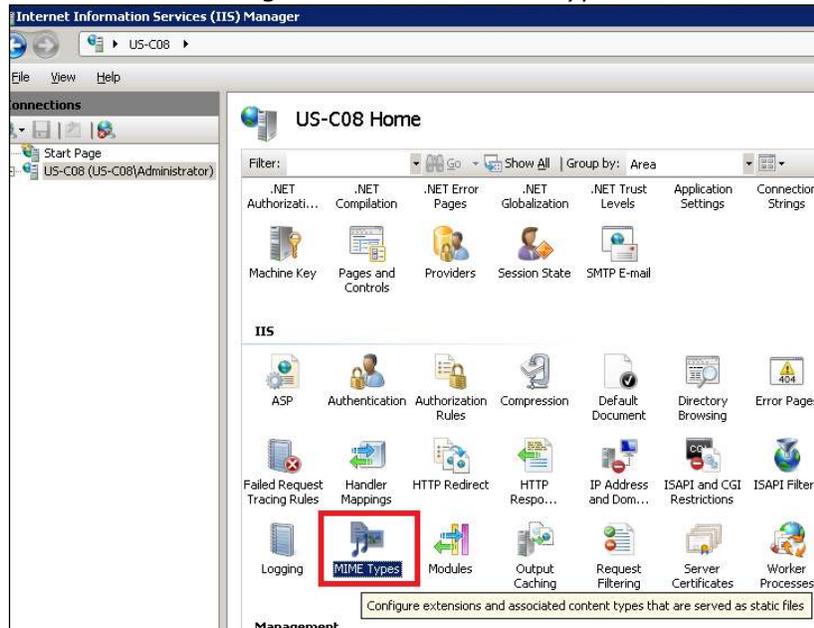
Prior to version 8.1, .rdp or .blaze files with saved passwords could not be transferred from one machine to another. This was a security mechanism to ensure that a .rdp or .blaze file was bound to the system that it was generated on.

Starting in 8.2, it is possible to create a 'generic' .rdp or .blaze file and use this on systems other than the origin. This is required to publish a .rdp or .blaze file with a saved password to be used for URL schemes. To create a generic file, launch blaze.exe with the **-generic-configuration** parameter. Then use blaze.exe to save the .rdp or .blaze file that will be used for the URL scheme.

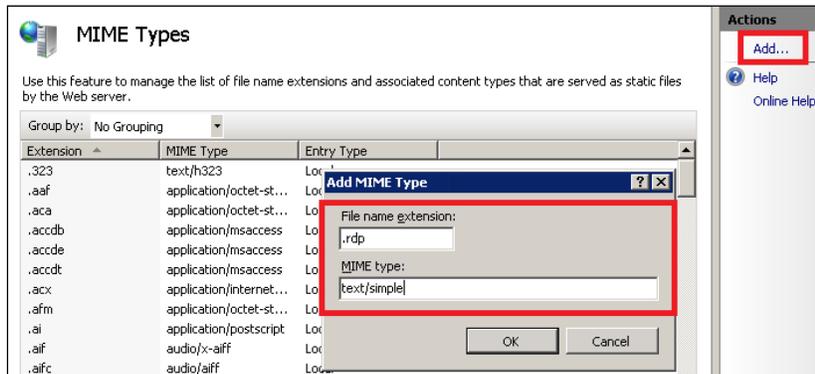
## Add MIME Type to Web Server

In order to use the AccessToGo URL Scheme, a MIME type must be added to a web server hosting the URL links. Here is an example of how to do this in Microsoft IIS 7:

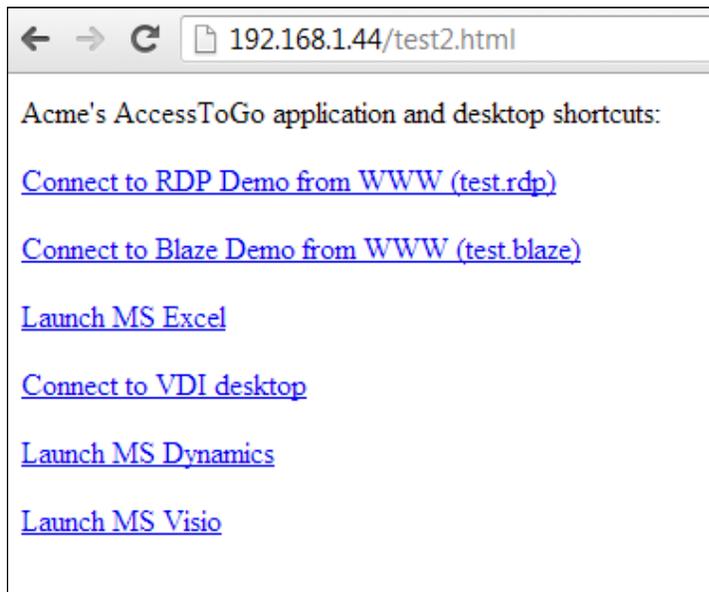
1. Go to the IIS Manager and launch *MIME Types*:



2. Click Action | *Add* and enter a new MIME Type:
  - a. File name extension: *.rdp*
  - b. MIME type: *text/simple*
  - c. Create another one for File name extension: *.blaze*



- Now use the device where AccessToGo is installed and use a browser to navigate to the web page with the configured link. Click the link and AccessToGo will automatically launch with the configured parameters:



## Configuration File Parameter Definitions

**NOTE** Some settings (e.g. Printing) are not used by AccessToGo

| Parameter       | Type | Default | Description   |
|-----------------|------|---------|---|
| alternate shell | s    | none    | Sets the shell used in the Terminal Services session. This can be used to set an alternate shell such as progman.exe or use it to set |

|                          |   |                            |   |
|--------------------------|---|----------------------------|---|
|                          |   |                            | the application which the user runs on logon to the Terminal Server.<br>Sample value: c:\temp\test.exe                                |
| audiomode                | i | 2 (Blaze)<br>0 (AccessNow) | 0, Bring to this computer<br>1, Leave at remote computer<br>2, Do not play  |
| auto connect             | i |                            | Not used  |
| autoreconnection enabled | i | 1                          | Attempts to reconnect when connection drops   |
| bitmapcachepersistenable | i |                            | Not used  |
| connect to console       | i | 0                          | 0, connect to a virtual session<br>1, connect to the console session  |
| desktopheight            | i | 600                        | height of session desktop in pixels   |
| desktopwidth             | i | 800                        | width of session desktop in pixels  |
| disable cursor setting   | i |                            | Not used  |
| disable full window drag | i | 0, Blaze<br>1, AccessNow   | 1, disables display of window contents while dragging in session  |
| disable menu animation   | i | 0                          | 1, disables menu animations in session  |
| disable themes           | i | 0                          | 1, disables use of themes in session  |
| disable wallpaper        | i | 0                          | 1, disables display of wallpaper in session   |
| displayconnectionbar     | i | 1                          | 1, displays the connection bar in a full-screen session   |
| domain                   | s |                            | Not used  |
| full address             | s |                            | IP address/name of server (and optional port value)<br>Sample value: 192.168.1.1:3389   |
| keyboardhook             | i | 2                          | For applying standard Windows key combinations<br>0, On the local computer<br>1, On the remote computer<br>2, In fullscreen mode only |
| maximizeshell            | i |                            | Not used  |

|                         |   |      |   |
|-------------------------|---|------|---|
| password 51             | b |      | Not used  |
| port                    | i | 3389 | Not used  |
| redirectcomports        | i |      | Not used  |
| redirectdrives          | i |      | Not used, see "drivestoredirect:s:" instead   |
| redirectprinters        | i | 0    | 0, don't redirect<br>1, redirects client printers in session<br>2, redirect with blaze universal printer driver |
| redirectsmartcards      | i | 0    | 1, redirects client smart cards in session (.NET only). Currently in Linux version only.                        |
| screen mode id          | i | 2    | 1, window<br>2, Full screen   |
| server port             | i |      | Not used  |
| session bpp             | i | 32   | all options are supported: 8,15,16,24,32  |
| shell working directory | s |      | Working directory if an alternate shell was specified.<br>Sample value: c:\temp\                                |
| smart sizing            | i |      | Not used  |
| username                | s |      | Username to be used for logon<br>Sample value: administrator  |
| winposstr               | s |      | Not used  |
| allow font smoothing    | i | 1    | 1, enabled font smoothing   |
| redirectclipboard       | i | 1    | 0, disabled<br>1, enabled   |
| prompt for credentials  | i | 0    | 0, disabled<br>1, enabled   |
| session sharing         | i | 1    | 0, disabled<br>1, enabled   |
| connection type         | i | 6    | 1, Modem  |

|                           |   |   |   |
|---------------------------|---|---|---|
|                           |   |   | 2, LowSpeed<br>3, Satellite<br>4, HighSpeed<br>5, WAN<br>6, LAN                   |
| drivestoredirect          | s |   | Drives to be redirected: Local disks (C:);CD-ROM / DVD Drive (D:)                 |
| dirstoredirect            | s |   | Folders to be redirected: "Desktop", "My Docs", (and "Media" on non-win)          |
| use multimon              | i | 0 | 0, current<br>1, use multi monitors<br>2, span multi monitors<br>#, use monitor # |
| remoteapplicationmode     | i | 1 | Not used  |
| allow desktop composition | i | 2 | Not used  |
| compression               | i |   | Not used  |
| disable cursor setting    | i |   | Not used  |
| bitmapcachepersistenable  | i |   | Not used  |
| redirectposdevices        | i |   | Not used  |
| authentication level      | i |   | Not used  |
| negotiate security layer  | i |   | Not used  |
| gatewayhostname           | s |   | Not used  |
| gatewayusagemethod        | i |   | Not used  |
| gatewaycredentialssource  | i |   | Not used  |
| gatewayprofileusagemethod | i |   | Not used  |
| promptcredentialonce      | i |   | Not used  |
| audiocapturemode          | i |   | Not used  |

|                             |   |    |  |
|-----------------------------|---|----|--|
| videoplaybackmode           | i |    | Not used   |
| use redirection server name | i |    | Not used   |
|                             |   |    |  |
| <b>Ericom Parameters</b>    |   |    |  |
| blaze version               | s |    | Version number<br>Sample value: 2.1                                      |
| blaze acceleration          | i | 1  | 0, disabled<br>1, enabled  |
| blaze image quality         | i | 40 | Blaze quality (100 – lossless, 95 – best, 75 – high, 20 – fair, 40 good) |
| Blaze password              | s |    | Encrypted password   |
| html password               | s |    | No encryption  |
| wc password                 | s |    | decrypt using CryptUnprotectData   |
| x password                  | s |    | decrypt using XTEA   |
| use ericom secure gateway   | i | 0  | 0, disabled<br>1, enabled  |
| use secure gateway creds    | l | 0  | 0, disabled<br>1, enabled  |
| ask secure gateway creds    | i | 0  | 0, disabled<br>1, enabled  |
| secure gateway hostname     | s |    | Ericom Secure Gateway address<br>Sample value: Test.abc.com              |
| timezone standard name      | s |    | for Mac and Linux  |
| timezone daylight name      | s |    | for Mac and Linux  |
| addins to use               | s |    | list of add-in component names to be used                                |
| ui language                 | s |    | Not Used   |

The following settings are used for the screenshot notification (iOS only) feature.

|                                      |   |   |  |
|--------------------------------------|---|---|--|
| atg screen capture notification      | i | 0 | (1 to enable, 0 to disable)<br>This enables/disables capture notification on iOS devices   |
| atg screen capture notification text | s |   | this is the text to display to the user after a screen capture was <i>detected</i> . It is not clear yet whether Japanese characters can be supported.   |
| atg screen capture url               | s |   | This is used as the initial part of the URL when doing the post. This allows the server side to include information for its own use in the URL. This is used EXACTLY as given when doing the POST so any URL character encoding must already be done beforehand. The names 'param1' and 'param2' can be anything (for example: time and address).<br>http://host:port/page?param1=value1&param2=value              |
| atg screen capture notification data | s |   | Parameter syntax: param1=val1&param2=val2<br>This is the data that will be sent in the body of the post message. By default, ATG appends local time and product details.<br>If this field is empty, then then the URL field is split such that the portion before the '?' is considered as part of the URL and the portion after the '?' is sent as the post data, acting as a placeholder for the data parameter. |

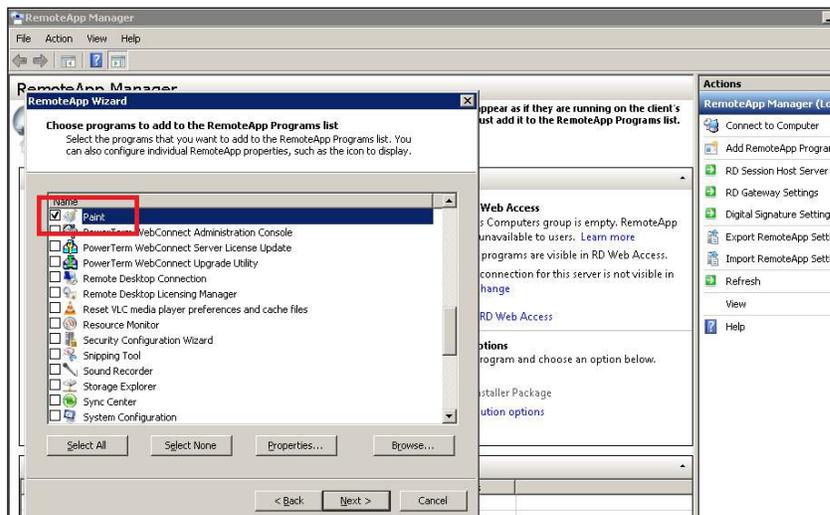
The following setting is used for the screenshot blocking (Android only) feature.

|                             |   |   |   |
|-----------------------------|---|---|---|
| atg screen capture blocking | i | 0 | (1 to enable, 0 to disable)<br>This enables/disables capture block on Android devices |
|-----------------------------|---|---|---|

## Launching Applications with URL Scheme

When using the URL Scheme to launch just an application from a Terminal Server/Remote Desktop Server, add the desired application(s) to the *RemoteApp Program* list.

The following image shows how to add MSPaint to the allowed application list:



In the .rdp or .blaze file, verify that the following parameters are configured:

- remoteapplicationmode:i:1
- alternate shell:s:mspaint
- (optional) shell working directory:s:

## Blocking Screenshots via URL Scheme (Android)

AccessToGo Android (8.1.2 or higher) supports the ability to block screenshot operations.

The enablement of the screenshot blocking is configured via the Blaze file. The Blaze file can be called by a URL Scheme to launch ATG client with the associated settings. The feature is configured using one setting in the Blaze or RDP file:

- atg screen capture blocking:i:1

When the user performs a standard screenshot operation in the AccessToGo (Android) application, a message will appear stating that the screenshot operation was blocked. This message is generated by the operating system and is not configurable.

## Notifying an Application of Screenshot (iOS)

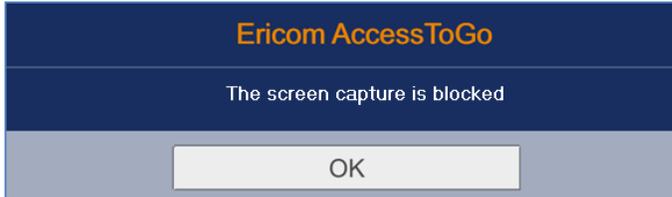
AccessToGo iOS (8.1.2 or higher) supports the sending of a notification to a webserver when a screenshot operation is taken. AccessToGo will send a notification using web POST to a server address and port with two available parameters (usually the time and address of the device). The URL syntax is (HTTPS or HTTP):

**https://host:port/page?param1=value1&param2=value**

The feature is configured using three settings in the Blaze or RDP file:

- atg screen capture notification:i:1
- atg screen capture notification text:s:
- atg screen capture [url:s](#):
- atg screen capture notification data:s:

When the user performs a standard screenshot operation in the AccessToGo (iOS) application, a message will appear with the text defined in "atg screen capture notification text". For example, this configuration: *atg screen capture notification text:s:The screenshot is blocked* will display this message when the user attempts to capture a screenshot.



## 10. TECHNICAL SUPPORT

### Release Notes

Starting in 9.2, release notes will be provided here.

Android Version 9.2: June 2019

Supports Android 9, 8, 7, 6 (24765)

Added "Up" arrow to the bottom bar (already exists in iOS version) so it can display the bar on devices that do not have a menu button (28291)

Ericom Connect edition: supports ability to deny the use of saved passwords (24416)

Removed demo connections (28293)

Discontinued VMware View support (29922)

Fixed issue with audio redirection (14112)

Fixed duplicate text in RADIUS message box (24371)

Fixed issue with display artifacts not refreshing properly (29402)

Fixed "Share" link

iOS Version 9.2: Coming soon

Ericom Connect edition: supports ability to deny the use of saved passwords

iOS v12 and higher: AccessToGo will automatically use the same language that is configured on the local device (functionality exists in Android version).

### Verify Connectivity

When experiencing connectivity problems - check that all firewalls between the AccessToGo application and RDP host are configured to allow the appropriate ports:

RDP: 3389

Blaze: 8080 (3399 in pre 3.x versions)

Secure Gateway: 443

To verify the connectivity of an address and port, download a Telnet app to the device and try connecting to the target address and port. If a *Connection Refused* message is returned, then the connection is not available.

## Not Compatible with Chromebooks

Certain Chromebooks supports Android applications. AccessToGo is not designed to run on Chromebooks, however this is on the roadmap. Contact Ericom sales and ask for the latest status from Product Management.

## URL Scheme is not working

If the URL Scheme launches AccessToGo, but does not connect using the configured parameters, check the following:

- AccessToGo was not already running
- The address of the RDP host configure in the RDP file (make sure that a DNS name can be correctly resolved on the device).
- Recreate the settings file (.rdp or .blaze) using the Ericom Blaze client (free download). This ensures that all parameters are defined correctly. Any typos will invalidate the file.

## Disable RDP SSL

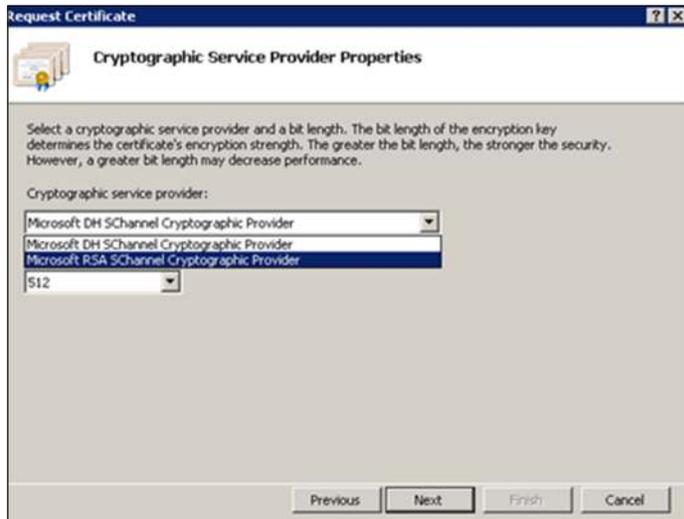
Access Server requires access to native RDP to be enabled on the RDP host. For this reason, do not change the *RDP Security Layer* to *SSL*. Leave the setting on *RDP Security Layer* and using the built-in AccessNow SSL encryption, or Secure Gateway, to add SSL encryption.



## SSL Certificate Error with PTWC and ESG

When using AccessToGo with the Ericom Secure Gateway (ESG) for Ericom Connect or PowerTerm WebConnect (PTWC) access, a trusted certificate is typically installed in the ESG. When requesting a trusted certificate from a third-party provider, a custom CSR must be sent to the provider.

To properly support AccessToGo, configure the following during the CSR creation. In the *Details* section of the Cryptographic Service Provider (CSR) - change the options for the *Private Key*. By default this is set to *Microsoft Strong Cryptographic Provider (Signature)*. Change this to *Microsoft RSA SChannel Cryptographic Provider (Encryption)*.



If the CSR not configured properly, there will be entries in the Event Viewer showing "The client and server cannot communicate, because they do not possess a common algorithm". When this error appears, a new certificate will have to be generated for the ESG.

## Tablet mode (Top bar) not available

AccessToGo considers a device a tablet when there is a 5.5" display. Older AccessToGo iOS versions enabled tablet mode when the device name was "ipad". Starting in v8.1.2 AccessToGo iOS enables tablet mode when there is a 5.5" (or greater) display present.

## Requesting Technical Support

To request technical support for AccessToGo, send the following information to [mobile@ericom.com](mailto:mobile@ericom.com)

- Description of problem
- Device type (i.e., Android)
- Operating System version (i.e., 6.x)
- Using Access Server on the RDP host?
- Number of users/devices affected by the problem?
- Contact Phone number

## ABOUT ERICOM

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

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](mailto: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](mailto: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](mailto:info@ericom.com)