

PowerTerm[®] WebConnect

Version 6.0

Administrator's Manual



Legal Notice

This manual is subject to the following conditions and restrictions:

This Administrator's Manual provides documentation for PowerTerm® WebConnect. Your specific product might include only a portion of the features documented in this manual.

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

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.

PTWC_AdminMan20190523

Copyright © 1999-2019 Ericom® Software.

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

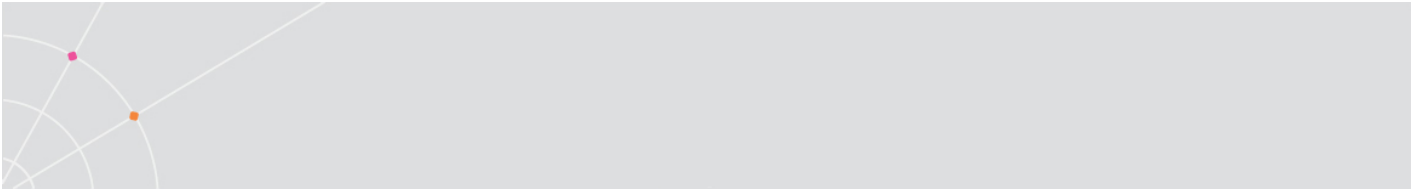
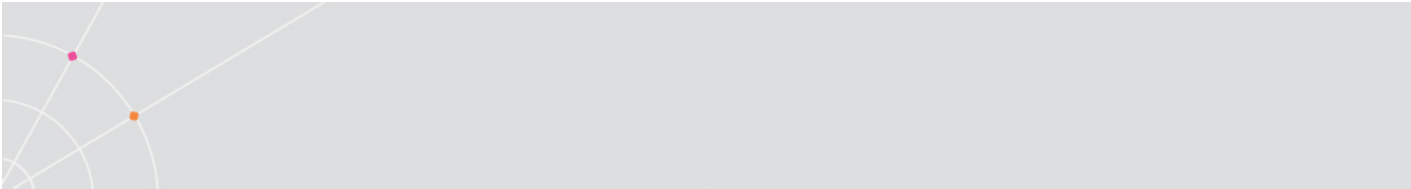
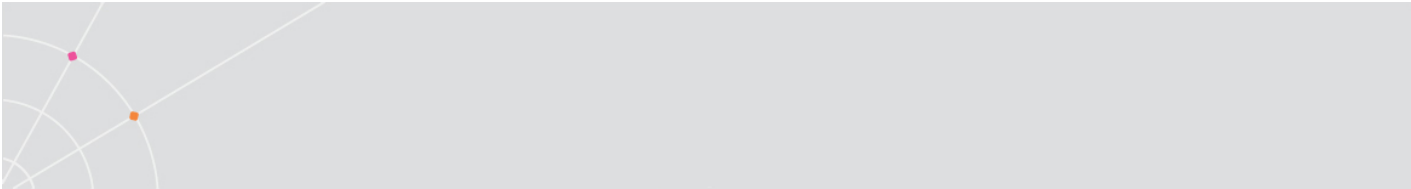


Table of Contents

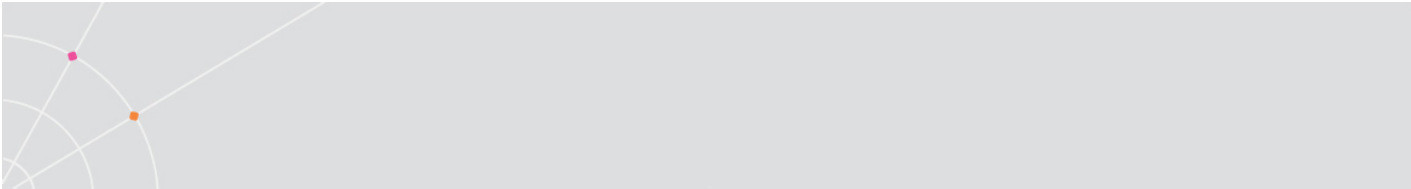
LEGAL NOTICE	2
ABOUT THIS DOCUMENT	8
1. INTRODUCTION	9
What is PowerTerm® WebConnect?	9
Application Publishing	9
End-User Client Components	9
Centralized management	10
AccessNow HTML5 Zero Download Client	10
Ericom Blaze RDP WAN Acceleration	10
Enhanced Connection Broker for VDI	10
2. GETTING STARTED	11
Preparing Windows 2008	11
Preparing Windows 2012	14
Installing the Ericom Secure Gateway	15
Terminal Server Preparation	19
Terminal Server Full Desktop or Application Deployment	22
Virtual Desktop (VDI) Connection Broker Deployment	23
Hardware-based PCoIP Connection Broker Deployment	23
3. POWERTERM WEBCONNECT SERVER	24
Installing PowerTerm WebConnect Server	24
Activating the Server	28
Starting and Stopping the PowerTerm WebConnect Windows Server	30
PowerTerm WebConnect Ports	30
High Availability	33
Using Failover Mode	36
Using Cluster Mode	36
High Availability Limitations	38
Local Server Mode and the Shadow Database	39
4. END-USER ACCESS CLIENTS	40
Application Portal Interface	41
Form Post SSO to the Application Portal	43
Application Zone for Windows	43
AccessPad	48
AccessToGo Mobile Client	50
AccessPortal	55
5. NATIVE CLIENT REMOTE DEPLOYMENT	57
The Downloader	58



6. NATIVE CLIENT INSTALLERS (MSI, PTSTART)	64
MSI/PKG Installation	64
Mobile Client App Stores	64
PtStart Downloader	64
7. CUSTOMIZING CLIENT PARAMETERS	70
Automatic Server Discovery	77
8. POWERTERM WEBCONNECT APPLICATION PORTAL	79
Application Portal Configuration	80
9. ADMINISTRATION TOOL	88
Launching the Administration Tool	88
Administration Console Interface	89
Modifying the View Pane	90
Useful Functions	92
Administration Console Parameters	94
10. DIRECTORY SERVICES	95
Administration Console Connection Process	95
Connecting to Directory Services	96
11. UNDERSTANDING USERS, GROUPS, AND CONNECTIONS	101
PowerTerm User Object Properties	104
Connection Object	110
Group Objects	110
Implementing Access Policy	118
12. DEPLOYING APPLICATIONS AND DESKTOPS WITH TERMINAL SERVICES	120
Overview	120
Publishing	129
Microsoft App-V Integration	147
Copy a connection based on an existing one:	153
Publishing Applications/Desktops from a Citrix XenApp Server	154
13. CONFIGURING POWERTERM LOAD BALANCER	157
PowerTerm Load Balancer Server	159
PowerTerm Load Balancer Agent	161
PowerTerm Load Balancer Administration Tool	162
Optimizing the Load Balancer	166
14. DEPLOYING DESKTOPS WITH VDI	170
Definitions	170
The VDI Connection Process	171
Getting Started with PowerTerm WebConnect	171



Installation	172
Preparing Virtual Desktops	172
Connection Broker Administration Tool	175
Using Pools	192
Auto Resizing Pools	194
Virtual Desktop Assignment Options	196
Creating a Simple VDI Implementation.....	197
Creating a Remote PC Access Solution	198
Creating an Enomaly Cloud	200
Connecting from WYSE ThinOS.....	201
DeskView Failover	203
Using the Built-In FTP Server	206
Troubleshooting	207
15. CREATING A PC-OVER-IP BROKER	209
Administering PCoIP Devices	213
RADIUS for PCoIP Devices	216
16. ENHANCEMENTS FOR TS AND VDI	218
Ericom AccessNow and Blaze	218
AccessNow and Blaze Client Configuration	220
Single Sign-on from Workstation	220
Built-in Login Scripting	221
17. UNIVERSAL PRINTING	223
Introduction	223
AccessNow and Blaze Printer on Windows 8 and 2012.....	225
Using Ericom Blaze Printing on Windows.....	225
Using Ericom AccessNow Printing.....	227
Universal Printing with Windows 8 or 2012 RDP Hosts.....	228
Using AccessNow Printer in HP Universal PS Mode.....	228
Using Net2Printer with PowerTerm WebConnect.....	229
Using triCerat ScrewDrivers with PowerTerm WebConnect	236
Using Microsoft Easy Print with PowerTerm WebConnect (RDP Only)	240
Selecting the Default Printer	240
18. ERICOM SECURE GATEWAY (ESG)	242
Disabling HTTP/HTTPS content filtering	242
PowerTerm WebConnect Configuration	243
Authentication Server.....	248
19. TERMINAL EMULATION WITH HOSTVIEW	253
Introduction	253
Configuring Legacy Connections	253
PowerTerm WebConnect HostView Settings	256
21. IMPROVING PERFORMANCE	266
Using a Dedicated Server	266



- Memory Resources 266
- Alternate Connection Points 267
- Best Practices for a Healthy Environment 267

- 22. IMPLEMENTING ACCESS SECURITY269**
 - Encrypting with SSL 269
 - Enabling FIPS Compliancy in RDP 272
 - Secure Access Based on Subnet 274
 - Deny access outside of a specified subnet..... 275

- 23. JUNIPER® SSL VPN INTEGRATION.....277**
 - General Portal Configuration 277
 - Form POST Single Sign-On with Portal..... 279
 - Set Ericom Portal Page as the Default 280
 - AccessNow HTML5 with Rewriter (Client-less) 280
 - Network Connect Usage (All Clients) 280
 - Set ActiveX Rewriting Parameter (Native Windows Downloader)..... 281
 - JSAM Configuration (Native Clients) 281
 - WSAM Configuration (Native Windows Client)..... 283
 - Application Portal Icons Fix..... 285

- 24. MONITORING AND AUDIT TRAILS286**
 - Monitoring Online Activity 286

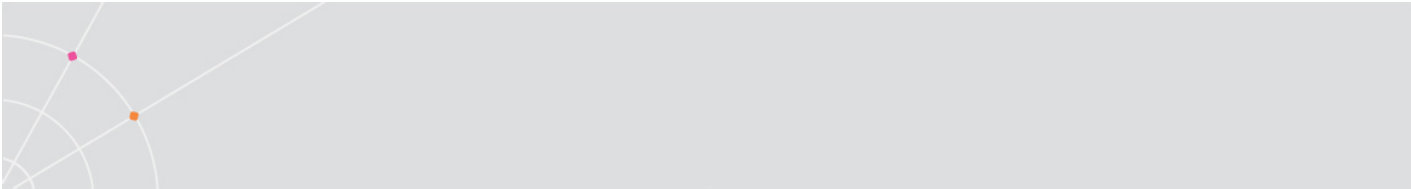
- 25. RECONNECT FEATURES293**
 - Application Zone Reconnect 293
 - Session Reconnect 294
 - Blaze Reconnect 295
 - Network Reconnect..... 295

- 26. UPGRADE INSTRUCTIONS299**
 - Uninstall the Current Installation 300
 - Backup the Previous Installation..... 300
 - Import after new installation 300
 - Upgrading Terminal Server Components 301
 - Updating the AccessNow Folder on Web Server 302
 - Updating the Native Clients on the Broker..... 302
 - Applying Windows Updates/Patches 302

- 27. CUSTOMIZATIONS.....305**

- 28. APPENDIX A – ENVIRONMENT VARIABLES308**

- 29. APPENDIX B – ADMINISTRATION CONSOLE315**
 - Information Panes 319
 - Properties Dialogs..... 328



30. APPENDIX C – TECHNICAL SUPPORT	345
WebConnect Troubleshooting Guide.....	345
Authentication Server Troubleshooting Guide	346
ESG Failover Log Verification.....	346
Requesting Technical Assistance	346
Technical Support Debug Logs.....	347
31. APPENDIX D - TERMINAL SERVER TIPS.....	350
ABOUT ERICOM.....	354



ABOUT THIS DOCUMENT

This guide assumes that the PowerTerm WebConnect administrator will be familiar with:

- Microsoft® Terminal Server or Citrix® XenApp management
- Intermediate networking knowledge
- Basic web server administration knowledge

Some features documented in this guide may not be available in the edition of PowerTerm WebConnect that you are using, for example, the DeskView line does not include seamless applications. There is no index provided in this document. The most effective method to find specific content is to use the find or search feature of the viewer that is being used to browse this document. Enter relevant keyword(s) into the search function and browse through the results.

Certain chapters will have pertinent configuration information for 64-bit (x64) operating systems. If an x64 platform will be used, be sure to search through this document using the keyword *x64* to find all relevant information.

All titles, labels, and names (such as product names, features, and functions) will be displayed using *italics*.

Useful descriptions, hints, and warnings will be bordered with a box.

Important terminology used in this document:

- Terminal Server (or Remote Desktop Server) – an operating system that can receive RDP requests from multiple users. This is usually Windows 2003, 2008, 2008 R2, or 2012
- Host (or RDP Host) – a remote system performing the computing. This can be a Microsoft Terminal Server or a workstation OS such as Windows 7
- VDI – Virtual Desktop Infrastructure
- RDP – Remote Desktop Protocol
- PTWC – PowerTerm WebConnect
- RemoteView – Native component used to access published applications and/or desktops
- AccessNow – HTML5 based component used to access published applications and/or desktops
- AccessNow – Native mobile app



1. INTRODUCTION

What is PowerTerm® WebConnect?

Ericom's PowerTerm WebConnect is a Connection Broker for managing access for various types of hosting platforms. Such platforms include Remote Desktop Session Hosts (Terminal Services), Virtual Desktop Infrastructure (VDI) and Legacy Systems. PowerTerm WebConnect enables IT administrators to get the most out of their Terminal Servers and VDI environments with minimal effort, while reducing complexity in managing access to applications, desktops and documents.

Users can utilize PowerTerm WebConnect to connect to applications, desktops and documents from a wide range of client devices including Windows®, Linux, and Mac OS X, tablets, smartphones, Chromebooks and various thin-client devices. In addition, PowerTerm WebConnect provides secure, encrypted connections for both internal and external access.

Application Publishing

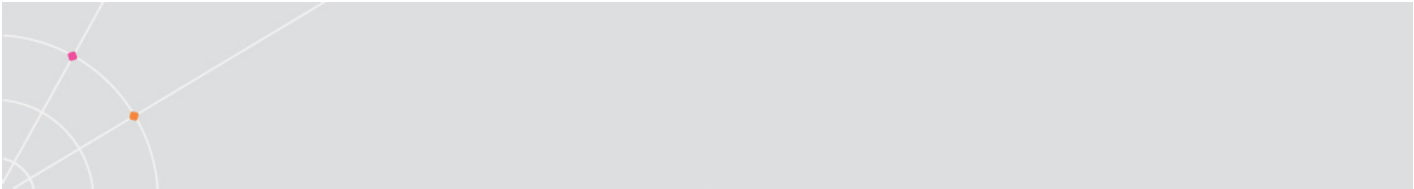
PowerTerm WebConnect enables remote access to applications and content by any authorized user. These are viewed as seamless windows, where the remote applications are fully integrated into the local desktop; thus local and remote applications look and behave similarly. PowerTerm WebConnect supports both *Microsoft Seamless* and *Ericom True Seamless* seamless windows functionality. Microsoft Seamless functionality is only available on Microsoft clients that support it natively.

The Administrator configures the published application's set of owners, the published application's location (locally on the client's machine or remotely on the Terminal server), and the location of the published application's icon (Desktop, Application Zone, and/or Start menu).

End-User Client Components

PowerTerm WebConnect includes several clients that are used with various back-end systems:

- *RemoteView* and *AccessPad* are native clients used for accessing Windows based applications and desktops. This is also used for *Blaze* enabled sessions.
- *AccessNow* is used for accessing Windows based applications and desktops using HTML5 browsers

- 
- *AccessToGo* is a native mobile client used for accessing Windows based applications and desktops. This is also used for *Blaze* enabled sessions.
 - *HostView* is used for accessing character-based applications running on legacy systems such as IBM Mainframe, Linux, etc.

NOTE A basic workstation or thin client is the sufficient to run the native client or AccessNow HTML5 client. By using a repurposed PC or thin client device, additional cost savings can be achieved with PowerTerm WebConnect.

Centralized management

PowerTerm WebConnect includes an administration console that can be used to tailor application usage for different types of end-users. All settings are saved onto a central and redundant platform for robust application and desktop delivery.

AccessNow HTML5 Zero Download Client

Ericom AccessNow is supported with the web-based Application Portal. This technology provides access to Chromebooks and devices that have an HTML5 browser. Refer to the AccessNow User manual for details on this technology.

Ericom Blaze RDP WAN Acceleration

Ericom Blaze provides end-users with an enhanced remote computing experience on most networks: WAN, LAN, Broadband, and air cards. This is achieved by accelerating and compressing Microsoft Remote Desktop Protocol (RDP). The results are higher frame rates, improved response times, and smoother screen updates.

Enhanced Connection Broker for VDI

PowerTerm WebConnect DeskView Connection Broker provides the following features for implementing a VDI based solution:

- *Linked Cloning* reduces virtual desktop storage requirements.
- *Auto-sizing Pools* ensures that an optimal amount of virtual desktops are running. New virtual desktops are created based on user demand. Extra virtual machines are deleted automatically making better use of server resources.
- *Availability Restriction Control* limits access to virtual desktops on pre-determined times of the day.

2. GETTING STARTED

This manual covers many different features included with PowerTerm WebConnect. To help you get started, the sections in this chapter will cover prerequisites, basic instructions, and direct you where to go for further instructions. You may find yourself coming back to a different section in this chapter for help on getting started with a different feature.

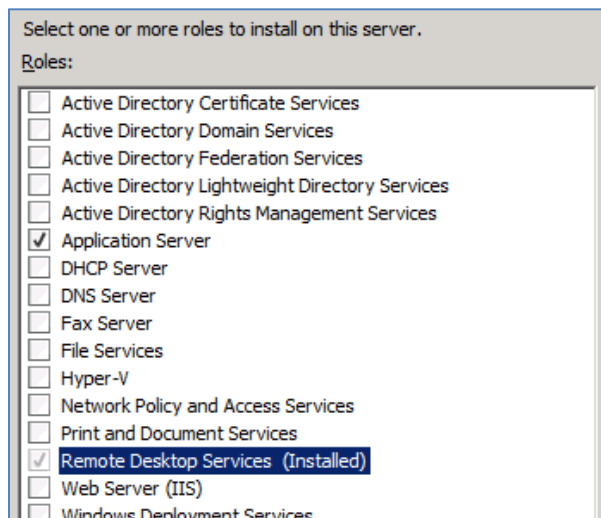
The following features of PowerTerm WebConnect have their own dedicated manuals for those looking for more in depth documentation. Each of these features are available as a Standalone version as well – fully functional without the PowerTerm WebConnect connection broker.

- Ericom AccessNow
- Ericom AccessToGo
- Ericom Blaze
- Ericom Secure Gateway

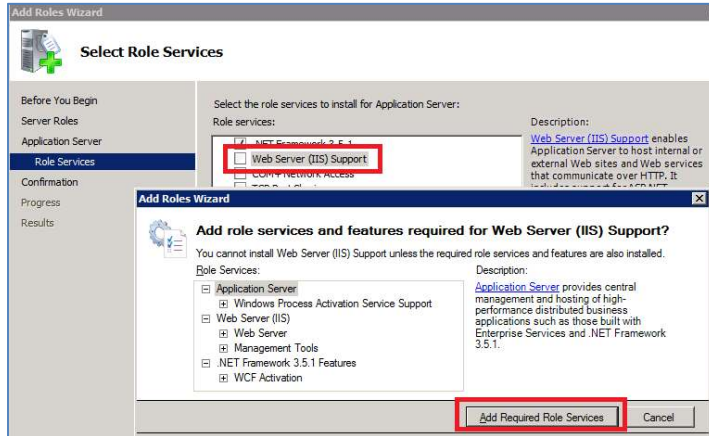
Preparing Windows 2008

This section will cover pre-requisites and help you get started with installing PowerTerm WebConnect on a Windows 2008R2 Server.

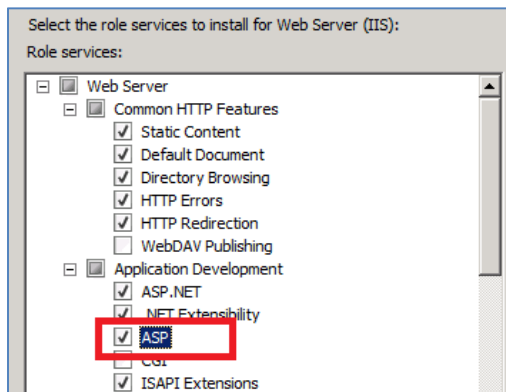
Enable the following Server roles: *Application Server*



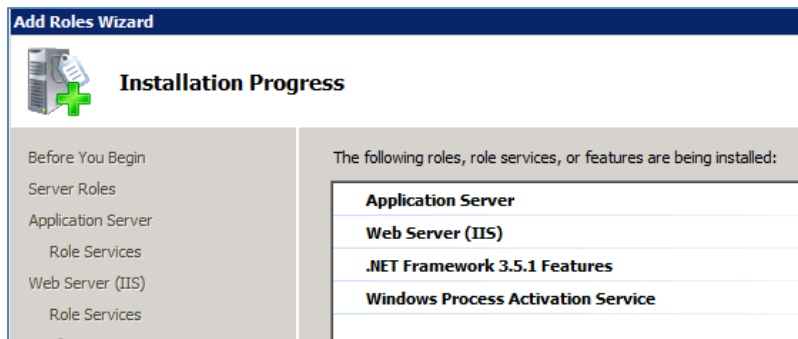
While adding the Application Server Role, check *Web Server (IIS Support)* and then click *Add Required Role Services*.



When prompted to select IIS features, check ASP.

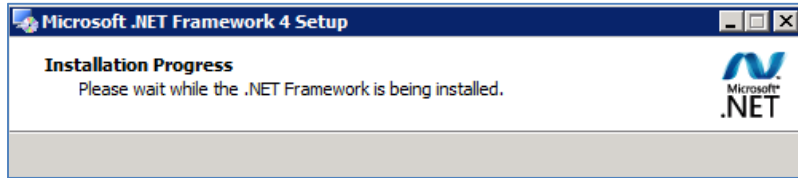


Continue through the wizard and complete the installation.



At the end of the installation, if a reboot prompt appears, reboot the server.

Next, install *.Net 4 Full* on the server. The installer may be downloaded for free from Microsoft. Ericom support can also direct you to the download link.



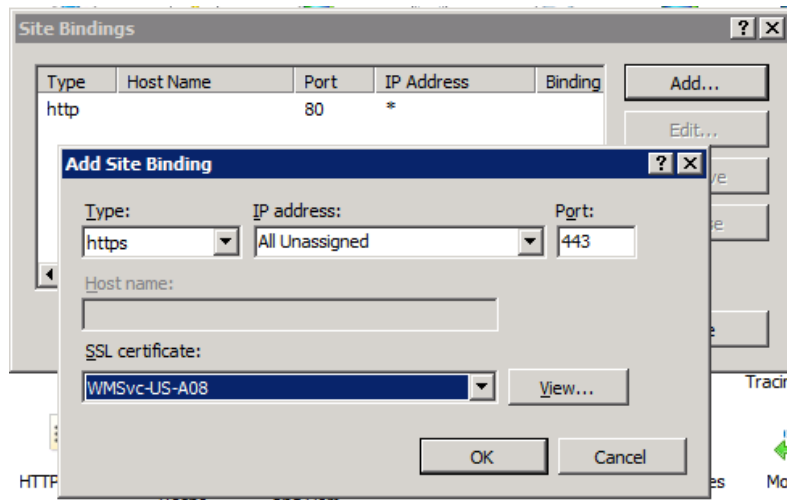
Once .Net 4 is installed, configure IIS for HTTPS (this may also be performed after the PowerTerm WebConnect application is installed).

Go to IIS and enable HTTPS on port 443. This is required for AccessToGo support.

Go to the "Web Site" where AccessToGo will be installed (usually *Default Web Site*) and click on *Bindings...*

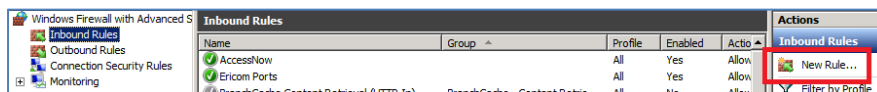


Click *Add* and change the type to *https*. Choose an SSL certificate from the drop down list (one must be selected).

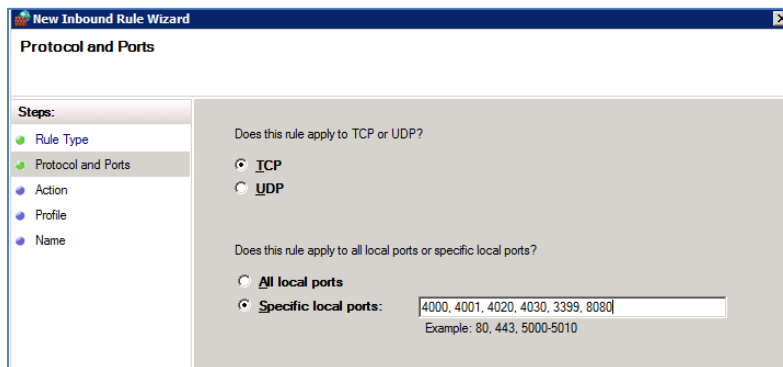


Click *OK* to complete the configuration and now IIS will be enabled with HTTPS as well.

Configure the Windows firewall with the appropriate Ericom ports. Create a new *Inbound Rule* for ports 4000, 4001, 4010, 4030, 8080. If the DeskView VDI broker will be used, add the VDI Ericom Tools agent port 4045.



Name the new rule *Ericom Ports*. The RDP port (3389) should already be configured) on the Firewall. Configure any network firewalls to allow the Ericom ports through to the server.



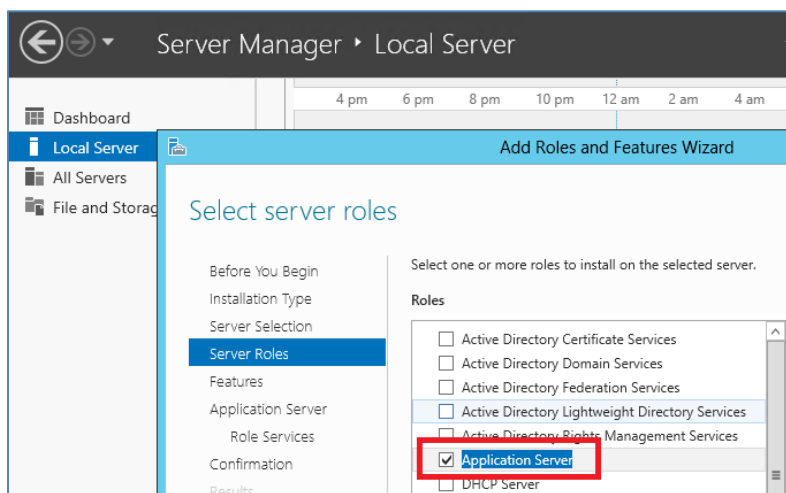
Continue to **Chapter 3** for instructions on how to install and activate PowerTerm WebConnect. The installation usually takes 15-30 minutes.

Return to this Getting Started Chapter to learn about using the Ericom Secure Gateway, Preparing the Terminal Server, and publishing applications and desktops.

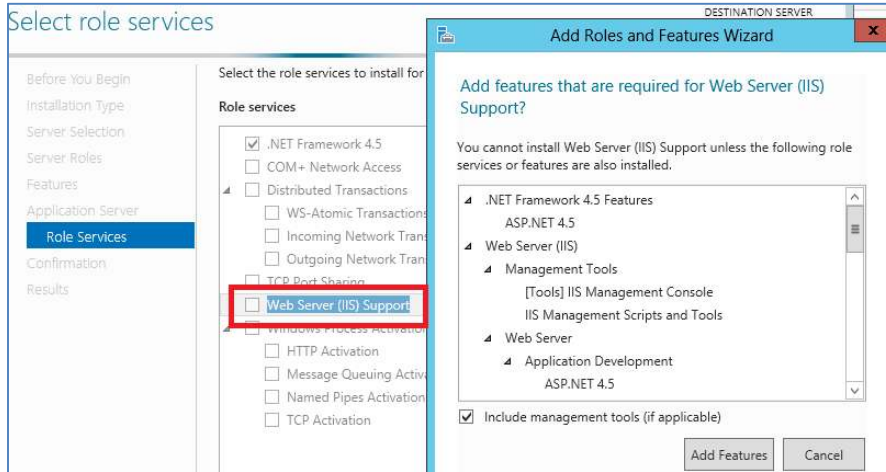
Preparing Windows 2012

This section will cover pre-requisites and help you get started with installing PowerTerm WebConnect on a Windows 2012 Server.

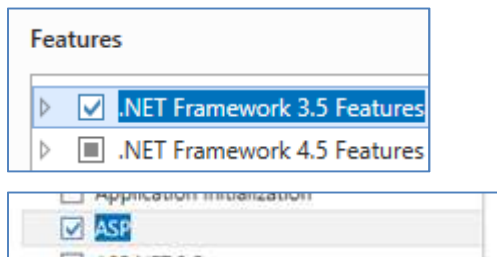
Enable the following Server roles: *Application Server*



While adding the Application Server Role, check *Web Server (IIS Support)* and then click *Add Required Role Services*.

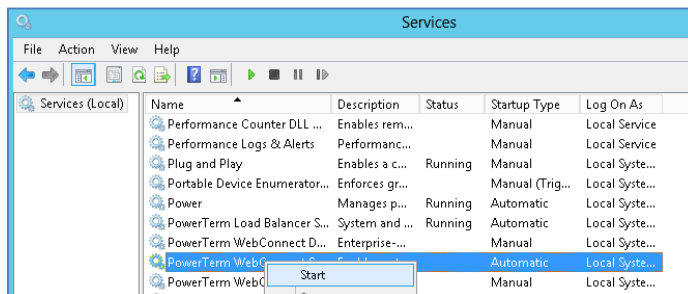


When prompted to select IIS features, check *.NET Extensibility 3.5* and *ASP*.



At the end of the installation, if a reboot prompt appears, reboot the server.

After the installation of PowerTerm WebConnect, the PowerTerm WebConnect Server service may need to be started manually the first time.



Installing the Ericom Secure Gateway

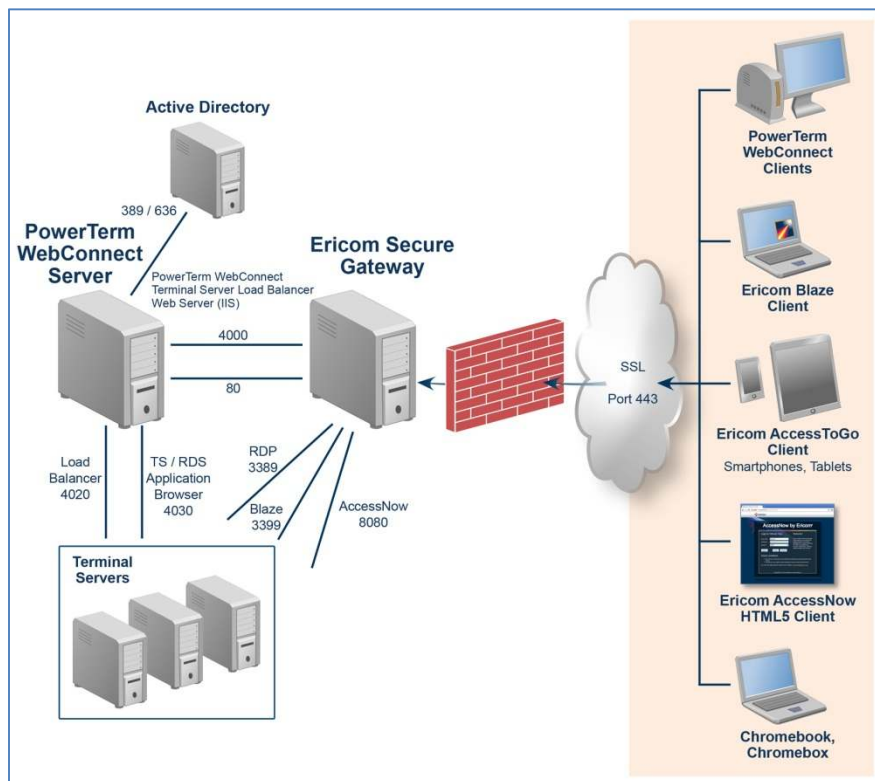
PowerTerm WebConnect includes a Secure Gateway to manage and proxy access between internal Ericom servers and remote end-users. The Secure Gateway is typically installed in the DMZ and acts as a single port relay proxy for all PowerTerm WebConnect related communication. This means that only one port needs to be opened on the external firewall. The Secure Gateway will securely tunnel all related communication through its port: PowerTerm

WebConnect (4000), RDP (3389), AccessNow/Blaze (8080), HTTP (80), HTTPS (443), emulation (80), SSH (22), and more.

The Secure Gateway server is typically installed in the DMZ, whereas the PowerTerm WebConnect server is installed on the LAN.

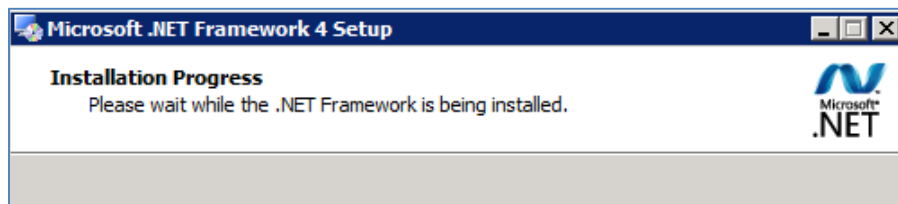
Each Secure Gateway can only be configured for one PowerTerm WebConnect broker server. In a clustered environment with multiple broker servers, add additional Secure Gateway servers to provide redundancy.

The following diagram illustrates the communication flow from users at remote connections to the PowerTerm WebConnect environment using the Ericom Secure Gateway.



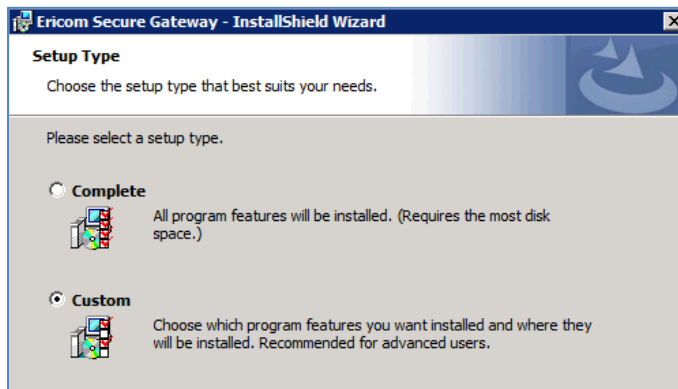
Installation and Configuration

Install *.Net 4 Full* on the server that will run the Secure Gateway.

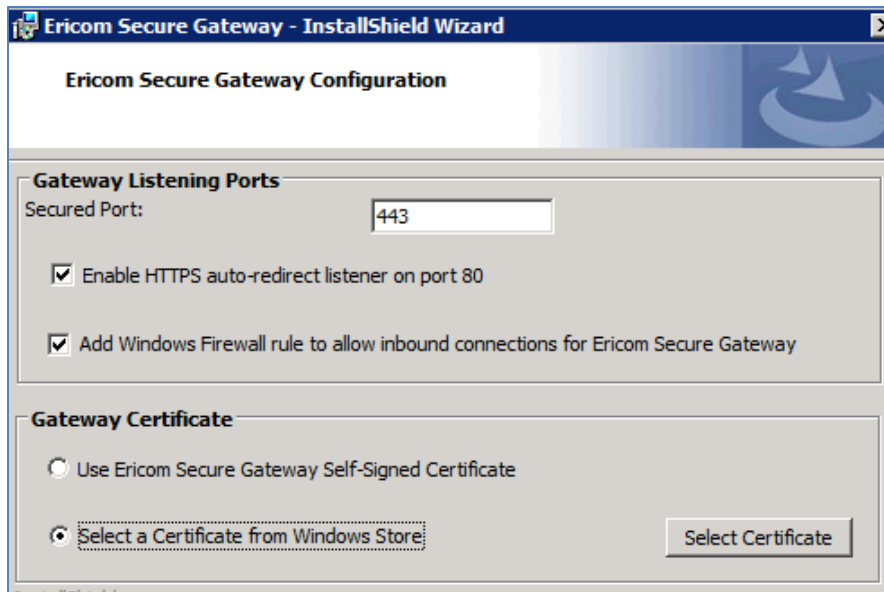


Once .Net 4 is installed, download and install the Ericom Secure Gateway using the MSI installer. The MSI installer is included with the PowerTerm WebConnect install under the *AddOns* folder: *C:\Program Files (x86)\Ericom Software\WebConnect x.y\AddOns\SecureGatewayEricomSecureGateway.exe*

When prompted for the *Setup Type*, select *Custom*. When PowerTerm WebConnect is in use, the *Secure Gateway's Authentication Server* optional and needed if two-factor authentication is required. This is only required if standalone clients (such as the Blaze client) will be used in the environment as well).



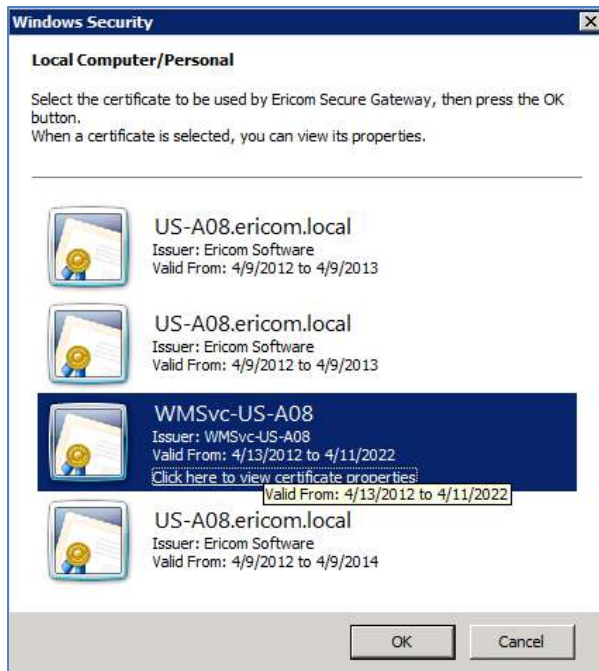
Next, select the port that the Secure Gateway will listen over. In most cases use the default value of 443.



The Secure Gateway includes a built-in web server to host various Ericom client pages, such as AccessNow Standalone). The web server will always operate over the Secure Gateway port. The Secure Gateway will

automatically redirect HTTP requests (over port 80) to HTTPS when the *Enable HTTPS auto-redirect* setting is checked.

To use a trusted certificate with the Secure Gateway, click *Select Certificate*. All available certificates in the Local Computer | Personal store will be displayed. Select the desired certificate for use with the Secure Gateway.



At the Connection broker selection dialog, check *PowerTerm WebConnect*.

The Secure Gateway has a security feature to only allow requests using a connection broker and to deny all requests from standalone clients. To enable this, check: *Only allow connections from a connection broker. Deny connections from standalone clients.*



At the PowerTerm WebConnect Configuration dialog, enter the address of the PowerTerm WebConnect server that will be accessible from the Secure Gateway.

PowerTerm WebConnect Server Configuration

WebConnect Server

Address: Port:

Reminder: Configure PowerTerm WebConnect Server Configuration with the address and port of this Secure Gateway

Ericom Web Server Proxy Configuration

Ericom Secure Gateway can act as an HTTP Proxy to Ericom Web Server Components

Address: Port:

HTTP
 HTTPS

Once the Secure Gateway has been installed and configured, continue to **Chapter 18** for instructions on how to configure PowerTerm WebConnect to use the Secure Gateway. The additional steps that are required to complete the configuration consist of:

- Configure three environment variables in the PowerTerm WebConnect Administration console to enable the Secure Gateway.
- Configure Application Zone, Application Portal and AccessToGo clients that will be used externally to point to the Secure Gateway for the PowerTerm WebConnect address. The Secure Gateway acts as a proxy to the broker server. A set of files to be configured for external use is present in the *web* folder and all start with "sg".

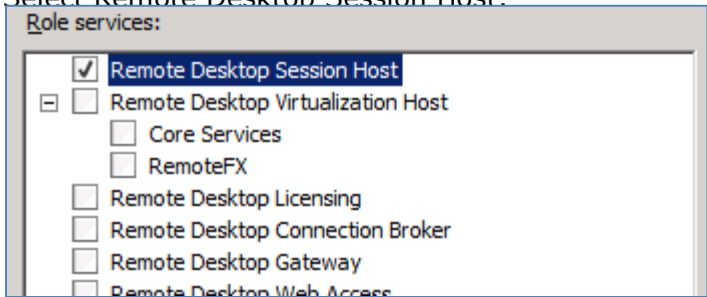
Terminal Server Preparation

Perform the following steps to enable Remote Desktop Services and prepare the server for use with PowerTerm WebConnect.

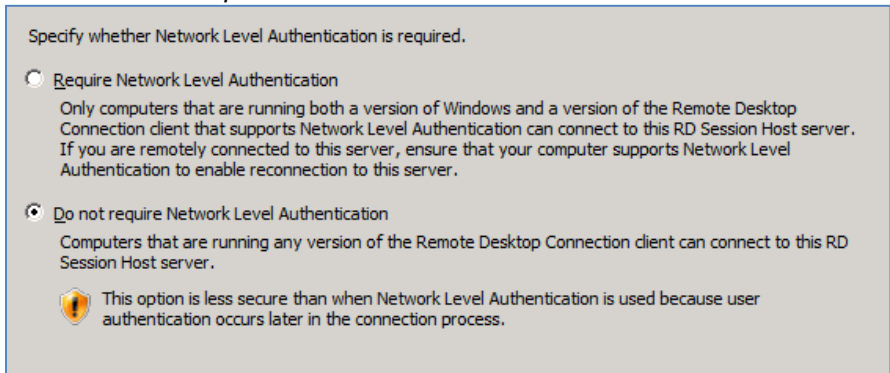
Go to the Server Manager and add the Remote Desktop Services role.

Print and Document Services
 Remote Desktop Services
 Web Server (IIS)

Select Remote Desktop Session Host:

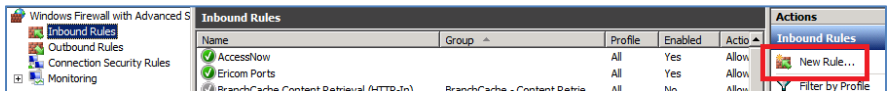


When prompted to configure Network Level Authentication in the role wizard, select *Do not require network Level Authentication*.



Continue through the rest of the wizard and reboot the server when prompted.

Configure the Terminal Server Windows firewall with the appropriate Ericom ports. Create a new Inbound Rule for ports 8080, 4020, 4030.



Name the new rule *Ericom TS Ports*. The RDP port (3389) should already be configured) on the Firewall. Configure any network firewalls to allow the Ericom ports through to the Terminal Server(s).

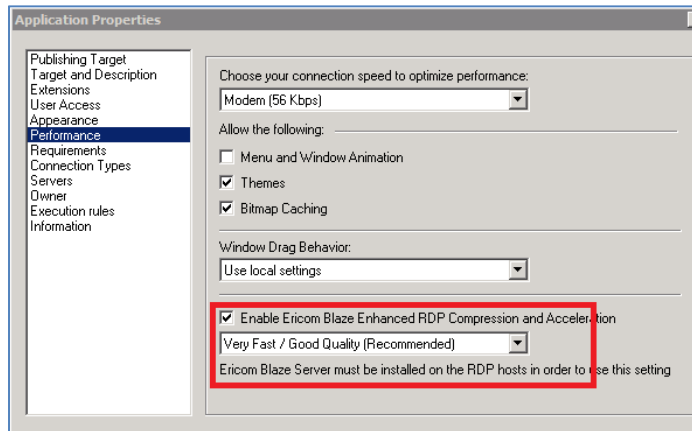


Install the Ericom **Access Server** services on Terminal Servers

All Ericom Terminal Server components can be found in the *AddOns* folder.

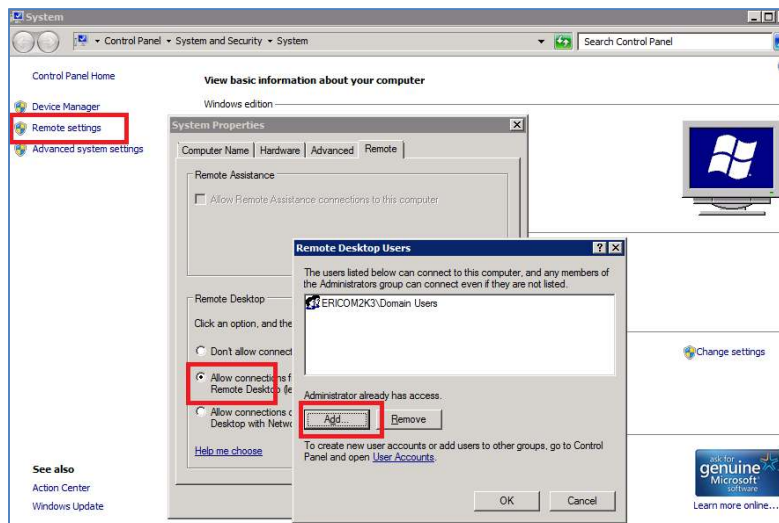
- *Access Server* – this must be installed on all Terminal Servers that will accept connections from clients using an HTML5 web browser or Blaze enabled connection

When publishing an application or desktop with *RDP Compression and Acceleration* enabled, *Access Server* must be available.



Next, install third-party applications that will be published through PowerTerm WebConnect.

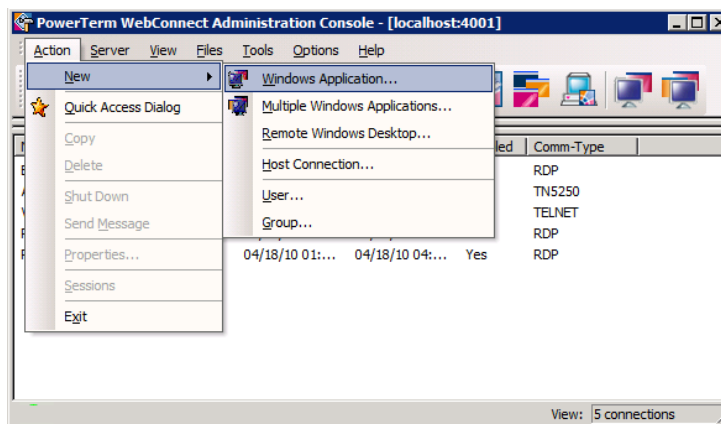
Remember to configure *Remote Settings* on Terminal Servers to allow users to be able to RDP into the Terminal Server.



Terminal Server Full Desktop or Application Deployment

PowerTerm WebConnect can serve as a connection broker for applications and desktops session on Windows Terminal Servers and Remote Desktop Servers (TS/RDS). Protocols that are available for TS/RDS deployments are AccessNow, RDP, and Blaze.

Once the Terminal Servers are prepared and the PowerTerm WebConnect broker is installed, publish desired applications and desktops and assign them to the Active Directory users and groups.



To deploy a TS/RDS connection broker, focus on these chapters:

- 9 – Administration Console – explains in detail how to use the Server Administration Console.
- 12 – Deploying Applications and Desktops – covers the steps required to publish applications and desktops. If Blaze will be used for RDP acceleration, remember to install Access Server on each Terminal Server.
- 13 – Load Balancer Configuration – explains how to configure and administer the Load Balancer for efficient Terminal Server usage.
- 16 – Enhancement features – covers enhancement features in more detail (i.e., Ericom Blaze).
- 17 – Printing – covers Universal Printing options and tips for standard RDP printing
- 4, 5 – PowerTerm WebConnect Clients – covers how to connect to applications and desktops using PowerTerm WebConnect.



Virtual Desktop (VDI) Connection Broker Deployment

PowerTerm WebConnect can serve as a connection broker for virtual desktops. Connections between end users and the virtual desktop environment are managed and secured by PowerTerm WebConnect. Protocols that are available for VDI deployments are AccessNow, RDP, and Blaze. To deploy a VDI connection broker, focus on these chapters:

NOTE It is recommended to read all the chapters covering Terminal Server deployment even for VDI deployments.
--

- 9 – Administration Console – explains in detail how to use the Server Administration Console.
- 14 – Deploying Desktops with VDI – instructions on how to configure the connection broker to manage access to VDI desktops.
- 16 – Enhancement features – covers enhancement features in more detail (i.e., Ericom Blaze).
- 17 – Printing – covers Universal Printing options and tips for standard RDP printing.
- 4, 5 – PowerTerm WebConnect Clients – covers how to connect to applications and desktops using PowerTerm WebConnect.

Hardware-based PCoIP Connection Broker Deployment

PowerTerm WebConnect can serve as a connection broker for hardware-based PCoIP devices. Connections between end users and the PCoIP host hardware are managed and secured by PowerTerm WebConnect. When an end-user connects from a PCoIP client (also known as a puck or portal), the PCoIP protocol will be used. When the end-user connects from a device that does not support PCoIP, RDP or Blaze protocol will be used. To deploy a PCoIP connection broker, focus on these chapters:

- 14 – Deploying Desktops with VDI – explains how to deploy virtual desktops from hosts such as VMware ESX and Microsoft Hyper-V.
- 15 – Creating a PCoIP Connection Broker – this chapter focuses on the using PowerTerm WebConnect as a connection broker for PCoIP hardware devices. Note that software based PCoIP is not supported.
- 4, 5 – PowerTerm WebConnect Clients – covers how to connect to applications and desktops using PowerTerm WebConnect.

3. POWERTERM WEBCONNECT SERVER

Installing PowerTerm WebConnect Server

PowerTerm WebConnect and its components are installed under *C:\Program Files\Ericom Software\WebConnect X.x* (where X.x is the version number) by default. The installation path can be specified during the installation process. Double-click on the installation file to begin.

NOTE PowerTerm WebConnect can be installed on the following platforms: Windows 2003 (all versions), Windows 2008 (all versions), Windows 2008R2, and Windows 2012.

Server Prerequisites

Before installing PowerTerm WebConnect, the following specifications are recommended for the target server:

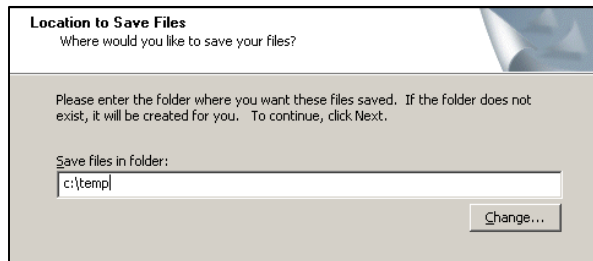
- Two CPU cores
- 1 GB of available hard disk space
- .NET Framework 4 Full installation. This can be downloaded freely from the Microsoft website.
- Application Server Role
 - Enable ASP.NET and ASP
 - IIS web server role (may also be installed on a separate system)
 - HTTPS enabled in IIS (required for AccessToGo)

HINT PowerShell script to enable requirements on a Windows 2008 R2 server:

```
# Run the following command first to allow you to run scripts:
# Set-ExecutionPolicy RemoteSigned
# Import the Server Manager Powershell modules
Import-Module servermanager
# Install ".Net Framework 3.5" Feature and "IIS" Role with "ASP.NET"and "IIS 6
  Scripting Tools"
Add-WindowsFeature Net-Framework, Web-WebServer, Web-Windows-Auth, Web-Asp-Net, Web-
  Lgcy-Scripting -restart
```

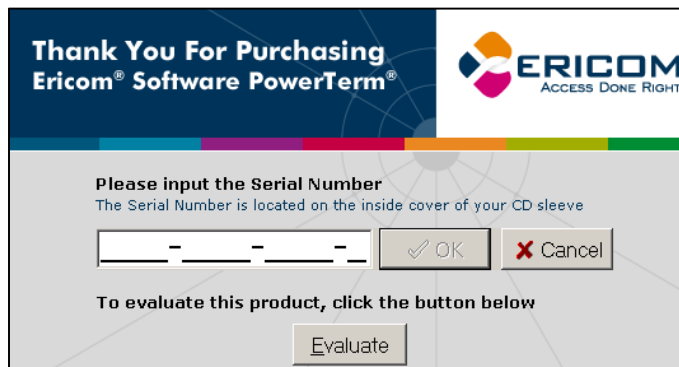

Step 1 - Specify local folder for installation files

When prompted, specify the local directory to extract the installation files to.



Step 2 – Evaluation Mode

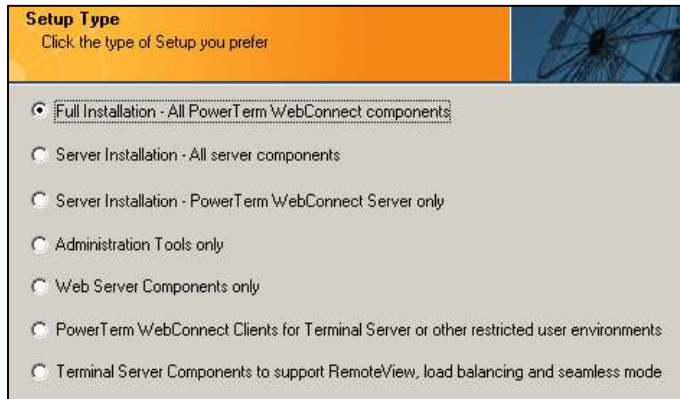
When prompted, enter the serial number or click *Evaluate* to install PowerTerm as a 30-day trial. Entering the serial number does not activate the product; go to the *Activation* section for more information.



NOTE The evaluation package of PowerTerm WebConnect runs in Enterprise mode. Once activated, the purchased PowerTerm WebConnect edition will be enabled.

Step 3 - Select the Setup Type

At the *Setup Type* selection screen choose one of the following options:



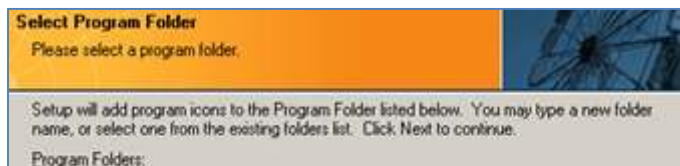
NOTE If PowerTerm WebConnect is already installed on the server, selecting a different Setup type will overwrite the existing type - resulting in unselected components being removed from the server

The *Full Installation* is used for most installations.

Step 4 – Local Directory for PowerTerm WebConnect

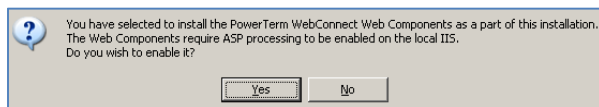
Specify the local directory for the installation of PowerTerm WebConnect.

Step 5 – Start Menu location for PowerTerm WebConnect



Step 6 – Web server ASP configuration

If prompted, enable ASP. The PowerTerm WebConnect's web based components (i.e., Application Portal and on-demand installations) requires IIS with ASP and HTTPS enabled.



Step 7 – Upgrade Message

If this is an upgrade install, the previous configuration will be imported at the end of the installation. See chapter on *Upgrade Instructions* for more details.



To copy the database and configuration from an existing PowerTerm WebConnect installation use the Upgrade Utility. The Upgrade Utility can convert the database of any previous version of PowerTerm WebConnect. Launch the Upgrade Utility from the Start Menu after the installation completes.

Step 8 – Set the WebConnect Cluster Name

The Cluster Name is a custom identifier for the PowerTerm WebConnect environment. This is something that is set by the administrator. If previous settings will be imported, the cluster name from the imported settings will be used.

When using more than one PowerTerm WebConnect server within the same environment (i.e., for redundancy purposes) a cluster name is used to identify all the servers of a common group. A PowerTerm WebConnect server can only be a member of one cluster.

Any cluster of one or more PowerTerm WebConnect servers must have a Cluster Name. This name must be unique in the network and will be viewable by end-users.

For instructions on how to change the Cluster Name after installation, please refer to the Administrators' Manual.

If there is only a single PowerTerm WebConnect cluster in the organization, it is recommended to use the organization name as the Cluster Name.

Registered Organization Name:

WebConnect Cluster Name:

Step 9 – Installing Ericom Access Server

If PowerTerm WebConnect is being installed on one of the Terminal Servers, click Yes to install the Ericom Access Server agent. This is required on all Terminal Servers that will be used with PowerTerm WebConnect.

Step 10 – Complete Installation

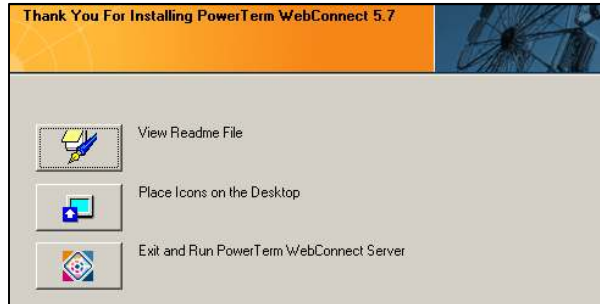
After the parameters are set, the PowerTerm WebConnect installation will continue.



Configuring setup components... Please wait!

At the end of the installation, click *Exit and Run* to launch the Administration Tool. The *PowerTerm WebConnect Server* service will usually start

automatically. If the service has not started, open *services.msc* and manually start the service, or reboot the server.



Step 11 – Install Optional Enhancements

In order to use the built-in Ericom RDP enhancements (AccessNow HTML5 access and Blaze RDP acceleration) the Access Server must be installed on the RDP hosts (Terminal Server/Remote Desktop Server). The Access Server is located under the *AddOns* folder.

Activating the Server

When PowerTerm WebConnect is first installed it will be started in Evaluation mode (30-day period). The server can be extended to continue an evaluation or activated once the product is purchased.

To extend or activate go to Start | Programs | Ericom Software | PowerTerm WebConnect | *PowerTerm WebConnect Server License Update*.

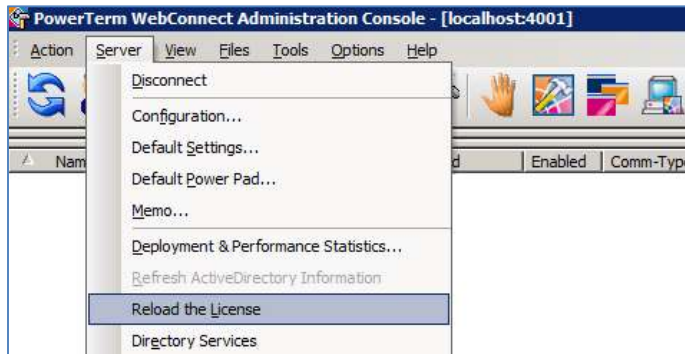
To activate PowerTerm WebConnect once it is purchased:

- Contact Ericom Support and send the *serial number* and “*Key to send*”.
- An activation key will be returned, enter this under “*Key received from Ericom*”.
- The “*Number of Licenses*” will be updated.

To extend PowerTerm WebConnect to continue an evaluation:

- Contact Ericom Sales and send the “Key to send” with the number of additional days to needed to continue evaluation.
- An extension key will be returned, enter this under “Key received from Ericom”.
- The duration will be updated.

To apply the license, either restart the PowerTerm WebConnect Server service or reload the license using the Administration Console (Server menu).



NOTE License errors may appear when hardware components are changed in the server running PowerTerm WebConnect Server. Changing the system time or copying the license file from one server to another will result in a license error as well. Please contact Ericom Technical Support to obtain a new license key in the event of an error.

Subscription Licensing Expiration Notice

PowerTerm WebConnect servers that are activated with a subscription license will display a warning notification to end-users 10 days prior to the term expiration. The administrator may change the amount of days prior to displaying the notification by adding and configuring this value in *ptserver.ini*:
 SubscriptionWarnBeforeExpirationDays

AccessNow and Blaze Activation with WebConnect

Certain editions of PowerTerm WebConnect include the AccessNow HTML5 access and Blaze RDP acceleration. Both components have built-in licensing mechanisms, however, these are **ignored** when used with PowerTerm WebConnect.

The individual AccessNow and Blaze licenses only need to be activated when the *standalone* AccessNow and Blaze clients will be used in addition to PowerTerm WebConnect.

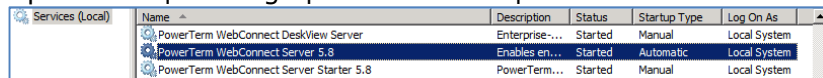
Starting and Stopping the PowerTerm WebConnect Windows Server

PowerTerm WebConnect is installed as a series of Microsoft Windows services. The Server must be running in order for clients to connect to it and establish connections to the host systems. A web server must be installed/available and running in order for end users to download the client components. By default, the PowerTerm WebConnect Windows server is installed as a server service, with the Automatic startup type. This means that during system startup, the service control manager automatically starts *PowerTerm WebConnect Server*.

Starting and Stopping the PowerTerm WebConnect service

To start/stop the server service (most common)

- Open Start | Settings | Control Panel | *Services*



Name	Description	Status	Startup Type	Log On As
PowerTerm WebConnect DeskView Server	Enterprise...	Started	Manual	Local System
PowerTerm WebConnect Server 5.8	Enables en...	Started	Automatic	Local System
PowerTerm WebConnect Server Starter 5.8	PowerTerm...	Started	Manual	Local System

- Right click on PowerTerm WebConnect Server
- Click *Start* or *Stop*.
- The *PowerTerm WebConnect Server Starter* and *PowerTerm WebConnect Deskview Server* services should not be manually stopped or started. If there is a problem with one of these services, reboot the server.

Starting the PowerTerm WebConnect service from command line

Run the *PtServer.exe* with the */start* parameter.

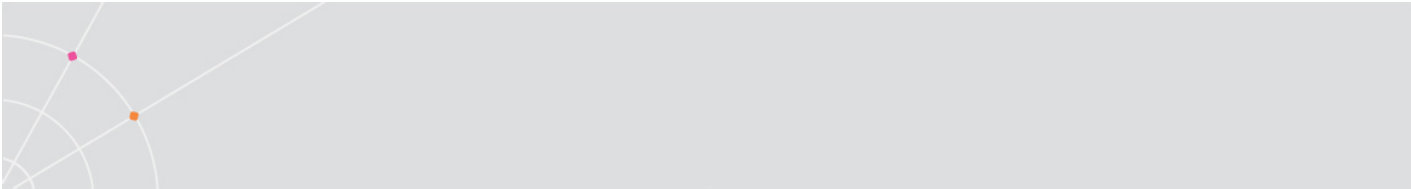
Starting the PowerTerm WebConnect service as a program

Run *PtServer.exe* with the parameter */run*.

PowerTerm WebConnect Ports

Most PowerTerm WebConnect components (Server, Starter, Administration Tool, and clients) use port 4000 (by default). This port value can be changed to avoid conflicts with other applications, as well as with firewalls or proxies.

NOTE When using a port other than the default (4000), it must be explicitly specified as a parameter to the server address in the client parameters. See the chapter on customizing client parameters for more information.



Modifying the PowerTerm WebConnect Ports

- In the Administration Console, go to File | Configuration | *Main*.
- Set the entry [ConnectionPoint=<name>] PortNo=new-port-number
- Update all HTML files with the custom port. (<webconnect server>:<port number>). When no port number is defined, the default 4000 is used.
- Update the comportal.ini with the new port number (Address and CustomAddress) settings.

Adding additional PowerTerm WebConnect Ports

PowerTerm WebConnect may listen on more than one port. To add additional ports, create new connection points and specify the port that it will use.

- Open the Administration Console and go to File | Configuration | *Main*.
- Create a new entry [ConnectionPoint=<name>] PortNo=new-port-number
- Update desired HTML files with the custom port. (<webconnect server>:<port number>). When no port number is defined, the default 4000 is used.
- Update the comportal.ini with the new port number (Address and CustomAddress) settings. See the section on the portal for detailed instructions.

Updating the Client to use a Custom port

Once the PTWC server is using a custom port, the client web pages also need to be updated in order to recognize the custom port.

To update the client pages, browse to the WebConnect *web* folder (C:\Program Files\Ericom Software\WebConnectX.X\web)

Edit the web pages are are planned for use and need to be updated:

For the *Application Zone*, change the line:

```
var PT_agentParameters = "-wc-client " + PT_server + "  
/SHORTCUT=BOTH /AUTOLOGIN=NO";
```

to:

```
var PT_agentParameters = "-wc-client " + PT_server + ":443  
/SHORTCUT=BOTH /AUTOLOGIN=NO";
```

For the *Application Portal*, edit the *Comportal.ini* file:

Address=localhost:4000

And the (sg)launch.asp page. Change the port value to the desired port.

Confirming the availability of a port

The availability of port can be verified by using the *telnet.exe* command-line utility. At a command prompt, *telnet* the server's address and specify the port to be verified (i.e. *telnet.exe server.ericom.com 4000*). If any response is received, then the port is reachable from the system running the telnet command. Note that some operating systems do not include *telnet.exe*.

Commonly Used Ports

Port #	Used by	Open On
4000	Default PowerTerm WebConnect components	PTWC
4001	PowerTerm WebConnect Administration Tool	PTWC
4010	PowerTerm Load Balancer Server	PTWC
4020	PowerTerm Load Balancer Agent	TS/RDS
4030	Remote Browser for application publishing	TS/RDS
4045	Ericom Tools (DeskView VDI users)	PTWC (DV)
4080	Automatic PTWC Server Discovery Broadcast	PTWC
3389	Microsoft RDP	TS/RDS
3399	Ericom Blaze 2.x Accelerated RDP	TS/RDS
8080	Ericom AccessNow HTML5 client	TS/RDS
80	Web services	PTWC/Web
21	FTP	PTWC
22	SSH (Emulation)	Legacy Host
23	Telnet (Emulation)	Legacy Host
389/636	LDAP/S-LDAP	AD Server
443	HTTPS/SSL	PTWC/Web
443	Ericom Secure Gateway (default port, modifiable)	ESG
515	LPD/LPR (Legacy)	PTWC
1812	RSA SecurID or Radius two-factor-authentication protocol	RSA/Radius

High Availability

To maintain high availability of the PowerTerm WebConnect services, multiple servers can be grouped to provide redundancy. There are two modes to provide high availability: *Cluster* and *Failover*. In both Cluster and Failover mode there is one *Primary* server and one or more *Monitoring* servers; and all servers must be members of the same cluster (use the same cluster name). Any WebConnect server in the cluster group can become the Primary server. The first server that is started is assigned the *Primary* role. In *Cluster* mode, the *Monitoring* servers are active and can process user's requests. In *Failover* mode, there is only one *Monitoring* server and it is in passive mode (does not accept user requests). A passive server becomes active when the primary server becomes unavailable. Both *Cluster* and *Failover* modes require access to a network directory that will host the shared cluster database.

NOTE The PowerTerm WebConnect DeskView VDI connection broker only supports Failover mode.

Shared Cluster Database

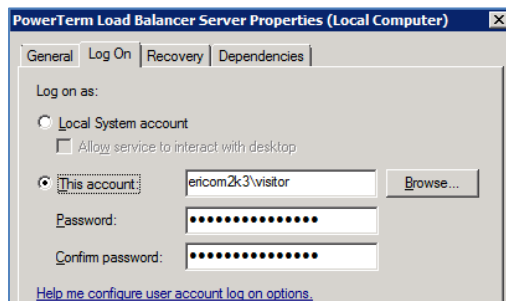
A *cluster group* is comprised of multiple PowerTerm WebConnect servers, sharing one database. The central database must be stored on a secure and robust network location (e.g., a storage area network). To maintain database integrity, only the *Primary* server can update the central database.

NOTE The database is in binary format. (In non-cluster mode, the database may be store in ASCII format as well)

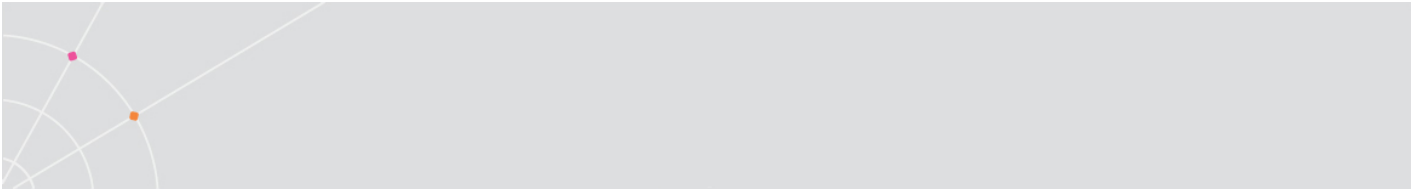
To secure access to the database, create a service account that will have *Full Control* to the shared database directory.

In order for PowerTerm WebConnect to access the shared database using the service account, go to the *Properties* of each Ericom service and set the service account in the *Log On* dialog.

In this example, the user *ericom2k3\visitor* is the service account:



In this example, all four Ericom services are configured to use the service account:



PowerTerm Load Balancer Server	System an...	Started	Automatic	ericom2k3\visitor
PowerTerm WebConnect DeskView Server	Enterprise...	Started	Manual	ericom2k3\visitor
PowerTerm WebConnect Server 5.7	Enables en...	Started	Automatic	ericom2k3\visitor
PowerTerm WebConnect Server Starter 5.7	PowerTerm...	Started	Manual	ericom2k3\visitor

NOTE The service account must have local *Administrator* access on the server running PowerTerm WebConnect. Make sure the service account is added to the local *Administrators* group.

Selecting Cluster or Failover

In both modes, a *PtServer.ptr* file is placed in the bin directory with the UNC path to the *PtServer.ini* file in shared Database directory.

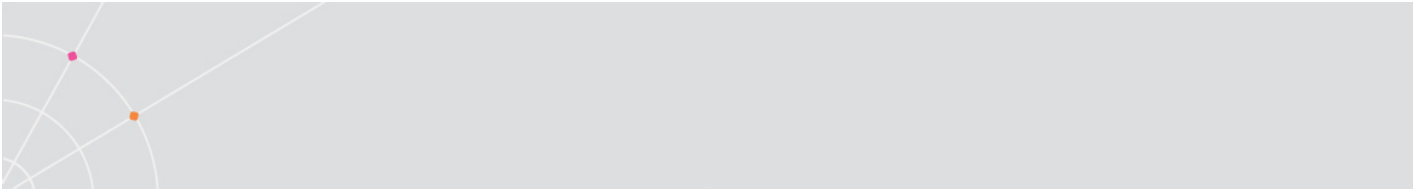
Cluster mode is enabled when the full network path is defined in the *PtServer.ptr* file, and the license file exists in the local \bin folder.

Failover mode is enabled when the full network path is defined in the *PtServer.ptr* file and the license file exists in the location of the share path.

NOTE When changing the location of the central database, remember to update the UNC path to the new location in all associated .ptr files.

Configuration

- Create a folder on a robust network share and give it a name.
- Define the newly created folder as a hidden share; this share must be secured such that only PowerTerm WebConnect servers and a backup account may access it.
- Stop the PowerTerm WebConnect Server service.
- Copy the **DataBase** and **Downloads** folders from the Primary WebConnect Server to the shared folder
- For DeskView users, copy the DeskViewServer | **Database.XML** file to the shared **Database** directory.
- *For Failover mode only:* Copy **PTS.LF** (and *PTS.LFD* if it exists) from the Primary WebConnect server's *bin* directory to the *DataBase* folder contained within the shared folder.
- *For HostView client only:* Open *PtServer_Connections.ini* file on the cluster database and modify the entries *login-command-file* and *terminal-setup-file* to designate their new location on the file server. By default, the specified directory is ...*DataBase*\Connections\ and should be replaced by [\\FileServerIP-addressOrName\WebConnect\\$](#)

- 
- Verify that the server is using Failover or Cluster mode by going to the ***PtStarter.log*** and confirm that the central database files are being loaded by the server.

Configure the Primary Server

- Create a file named *PtServer.ptr* in the \bin folder of the Primary WebConnect Server.

NOTE Make sure there is not a hidden .txt extension if the ptr file was created with a text editor, such as Notepad.

- Edit the *PtServer.ptr* with a text editor and enter the full UNC path to the Main Configuration file (PtServer.ini) located on the central share (i.e., [\\FileServer\WebConnect\\$\DataBase\PtServer.ini](#)). Do not use a local path (i.e., C:\).
- Restart the PowerTerm WebConnect Primary server.

Configure additional servers

- Copy *PtServer.ptr* from the \bin folder on the Primary server to the same folder on the Monitoring server(s). It is also possible to just create a new *PtServer.ptr* file in the \bin folder and point it to the shared PtServer.ini file.
- Restart the PowerTerm WebConnect Monitoring server(s).

NOTE Since the PtServer.ptr file is stored in the *bin* folder, upgrading a WebConnect server will not automatically put it into cluster/failover mode.

Client Configuration

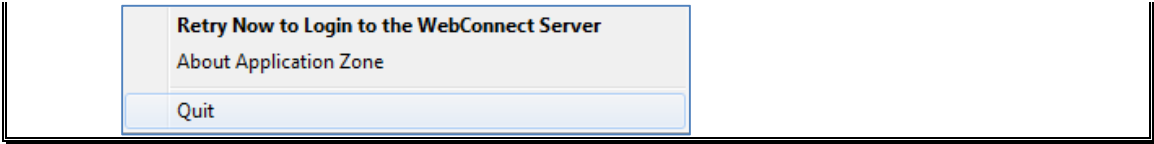
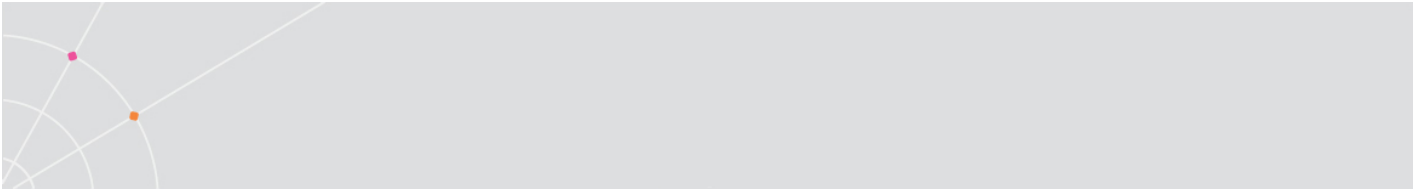
Once the PowerTerm WebConnect servers are configured for either high availability modes, the user access parameters must be updated as well.

When using *Failover* mode, the *Server* parameter must contain the list of WebConnect servers separated by semi-colons. Please refer the *Custom Client Parameters* (Failover Configuration) chapter for detailed instructions.

In *Cluster* Mode, a third-party load balancer (e.g., Microsoft NLB) may be used to load balance between the clustered *PowerTerm WebConnect* servers. The client's server parameter is then configured with the clustered address (of the load balancer), which will redirect the request to the least loaded PowerTerm WebConnect Server in the cluster.

Client Usage

NOTE Active Application Zones do not failover automatically. Since only one Application Zone may run on a single machine, the inactive Application Zone must be closed manually.



After the failover process is complete, instruct the users to run Application Zone again. The failover mechanism on the client will timeout on the primary server and connect to the failover server.

Using Failover Mode

In the event that the Primary server goes down, the Failover server becomes the *new* Primary server.

NOTE When the primary server goes down, the transition to the failover server will take a few minutes. During this time, users will not be able to login.

The *new* Primary server maintains all functionality of the original Primary server. The only difference is that the clients will take longer to connect since each client tries to connect to the original primary server first. The client must wait for the first server to timeout before it attempts to connect to the second server.

Restoring the original Primary server only puts it into failover mode (the roles are now reversed). Clients cannot connect directly failover servers, so the longer connection time will persist. If a user tried to connect directly to a failover server, an error message will be displayed:



In order to restore the original configuration:

- Stop the *new* Primary server
- Wait for the original Primary server to become the primary again
- Restart the original Failover server, and it will now revert back to its original failover role.

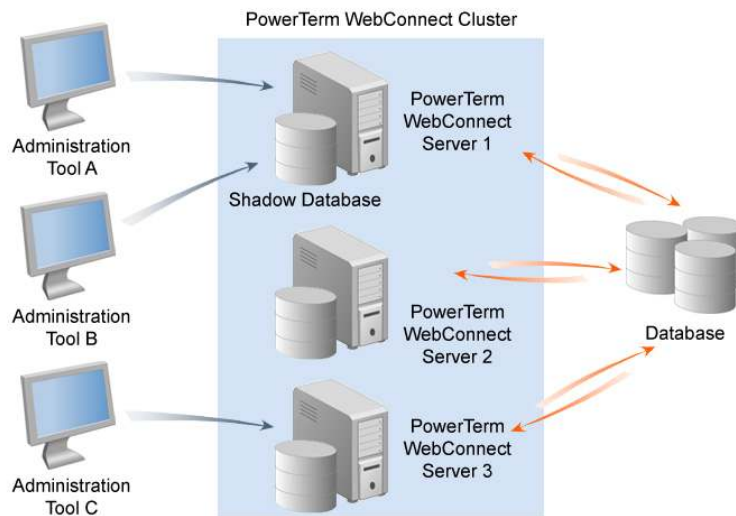
Using Cluster Mode

In the event that the Primary server goes down, any of the Monitoring servers can become the *new* primary server. Only the Primary server can update the database. However, all servers have equal functionality and can accept user requests. The user can connect to any active PowerTerm WebConnect server in the cluster to access published resources.

PowerTerm WebConnect servers in a Cluster Mode environment can also be load balanced using a third-party load balancer. The PowerTerm WebConnect Server service supports ping based load balancers that monitor an address or port for service presence.

Cluster Administration

In the example below, there are three PowerTerm WebConnect Servers in the cluster: Servers 1, 2, and 3. All servers are connected to the central database. In this configuration, if Server 1 is able to update the database, then both Administrators A and B will have write permission.



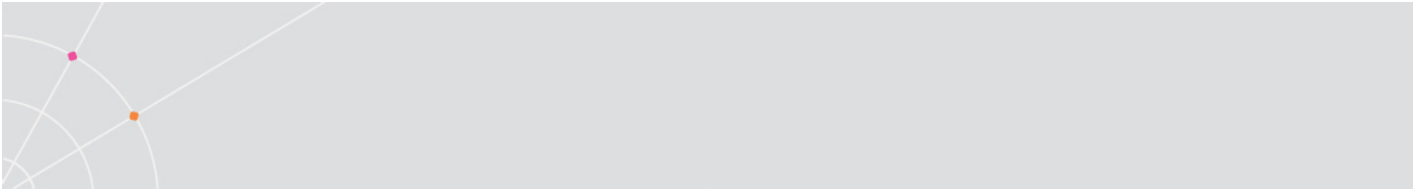
Users connecting to Monitoring servers (Administrator C) will only be able to see the current configuration and will not be allowed to make changes. When an Administrator connects to a *Monitoring* server a message is displayed:



If the Administrator clicks *No*, the Administration Console will connect to the selected PowerTerm WebConnect server, but will only have read access.

- The title bar of the Administration Console will indicate that it is in *Monitor Mode* only.
- A small, solid blue circle will appear in the lower left hand corner of the Administration Tool.

Clicking on *Yes* will redirect the Administrator to the Primary server.

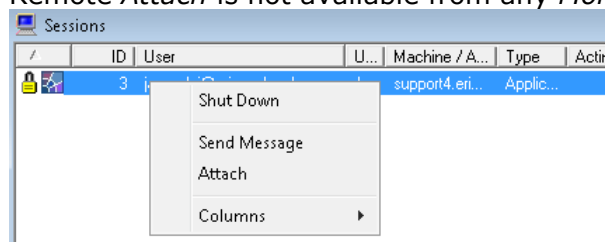


PtServer.ini Parameters

ShadowDbSyncFrequencyMinutes	Sets the synchronization interval of the shadow database. Default: 60
CashDbSyncFrequencySeconds	Updates interval in seconds for copying the database to memory. Default: 60
CashDbSyncToleranceSeconds	Updates the wait interval in seconds if the database cannot be updated immediately. Default: 5
CashDbSyncMaxToleranceSeconds	The maximum number of repeats of CashDbSyncToleranceSeconds to wait before updating the database in memory. Default: 60

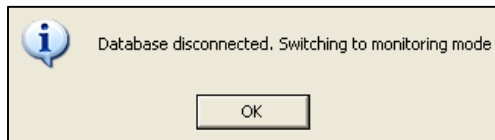
High Availability Limitations

- Monitoring of active sessions is not clustered – active sessions are monitored by *each* individual PowerTerm WebConnect server.
- Users that are auto-created are always in *non-persistent* mode.
- Do not switch the database to a different network location when any PowerTerm WebConnect servers are connected to it.
- The *DeskView* Connection Broker database does not support Cluster mode, therefore Failover mode must be used.
- The *Load Balancer* clustering is handled separately. See chapter on the PowerTerm WebConnect Load Balancer on how to configure this.
- There is no indicator in the Administration Console to notify the Administrator if the cluster database is being used (only *Monitoring* mode notification is available).
- Client (*View* | *Client Sessions*) functions are disabled on *Monitoring* servers. Right-clicking on a user in the *Sessions* list will present an action menu. However, all functions of this menu are disabled. Remote *Attach* is not available from any *Monitoring* server.



Local Server Mode and the Shadow Database

In the event that the central database is not available (network failure, lack of permissions, etc.), the Administration Console that has write access (*Primary server*) will automatically switch to Monitoring mode. The switch will occur the next time the server tries to access the database (i.e., a configuration change needs to be applied). Monitoring mode does not allow updates to the central database.



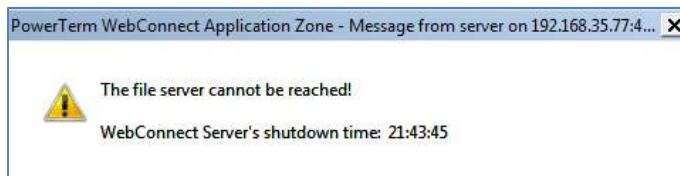
A local copy of the main database (shadow database) is stored in each PowerTerm WebConnect Server and is updated periodically from the central store. This database is non-persistent and is lost if the server is shut down.

The shadow database is used when the primary database is not available. This allows the servers to start and provide service, but not with the central database. When the central database becomes available again, the Monitoring servers will update their information from the central store.

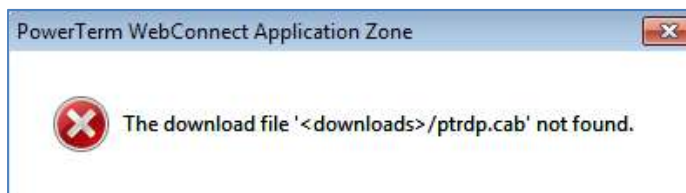
In a *Cluster* environment, the first PowerTerm WebConnect server to connect to the central store becomes the *Primary* server.

NOTE The shadow database may be outdated if it has not been updated recently.

In a Failover environment, there must be a very robust connection to the shared database. If the central database becomes unavailable, all active users will no longer be able to access published resources. This error message will appear:



When a user tries to launch a resource, if the central *Downloads* folder is unavailable, an error message will be returned:





4. END-USER ACCESS CLIENTS

PowerTerm WebConnect supports access from a wide variety of operating systems and devices.

- Most HTML5 web browsers (using the AccessNow client)
- Windows (XP, Vista, 7, 8, 2003, 2008, 2012, and higher)
- Apple Mac OSX 10.5 and higher (Intel only)
- Most Apple iOS devices (iPad, iPhone, and iTouch)
- Most Android devices
- Most Blackberry 10 devices
- Windows CE and XPe thin clients
- Google Chromebook/Chromebox (using AccessNow)
- Upcoming - Linux workstations and thin clients (Debian and RedHat based)

End users may use any one of these interfaces to login and view their assigned applications and desktops:

- Application Portal – Web based interface that launches applications and desktops that will use the RDP, Blaze, or AccessNow protocol.
- Application Zone – Native application that launches applications and desktops that will use either the RDP or Blaze protocol.
- AccessToGo – Native mobile client for iOS or Android that that launches applications and desktops that will use either the RDP or Blaze protocol.

There are two types of clients that maybe used to display an application or desktop:

- Native client – this is an application that is native to the end-user's operating system. A native client will usually provide better performance and has the option to use the Blaze acceleration protocol.
- HTML5 Web browser – may be used as a client when the AccessNow HTML5 protocol is enabled. Applications and desktops that are launched will appear inside the web browser and does not require anything to be downloaded onto the end-user's device.

NOTE There is no Java-based client for PowerTerm WebConnect
--



Application Portal Interface

PowerTerm WebConnect provides an ASP-based web interface for accessing published applications – the Application Portal. The Application Portal is compatible with most modern web browsers.

There are two modes for the Application Portal, which is configured by editing the *Config.inc* file (located under `..\Ericom Software\WebConnect x.y\web\AppPortal`).

The Administrator can enable either AccessNow HTML5 or the Native client for use with the Application Portal. Different Application Portal configurations may be added by creating additional instances of the *AppPortal* folder (and using a different name).

AccessNow HTML5 Prefer Mode (Default)

When a user selects an application or desktop from the Portal, the resource will open as a new browser tab or window. To enable AccessNow mode, configure this variable in the *config.inc* file (default configuration):

```
Const AccessNow_over_ActiveX = 1
```

```
Const AccessNow_over_Java = 1
```

AccessNow HTML5 Only Mode

When this setting is enabled, only the HTML5 client will be used if the browser supports it. Native client fallback will be disabled.

```
Const Always_Use_AccessNow = 1
```

Native Only Mode

When a user selects an application or desktop from the Portal, the resource will open using the native client (also known as a new PtAgent session.) To enable this, configure this variable in the *config.inc* file:

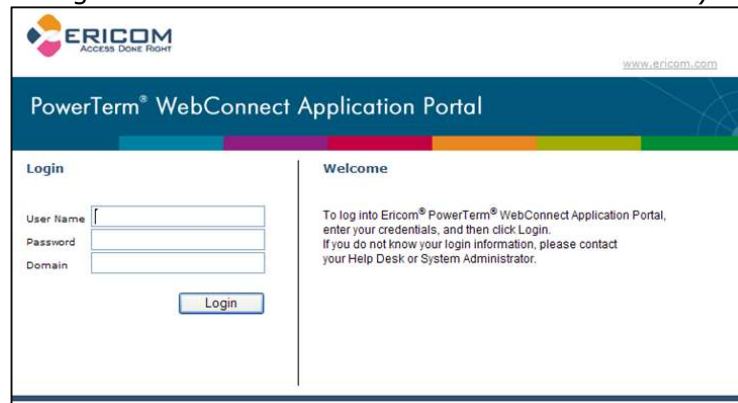
```
Const AccessNow_over_ActiveX = 0
```

```
Const AccessNow_over_Java = 0
```

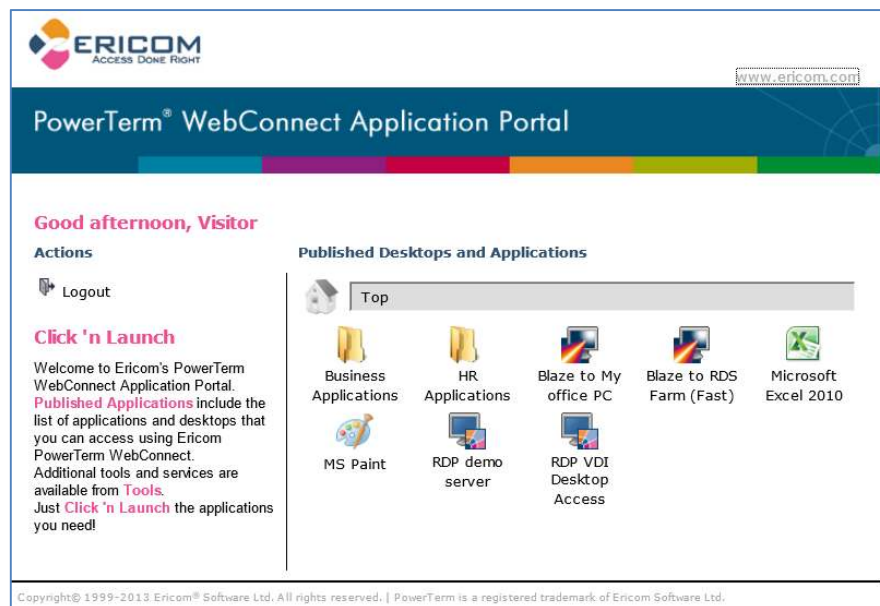
Launching Application Portal from a web browser

- Using a web browser open the following link:
Application Portal:
<http://server-address/webconnect/AppPortal/index.asp>
- At the login dialog, enter the user's credentials (if a domain is not specified as part of the username, the default domain that is

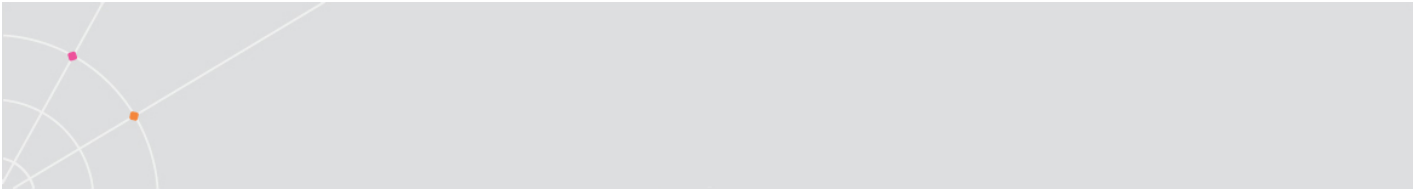
configured on PowerTerm WebConnect will be used).



- Once authenticated, the user will be presented with Application Portal.



- To launch any published application or desktop, click on the desired icon. If AccessNow is configured, and the user is connecting from an HTML5 browser, the selected application or desktop will appear within a new browser tab or window. If AccessNow is not available or disabled, the application or desktop will run using the native client (i.e. RemoteView) if it is available.
- To close the Application Portal session click on *Logout* to the left of the application and desktop icons.



NOTE AccessNow and AccessToGo do not support the SmartInternal feature. By default, SmartInternal connections use *Direct* mode with these clients. To force all connections set to *SmartInternal* to use *Gateway* mode, set this environment variable:

SmartInternalIsGateway set to *1*

Form Post SSO to the Application Portal

If a third-party interface is used in front of PowerTerm WebConnect (e.g. an SSL VPN) to capture user credentials, the user's credentials may be passed into the Portal using the Form POST method to enable single sign-on. To configure the POST operation:

- POST the following values to the PowerTerm WebConnect Portal URL: *http://<server>/webconnect/AppPortal/LoggedIn.asp*
- username / <USERNAME>
- password / <PASSWORD>
- domain / <enter your domain>

Application Zone for Windows

The PowerTerm WebConnect Application Zone provides a native client interface for accessing published applications and desktops. The Application Zone also provides local desktop integration by placing icons for published resources on the local desktop and in the local Start menu. The *Application Zone* uses an agent (ptagent.exe on Windows systems) to acquire the latest configuration and client components from the PowerTerm WebConnect server.

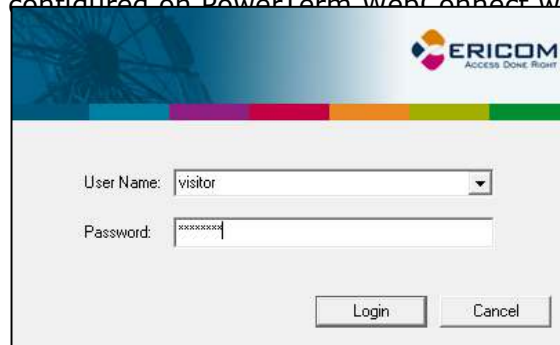
Windows Application Zone will automatically update the resource list whenever a change has been applied to the Connection's properties. For example, if the HR group is removed from a connection's Owner list, all users that are members of the HR group who are currently logged into Application Zone will see the connection disappear from their list of resources.

NOTE When Users are added or removed from Groups that are an *Owner* of a connection, the change is not reflected in Application Zone until the user logs off and back on. This is normal Windows operation. Only direct changes to the Connection's *Properties* will be automatically updated in Application Zone.

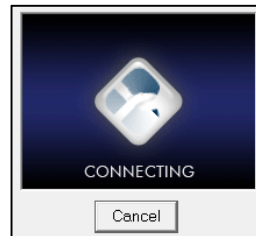
Launching Application Zone from a web browser

- Using a web browser open: <http://server-address/WebConnect/ApplicationZone.html>

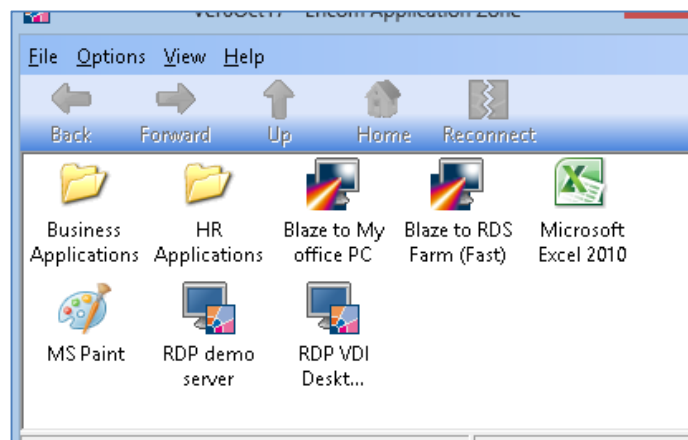
- At the login dialog, enter the user's credentials (if a domain is not specified as part of the username, the default domain that is configured on PowerTerm WebConnect will be used).



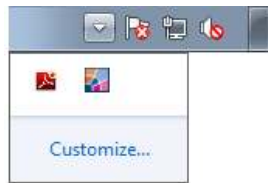
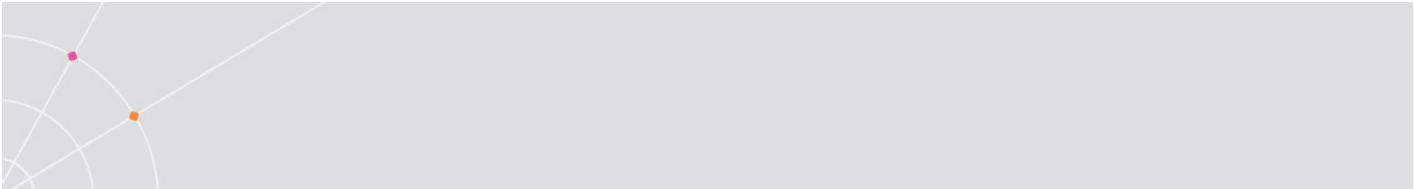
- Click Login



- Once authenticated, the user will be presented with Application Zone.



- All published resources may also be accessed from the Systray agent.



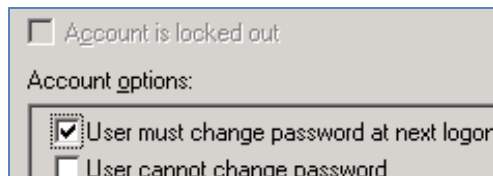
- To launch any published application or desktop, double-click on the desired icon. This launches the *RemoteView* client on the local device to connect to the appropriate Terminal Server or virtual desktop.

NOTE Only one user can be logged into Application Zone from any system. However, the same user may be logged into multiple systems if *Allow Concurrent Machines* is enabled.

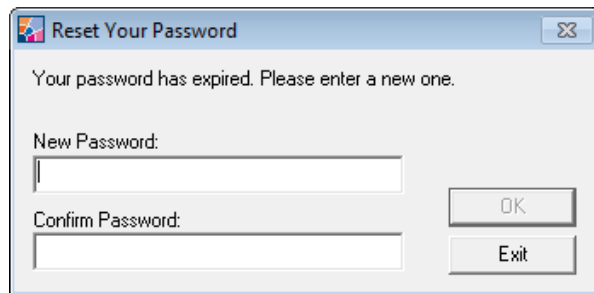
Expired Passwords

The Application Zone will properly handle expired passwords.

For example, if the user's account is set to "must change password":



When the user logs in to Application Zone, it will be prompted with an expired password message and allowed to change its password.

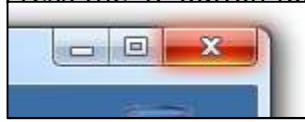


NOTE This feature is currently not available with Application Portal, AccessToGo or AccessPad.

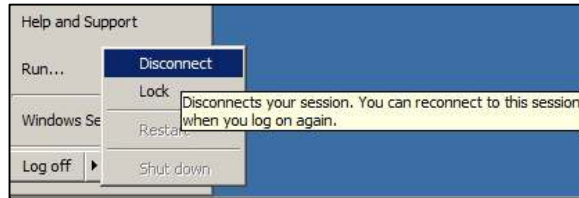
Disconnecting a Full Desktop Session

A user may disconnect an active desktop session so that it can be used at a later time. There are two ways to disconnect a session:

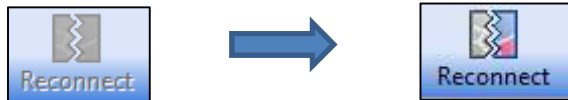
- Press the 'X' button for the RDP or Blaze session window.



- Select *Disconnect* from Start menu.



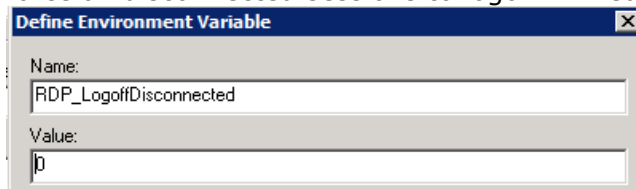
Upon successful disconnect, the Application Zone's *Reconnect* button will turn active. Click on the active *Reconnect* button to reconnect to the existing session.



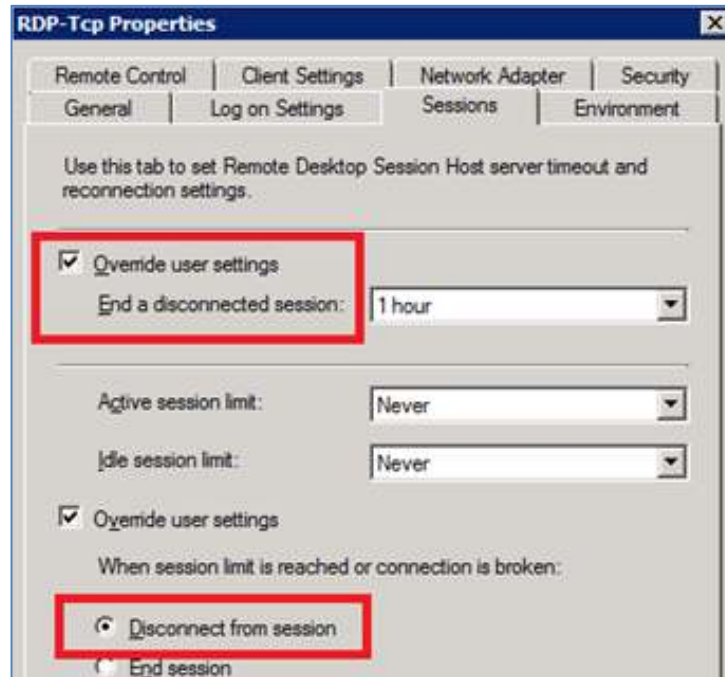
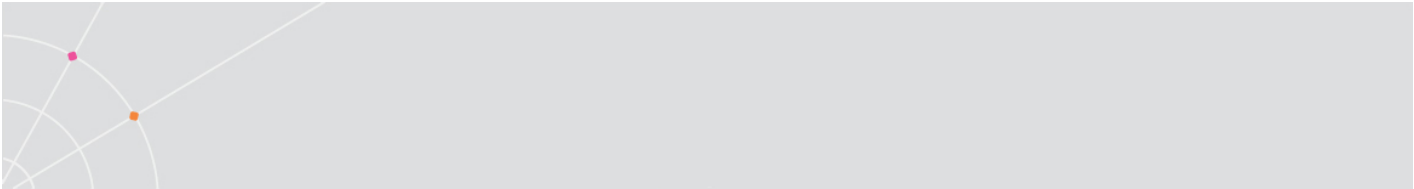
NOTE Published applications cannot be put in a *Disconnected* state by the end-user. They may be disconnected due to network failure, and reconnected at a later time.

In order to use the Session Reconnect feature, verify that these two settings are configured:

- The PowerTerm WebConnect *RDP_LogoffDisconnected* variable is set to 0 (false) by default. This setting will allow any Disconnected sessions to be available for future reconnect. Setting this to 0 will force all disconnected sessions to logoff immediately.



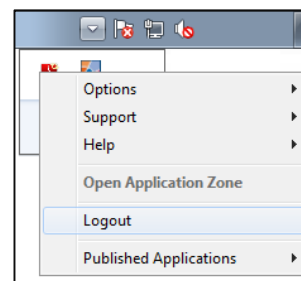
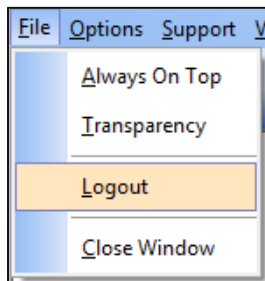
- In the Terminal Server (RDS) configuration, allocate enough time for disconnected sessions to remain active before ending them. This will ensure that users can move from one location to another and have enough time to reconnect into their disconnected sessions.



Logging Off

There are two methods to logout of Application Zone.

- From the Application Zone File menu, select *Logout*.
- Right-click on the Application Zone systray icon and select *Logout*.



NOTE The Application Zone shortcut format is *<OrganizationName> PowerTerm Application Zone by Ericom*. If there are more than one Application Zone running with the same organization name, there will be only one desktop shortcut for them. The organization name configuration is done from the Main Configuration (*PtServer.ini*) *OrganizationName* setting.



AccessPad

Two native clients are available for *Windows*: the Windows Application Zone and AccessPad. AccessPad adds support for two-factor authentication (requires Authentication Server) and functions more similarly to the *Mac* native client (where AccessPad is the only available client. AccessPad also includes a universal printer for RDP and Blaze connections. See chapter on printing for more details. AccessPad 9.0 and higher adds the ability to use the EricomRDP client for RDP-enabled sessions.

<p>NOTE To disable the use of EricomRDP add a Blaze_Setup_Params of "rdp client preference:i:0" – this will force AccessPad to use the Blaze protocol</p>
--

AccessPad for Mac include a universal printer for RDP and Blaze connections. See chapter on printing for more details.

The following features are not supported by AccessPad 3.x:

- Session Disconnect/Reconnect
- Server failover
- HostView, FTP Components
- Desktop/Start-menu shortcut icons.
- Workstation single-sign on component (PtSSOLogin)
- RemoteView PARAM line options
- Reconnect to known disconnected sessions
- Desktop shortcuts
- Other minor Application Zone functions

Usage

- Launch AccessPad
 - AccessPad may be launched as a standalone client. There is an MSI installer for Windows and PKG installer for Macs.
 - Mac Users: Browse to the Application Zone URL (or the Application Portal with native mode enabled):
`http://<WC_server address>/webconnect/applicationzone.html`
- A login prompt will appear. Verify that the *Server* address is correct and enter the user's credentials. Refer to the two-factor

authentication section in this manual if this feature is required.



- Once logged in, the AccessPad will appear with available connections.







- The user simply clicks or taps the desired connection to launch it.
- When exiting AccessPad, **all** active connections will be closed.

NOTE To use third-party add-ons with WebConnect, such as net2printer, these clients need to be installed manually on the end-user device.

AccessPad Menu bar

The AccessPad menu bar contains four useful functions:



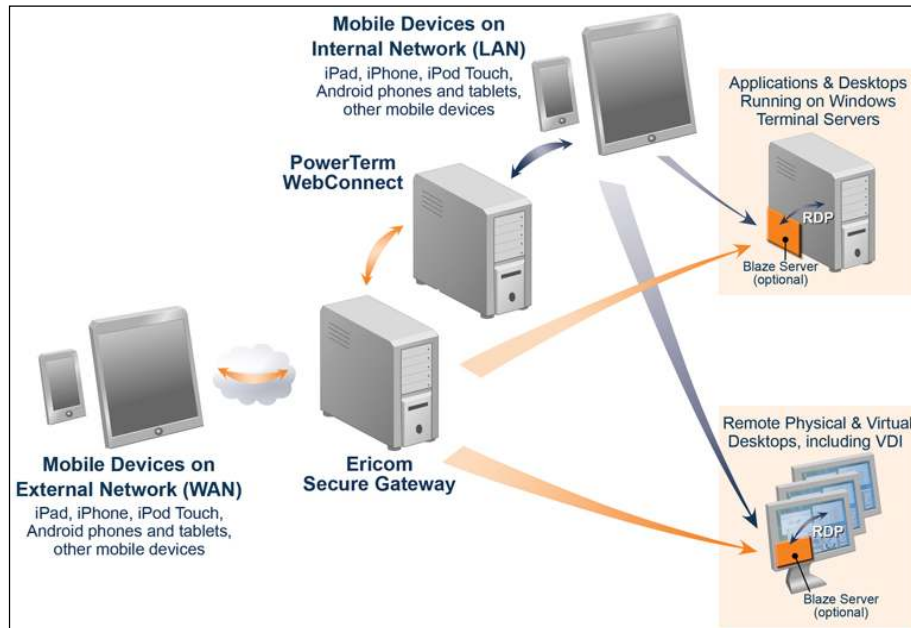
	Function	Description
	Home	Returns to the main list
	Parent folder	Return to the parent folder list
	About	Displays version number, installation folder, PowerTerm WebConnect server address, and username that is currently logged in.
	Exit	Logoff

NOTE If changes are made to the user's application set, the user must logoff and log back into AccessPad to see the changes.

AccessToGo Mobile Client

NOTE This chapter is taken from the AccessToGo manual. Refer to the AccessToGo manual for full documentation.

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



Prerequisites

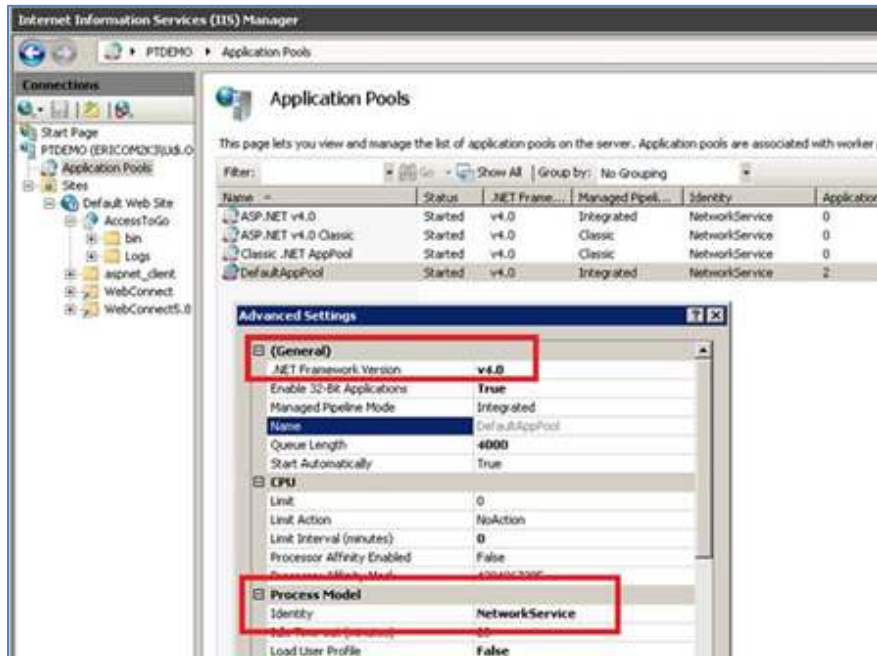
In order to connect to PowerTerm WebConnect resources, the AccessToGo server-side component must be enabled on the PowerTerm WebConnect server. This is installed by default.

Organize ▾ Uninstall Change Repair	
Name ▲	Publisher
AccessToGo	Ericom Software
Ericom AccessNow Server	Ericom Software
Ericom Blaze Server	Ericom Software

The AccessToGo component requires ASP.Net 4 and IIS with HTTPS enabled.

NOTE Since HTTPS requires port 443, be careful not to run the Ericom Secure Gateway on the same machine using 443. The Secure Gateway is typically installed on a different system, that is in the DMZ, to act as a proxy.

The Application Pool must be configured to use ASP.Net version 4.0



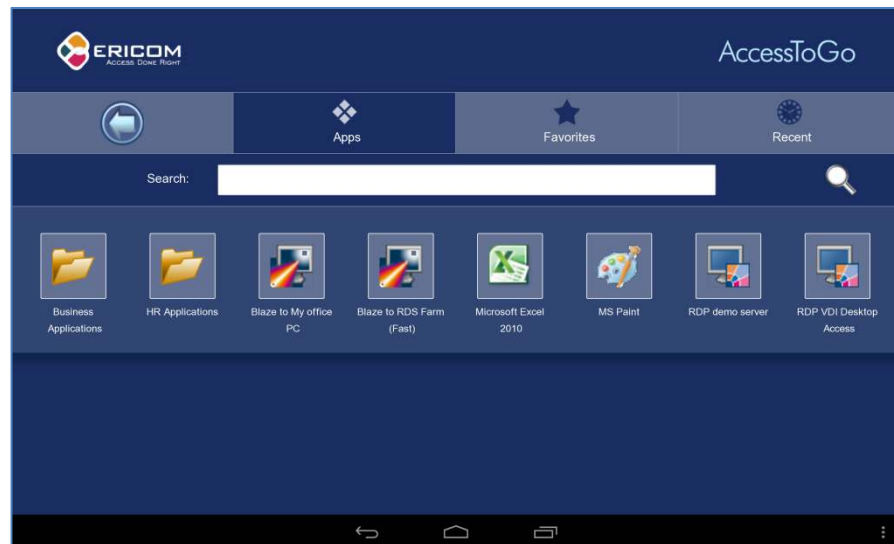
Usage

AccessToGo may be used to connect to an application or desktop hosted through a PowerTerm WebConnect connection broker. Here are the steps to use AccessToGo with PowerTerm WebConnect:

- Install AccessToGo on the end-user device (i.e. iPad).
 - On iOS, AccessToGo may be downloaded from iTunes. AccessToGo version 1.3.2 is required for PowerTerm WebConnect compatibility.
 - On Android, AccessToGo is downloaded from Google Play or the device's application market. AccessToGo version 1.3.2 is required for PowerTerm WebConnect compatibility.
- Configure AccessToGo to connect to the address of the PowerTerm WebConnect server. Explicitly specify the port if it is not 4000 or 443 (i.e. 192.168.1.1:4343)
 - If the connection is being made remotely, point to the external address and port of the firewall/router that has been configured with the rule to port forward incoming connections to the PowerTerm WebConnect server.
 - If the optional Ericom Secure Gateway is used for remote connections, specify its external address and port (rather than the PowerTerm WebConnect internal address). 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.

- Once the user is logged in, all assigned resources will be displayed.



- Tap on the desired resource to start the connection.

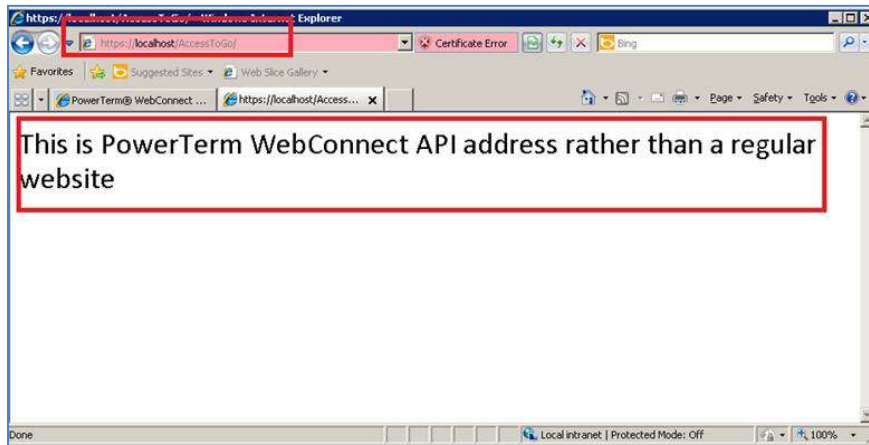
NOTE AccessNow and AccessToGo do not support the SmartInternal feature. By default, SmartInternal connections use *Direct* mode with these clients. To force all connections set to *SmartInternal* to use *Gateway* mode, set this environment variable:

SmartInternalIsGateway set to 1

Troubleshooting

Connectivity Problems

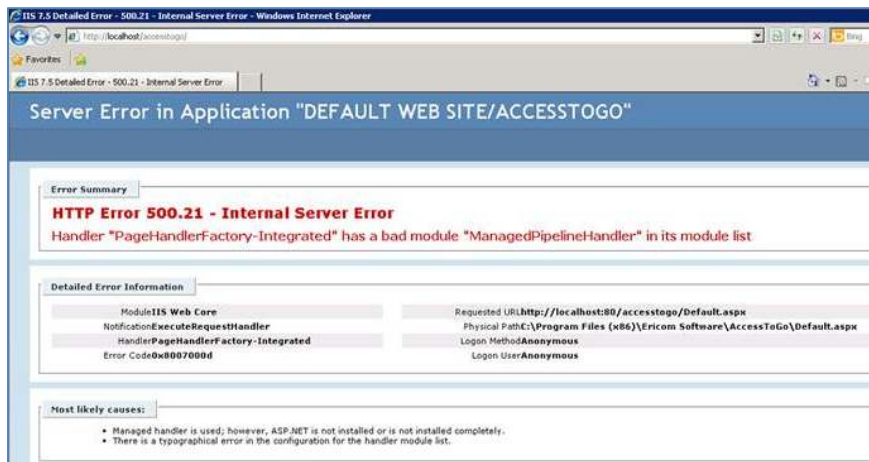
If users are experiencing connectivity or data errors when connecting to PowerTerm WebConnect with AccessToGo, verify that the API is active and available. On the PowerTerm WebConnect server, open a browser and go to <https://localhost>. If the API is active, a message will be displayed: "This is the PowerTerm WebConnect API address".



If this message does not appear, first verify that port 443 is assigned to IIS. IIS and HTTPS is required to run the AccessToGo component.

Internal Server Error

If ASP.Net is not properly registered on the server, this message will appear:



To resolve this error, open the command prompt as an Administrator and run the following command:

%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -i

AccessToGo Session Disconnected Error

If the AccessToGo app can display the list of connections, but cannot launch any applications or desktops, verify that the version is **1.3.2** under the *Settings* button. Earlier versions of AccessToGo are not compatible with PowerTerm WebConnect and will display a message "Session Disconnected" when the user tries to launch an application or desktop.

AccessPortal

Two web based launch portals are available with PowerTerm WebConnect 6.x: *Application Portal* and *AccessPortal*. *AccessPortal* adds support for two-factor authentication (requires Authentication Server) and functions more similarly to the *AccessPad* native client. *AccessPortal* will become the primary web access page in future versions of PowerTerm WebConnect.

The following features are not supported by *AccessPortal*:

- Server failover
- HostView, FTP Components
- Ericom workstation single sign-on component (PtSSOLogin)
- RemoteView (PARAM) parameter options
- Session Disconnect/Reconnect
- Reconnect to known disconnected sessions

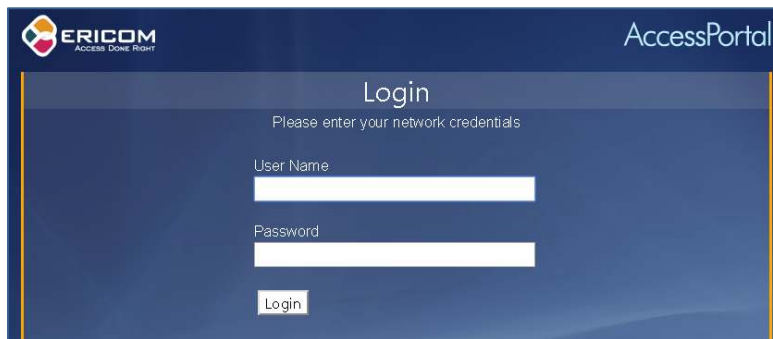
Installation and Usage

AccessPortal is provided as an MSI installer and is generally installed on the WebConnect server. Verify that IIS is enabled before installing to allow the *AccessPortal* installer to automatically add the necessary configuration to IIS.

Once *AccessPortal* is installed, direct users to the *AccessPortal* URL:

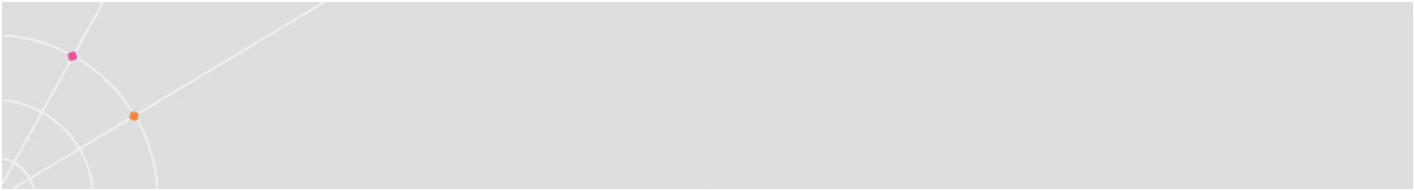
http://<WC_server_address>/webconnect/WebConnect/AccessPortal/

A login prompt will appear displaying fields for the user's credentials. Refer to the two-factor authentication section in this manual if this feature is required.



Enable Native Client

AccessPortal is configured to launch the HTML5 client, *AccessNow*. To change this to the native client, edit the *Settings.xml* file located under `<drive>:\Program Files (x86)\Ericom Software\WebConnect 6.0\web\AccessPortal`



Find the *ClientType* and change the setting from *AccessNow* to *Native*

```
<ClientType AllowLocalSetup="false">Native</ClientType>
```

After the change is saved, run *iisreset.exe* on the server to apply the changes.

5. NATIVE CLIENT REMOTE DEPLOYMENT

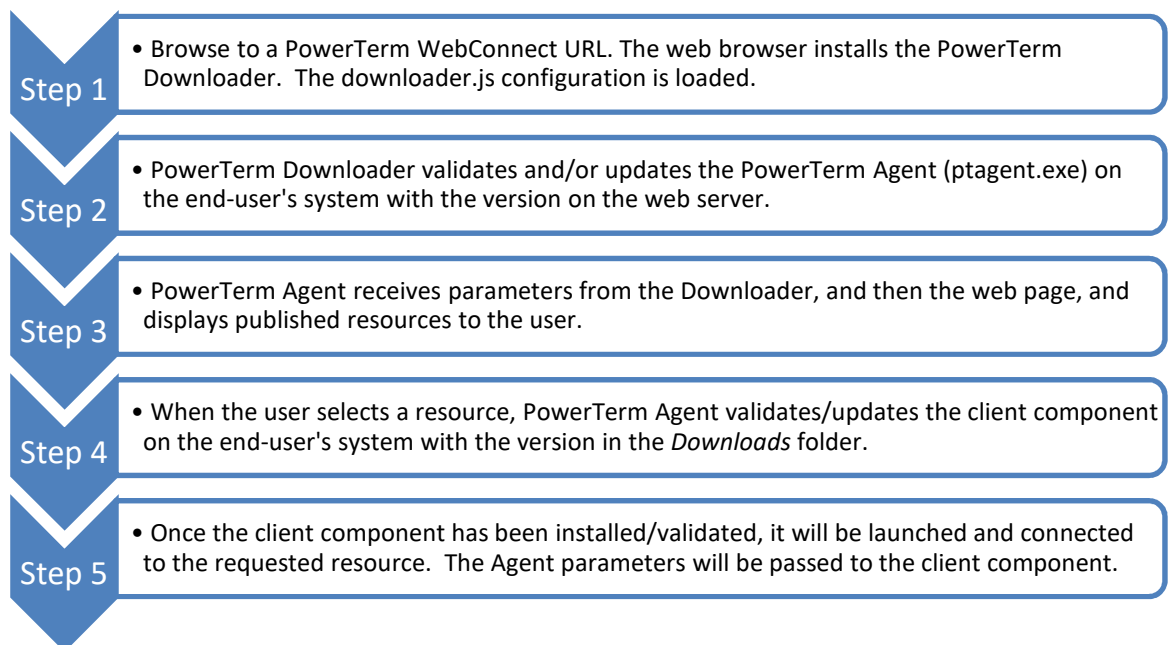
A key feature of PowerTerm WebConnect is its ability to remotely install and update the native client components. Two mechanisms are available to launch PowerTerm WebConnect resources from a web browser:

- Windows (ActiveX) Downloader
- Java Downloader

The downloader can be modified in the following ways:

- Place an Application Zone shortcut icon on the user's desktop
- The installation folder of the client download can be modified.
- Enable auto-update to ensure that all clients are using the latest version.
- Create a custom access page (i.e., use generic users to login).

When using the Application Zone and Application Portal, both ActiveX and Java downloaders do not directly launch the requested client. The Application Zone/Application portal (ptagent.exe) is launched and then instructed on which client to launch based on the user's selection. The Application Zone/Application portal will then initiate the installation of the requested client component (i.e., RemoteView/ptrdp.exe).





The Downloader

PowerTerm WebConnect Downloader's role is to download, install and launch pre-configured client components through a web browser. There are two such Downloader types:

- Windows ActiveX control
 - Available for Windows workstations only
 - ActiveX compatible browser required (Internet Explorer)
 - Permissions to run signed ActiveX components required
 - Does not support x64 Internet Explorer
- Java applet
 - Cross platform, compatible with Windows, Mac, and Linux
 - Java/JVM is required on the end-user system
 - Permissions to run Java applications required
 - Supports x64 Internet Explorer if Java 64-bit is installed (http://www.java.com/en/download/faq/java_win64bit.xml #Java for 64-bit)

NOTE The Java Downloader is not compatible with IE on Windows 7 or Vista when UAC is enabled (which is the default)

If neither Downloader components can be used (i.e., the user's browser does not support ActiveX and is not Java enabled) the user will be notified and the MSI should be used.

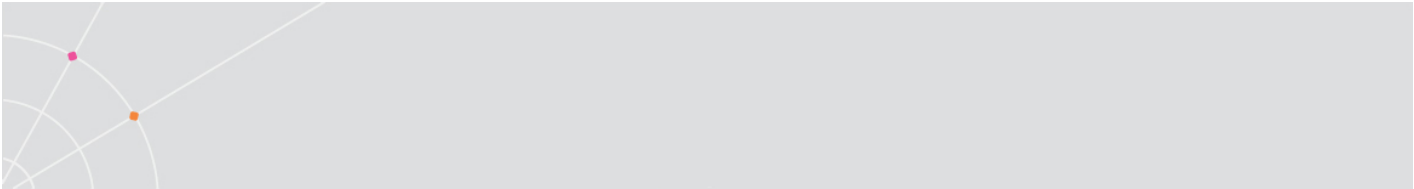
Configuring downloader.js Parameters

The *downloader.js* automatically launches the appropriate Downloader type based on client's properties. Since *downloader.js* is executed on the client side, it does not require any special changes on the server-side.

NOTE The only requirement to use *downloader.js* is to enable JavaScript on the client side.

Custom parameters can be passed to *downloader.js* in order to modify the behavior of the Downloader components. The *downloader.js* passes the appropriate values to the Downloader component being used in the proper format. This *downloader.js* is compatible with most web browsers, including the latest versions of Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera.

Parameters for *downloader.js* are specified by assigning values to global script variables. The script assigning the values must be executed before



downloader.js. For this reason it is a good idea to place the script inside the <head> section. Do not set the values in the page's *onload* event handler as that will execute after downloader.js.

The variables that specify values for downloader.js start with *PT_ prefix*. Here is an example of a script block that specifies the settings:

```
<head>
...
<script type="text/javascript" language="javascript1.2">
  // Parameters for downloader.js
  var PT_windowsDownloaderURL      = "windows/ptdownloader.cab";
  var PT_ns6DownloaderURL         = "Downloader_NS6WS_Signed.jar";
  var PT_identifyJVM              = "windows/IdentifyJVM.class";
  var PT_javaDownloaderImagesURL = "images";
  var PT_windowsAgentURL          = "./windows/ptagent.cab";
  var PT_linuxAgentURL            = "./linux/ix86/qterm-wc.zip";
  var PT_server                    = location.hostname;
  var PT_agentParameters          = " -wc-client " + PT_server + "
  /SHORTCUT=BOTH /AUTOLOGIN=NO";
  var PT_clientDst                 = "";
  var PT_downloaderLog             = "";
  var PT_selectedConnection       = "";
  var PT_shortcut                  = true;
  var PT_useJavaOnIE              = true;
</script>
...
</head>
```

<p>NOTE The use of the prefix <i>PT_</i> make it unlikely that there will be a conflict with global variables of any framework that might be used in the web page.</p>

Embedding downloader.js

To use downloader.js in a web page, use the <script> HTML tag to embed a reference to it in the page. This reference must be inside the <body> section of the page. This <script> section will not generate any visible output to the user, other than launching a Downloader component.

```
<html>
<head>
...
</head>
<body>
...
  <script type="text/javascript" language="javascript1.2"
  src="AppPortal/downloader.js"></script>
...
</body>
</html>
```

The *src* attribute of the <script> tag must specify a valid URL where the downloader.js file is located. This URL can be either relative, as in the example above, or absolute.

NOTE While it is possible to embed the Downloader components directly into web pages, the preferred method is to use the *downloader.js*.

downloader.js Settings

Settings that specify locations, such as PT_windowsDownloaderURL and PT_identifyJVM, are assigned a URL.

Name	Description
PT_windowsDownloaderURL	Location of ActiveX Downloader
PT_ns6DownloaderURL	Location of Java Downloader – signed Java Applet
PT_identifyJVM	Location of Java applet that determines JVM type and version
PT_javaDownloaderImagesURL	Location of folder containing images used by Java Downloader
PT_windowsAgentURL	Location of cab containing the PowerTerm WebConnect agent for Windows – PtAgent.exe The .ver.txt file must be located in the same location as the cab file
PT_linuxAgentURL	Location of zip file containing the PowerTerm WebConnect agent for Linux The .ver.txt file must be located in the same location as the cab file
PT_server	Address of the PowerTerm WebConnect server
<i>PT_agentParameters</i>	Parameters (PARAMS) passed to the agent when it is launched
PT_clientDst	Installation destination on end-point device
PT_downloaderLog	Path to log file on end-point device. If empty then no log file will be generated
PT_selectedConnection	Specify connection, e.g. id of published application, to launch. If empty then no connection is launched – instead a list of connections will be displayed by the agent.
PT_shortcut	A Boolean value indicating whether a desktop shortcut to the agent should be created on the end-point device
PT_useJavaOnIE	Use Java on Internet Explorer if ActiveX fails to start



Windows Downloader

The advantages of using ActiveX for downloading and installing PowerTerm WebConnect clients are:

- The HTML file is easy to configure.
- Small download size.
- Does not require any external components beyond the browser itself (such as the JVM).
- Best control over the download destination.

The Windows Downloader can only be activated by a browser that is compatible with ActiveX technology, such as Microsoft Internet Explorer.

The Windows Downloader is a stand-alone executable, PtDownloader.exe, and has the following COM attributes:

GUID – {7EC816D4-6FC3-4C58-A7DA-A770EE461602}

ProgID - PowerTerm.Downloader

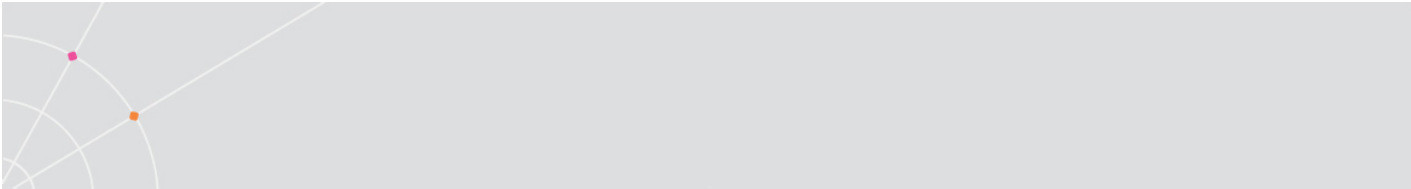
It can also be activated by COM compatible applications other than the browser, as well as a command prompt.

The Windows Downloader has been digitally signed by Ericom Software, and the signature has been verified by VeriSign. When the browser downloads the Windows Downloader it will display the certificate and ask the user to accept the component's installation.

HINT To avoid the certificate message, place the Web hosting the Windows Downloader in the browser's "Trusted sites" security zone. Alternatively, the user can select *always trust content from Ericom Software*. Once trusted, the certificate will not be displayed again, even if it is updated.

Features of the Windows Downloader

- During installation a progress bar is displayed showing: component's total size, percent downloaded, and an estimate of the remaining download time.
- Cancel button to terminate the download.
- Configurable download destination.
- Continues to download and install even if the browser is closed.
- Security notice is presented only once – the same Windows Downloader can download multiple client types.
- Once installed, it can download components to locked systems.
- Optional log file to troubleshoot failed installations.



Java Downloader

The advantages of using the Java downloader are:

- Cross-platform
- Cross-browser
- Works when security settings do not allow ActiveX.

The Java Downloader is a signed Java applet that is compatible with JVM 1.4.0 or higher. The Java Downloader should be used when ActiveX is not supported by the browser or operating system.

Ericom Software has digitally signed the Java Downloader, and VeriSign has verified the signature. When the browser downloads and launches the Java Downloader it will display the certificate and ask the user to accept the component's installation. To bypass this message, place the Web server address (where the Java Downloader is hosted) in the browser's "Trusted sites" security zone. Once selected, the certificate will not be shown again, even if updates are downloaded.

Features of the Java Downloader

- HTTPS protocol support
- Download progress indicator, showing the name and version of the component being downloaded
- Configurable download destination
- The ability to download components to locked systems (requires write access to download destination)
- Support for side-by-side installation of multiple client versions
- Error messages and log file to troubleshoot failed installations.

The Java Downloader does not connect to PowerTerm WebConnect Server, and thus does not require the user to login. It connects and downloads components from a standard Web server.

Using the Java Downloader involves complex JavaScript functions to support the user's operating system as well as the browser-enabled Java Virtual Machine version. All modifiable parameters are located in the Java Script configuration file *PtAgentSettings.js*. The Java Script functions located in *PtAgent.js* should not be changed.

<p>NOTE The Java Downloader uses JavaScript to modify its behavior based on the user's operating system and browser type. Browser scripting must be enabled in order to use the Java Downloader.</p>



Using Java Downloader with Internet Explorer

On Internet Explorer `downloader.js` will always try the ActiveX Downloader first. The ActiveX Downloader may fail to launch in the following scenarios:

- ActiveX is disabled by security settings
- User does not accept initial ActiveX installation
 - The user has 10 seconds to approve the use of ActiveX
- User does not have permissions to install ActiveX
- User does not notice browser notification for ActiveX installation or denies the installation.

When the ActiveX method fails and if `PT_useJavaOnIE` is set to `true`, then `downloader.js` will try to use the Java downloader.

<p>NOTE if the ActiveX Downloader is launched, but fails in its operation (i.e., the URL to the agent is incorrect) the Java Downloader will not be used.</p>
--

The Downloader process when ActiveX is denied on Internet Explorer:

- ActiveX Downloader fails to start.
 - a. Verify `PT_useJavaOnIE`. If it is 'false' then stop.
 - b. Check Java support in the browser. If the browser does not support Java then stop.
- Display message asking user to allow Java Downloader.
 - a. If user does not allow Java Downloader use then stop.
- Launch Java Downloader



6. NATIVE CLIENT INSTALLERS (MSI, PTSTART)

The PowerTerm WebConnect native client standalone installers consist of:

- MSI: Windows RemoteView, HostView, and AccessPad
- PKG: Mac AccessPad
- Online App stores: AccessToGo for iOS, Android, and Blackberry
- PtStart: Windows and Linux thin clients

MSI/PKG Installation

PowerTerm WebConnect provides Microsoft Windows Installer packages (MSI files) for all of its clients. Each PowerTerm WebConnect client is packaged in a separate MSI to support both manual and automated installation. Various settings such as the installation location can be specified manually via the user interface, or using standard command-line parameters (may not apply to all installers).

Mobile Client App Stores

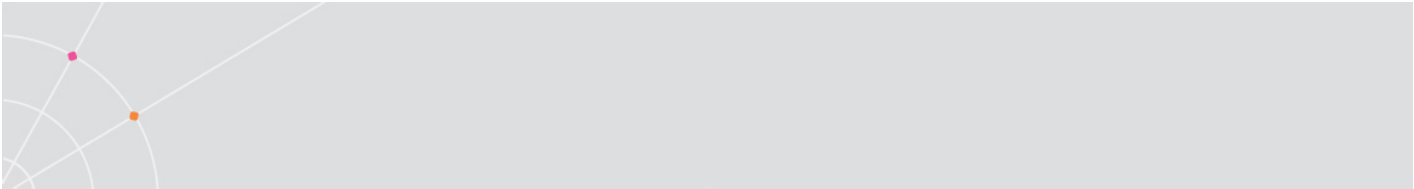
The AccessToGo app for mobile devices may be downloaded from the respective app store:

- Apple iOS: *Apple* App Store
- Android: *Google* Play or *Amazon* Appstore
- Blackberry: *Blackberry* World

PtStart Downloader

PtStart is an application that will download, install, and launch PowerTerm WebConnect Application Zone, primarily for thin client devices.

Each time PtStart runs, it checks the version of the PowerTerm WebConnect components on the server and compares it with the version of components previously downloaded to the device. If the versions are the same, then PtStart will run the PowerTerm WebConnect Application Zone. If PtStart finds that the PowerTerm WebConnect components on the server are of a newer version, then it will first download and install the newer version, prior to running the PowerTerm WebConnect Application Zone.



The first time PtStart runs it creates a configuration file, *PtStart.ini*, in the same folder as the downloader. This file contains the paths to the Install folder and the Working folder. The final path to these folders may vary depending on the thin client type.

It is also possible to define all PtStart.ini values in a parameter file located on the web server where PowerTerm WebConnect Application Zone is downloaded from. This parameter file will take precedence over PtStart.ini.

The parameter file names are:

- *WebConnect-Client-CE.ini.txt* for Windows CE Thin Client
- *WebConnect-Windows.ini.txt* for XPe Thin Client
- *WebConnect-LINUX.ini.txt* for Linux Thin Client

NOTE The PtStart downloaders do not currently work with the Ericom Secure Gateway (ESG).

PtStart for XPe Thin Client

NOTE Some thin client device are pre-installed with the "Ericom PowerTerm WebConnect Client" shortcut to start the PtStart Client.

The default Install and Working folders are:

- **Install folder:** C:\Documents and Settings\\Application Data\Ericom\Clients\- On Windows 7 and higher:
C:\Users\\AppData\Roaming\Ericom\Clients\\<Web Connect Host name>
- **Working folder:** C:\WebConnectClient\

It is possible to modify the path:

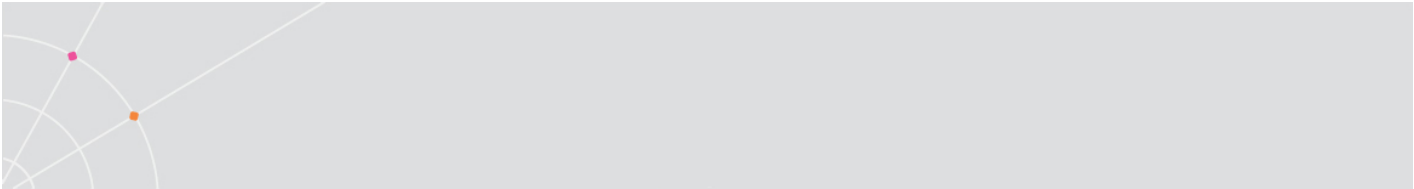
- **Create a text file on the PowerTerm WebConnect server machine:**
<WebConnect Server installation folder>\web\windows\PtStart\WebConnect-Client-Windows.ini.txt

The file syntax is:

[General]

Install-Folder=<desired path - where the WebConnect-Client-Windows.cab and WebConnect-Client-Windows.ver.txt are downloaded>

Working-Folder=<desired path - where the WebConnect-Client-Windows.cab is extracted>

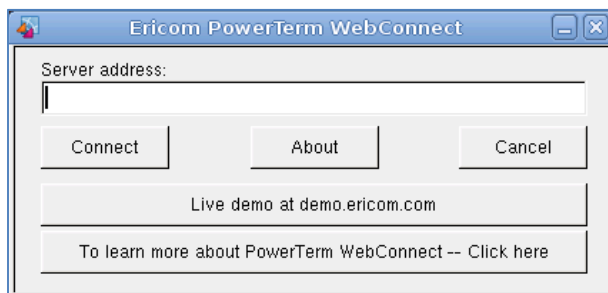


PtStart.ini Options

Option	Description
Address = <IP> <Full path of the zip file>	The Web server location or the full path of the PowerTerm WebConnect client ZIP file. If not specified, the user will be prompted for it.
Install-Folder = xxx	The folder where to download the zip and version files.
Working-Folder = xxx	The folder where to unzip the client components.

PtStart for Linux Thin Client

When PtStart for Linux is launched without any parameters, a dialog will appear requesting the PowerTerm WebConnect Server address.



Once connected to the PowerTerm WebConnect server, all necessary client components will be downloaded and the user login prompt will appear. PtStart can be configured to start with command line parameters to automate the connection and login process.

The default Install and Working folders are:

- \$HOME/Ericom

To modify the path:

- Create a text file on the PowerTerm WebConnect server machine:
<WebConnect Server installation folder>\web\linux\PtStart\WebConnect-Client-Linux.ini.txt

The file syntax is:

```
Install-Folder=<desired path - where the WebConnect-Client-Linux.zip and WebConnect-Client-Linux.ver.txt are downloaded>
```

Working-Folder=<desired path - where the WebConnect-Client-Linux.zip is extracted>

PtStart command line options

(All options start with a double minus "--")

--thin-client	The thin client command, needed to use with font, pre, and post command-line option parameters (see below).
--install-folder=xxx	The folder where to download the zip and version files.
--working-folder=xxx	The folder where to unzip all the client components.
--config-file=xxx	Specifies the full path and name to the PtStart.ini.
--parameters=xxx	qterm-wc parameters. Default: none
--locked	Does not save any changes to the PtStart.ini. Default: off
--log=xxx	Full path and filename to the log file. Default: no logging
--pre-font-install=xxx	Runs before installing the fonts.
--font-install-command=xxx	To install the fonts into the system. Runs in the fonts-folder directory and after the fonts are unpacked there.
--fonts-folder=xxx	Full path to the location where the fonts should be unzipped. Default: WORKING-FOLDER/fonts
--post-font-install=xxx	Runs after installing the fonts.
--pre-install-command=xxx	Runs before downloading a component.
--post-install-command=xxx	Runs after downloading a component.
--version	Returns the version of the PtStart application.
--help	Shows these command line options in a Terminal window.

Parameters limited with the --thin-client command-line option

Pre-Install-Command = xxx	Runs before downloading a component.
---------------------------	--------------------------------------

Post-Install-Command = xxx	Runs after downloading a component.
Pre-Font-Install = xxx	Runs before installing the fonts.
Post-Font-Install = xxx	Runs after installing the fonts.
Font-Install-Command	To install the fonts into the system. Runs in the fonts-folder directory and after the fonts are unpacked there.
Fonts-Folder = xxx	Full path to the location where the fonts should be unzipped. Default: WORKING-FOLDER/fonts

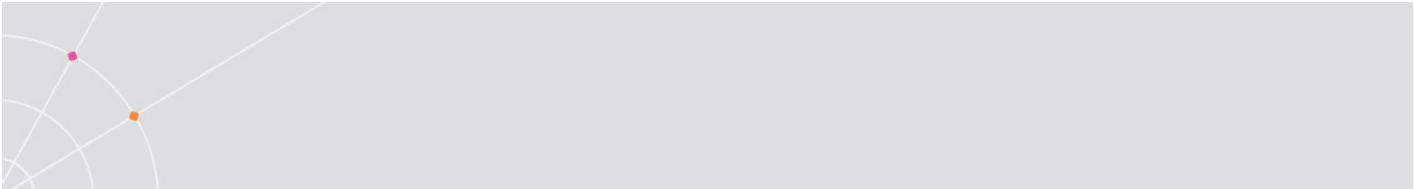
PtStart.ini options

Option	Description
Address = <IP> <Full path of the zip file>	The Web server location or the full path of the zipped PowerTerm WebConnect client. If not present, the user will be prompted for it.
Install-Folder = xxx	The folder where to download the zip and version files.
Working-Folder = xxx	The folder where to unzip all the client components. It is recommended to set the value of <i>/tmp/Ericom for thin clients</i> if the space in the home directory is limited.
Parameters = xxx	qterm-wc parameters. Default: none
Log = xxx	Full path and filename to the log file. Default: no logging
Locked	Does not save any changes to the PtStart.ini. Default: off
Override-Command-Line	Overrides all command line options.

PtStart for Windows CE Client

Select *Add* in the *Connection Manager* and then enter *Ericom WebConnect Client* to start the Ericom PowerTerm WebConnect Client.

The Install and Working folders are by default located:



- Install folder: ...\[persistent folder name]\WebConnect\- Working folder: ...\WebConnect\

The Install folder must be in a persistent location so that the files will remain after turning the thin client off.

It is possible to modify the path:

Create a text file on the PowerTerm WebConnect server machine:

<WebConnect Server installation folder>\web\Windows\PtStart\WebConnect-Client-CE.ini.txt

The file syntax should be:

[General]

Install-Folder=<desired path - where the WebConnect-Client-CE.zip and WebConnect-Client-wbt.ver.txt are downloaded>

Working-Folder=<desired path - where the WebConnect-Client-CE.zip is extracted>

PtStart.ini options

Option	Description
Address = <IP> <Full path of the zip file>	The Web server location or the full path of the zipped PowerTerm WebConnect client. If not specified, the user will be prompted for it.
Install-Folder = xxx	The folder where to download the zip and version files.
Working-Folder = xxx	The client components cache folder.

7. CUSTOMIZING CLIENT PARAMETERS

Command line parameters provide a useful method to control the behavior of the PowerTerm WebConnect clients. Parameter values are not case-sensitive.

NOTE Certain parameters listed in this section may not apply to Application Portal, AccessNow, AccessPad, and AccessToGo components. Certain command-line parameters, such as /COORD_DLG, are designed to work with the native components: ptagent.exe, ptrdp.exe and ptermx.exe.

To see the possible parameter values for a component, launch the component with the "/help" parameter.

Example Specifying Multiple Broker Addresses

Server's address and port number are in the following format:

<address>:port or address:port

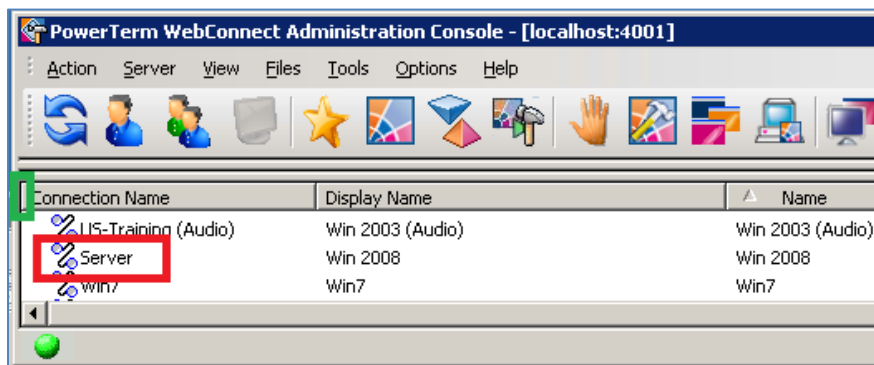
To specify a list of a broker address that the client should attempt to connect to, use the setting: <webserver>:4001, 192.168.0.100:4001

If the port number is omitted, the default (4000) is used. Example
Launching a Preset Connection

Connects to the PowerTerm WebConnect server 192.168.1.111 and auto-launches the RemoteView connection named "server". The parameters are not case sensitive.

ptagent 192.168.1.111 /run=remoteview extra_params=/connection=server

The "Connection Name" may be found using the Administration Tool. Drag the vertical subject bars from the left to right to reveal the field if it is hidden.



PtAgent.exe /help shows all available parameters:



```
PtAgent.exe <WebConnect-Server-Host>[:<WebConnect-Server-Port>]
[/USER=<user-name>] [/PASS=<password>] [/SID=<session-id>]
[/ssl-usage] [/WEBSOCKET] [/show-login-dialog-mode]
[/use-coordinator-dialog-mode] [/VAR="<var-name>=<var-value>" ...]
[/reconnect-mode] [/SHORTCUT[=<shortcut-location>]]
[/RUN=run-component-id [/EXTRA_PARAMS=<extra-params>]]
[/SYSTRAY[=REGULAR / HOLDUP / HIDE]] [/AUTOLOGIN[=YES / NO]]
[/INSTALL=install-component-id [/VERSION=<version>]]
[/CALL_ADMIN] [/CALL_SUPPORT]
```

NOTE that the regular, /RUN, /INSTALL, /CALL_ADMIN and /CALL_SUPPORT execution modes are mutual exclusive.

Where:

```
ssl-usage
    NOSSL
    SSL (*)
    SSLCERTFILE[=[*]<files-list>]
    SSLCERTPATH[=[*]<paths-list>]
show-login-dialog-mode
    C2S_DLG (*) or NO_C2S_DLG
use-coordinator-dialog-mode
    COORD_DLG (*) or NO_COORD_DLG
reconnect-mode
    RM_NONE (*), RM_ON_DEMAND, RM_WIRELESS or
RM_INTERACTIVE
shortcut-location
    DESKTOP (*), STARTUP, BOTH or DISABLED
run-component-id
    HostView, PrintView, RemoteView, QuickVNC, QuickFTP,
ADMIN, FTP, DFT
extra-params
    additional command line parameters to be passed to the
component
    SYSTRAY
        HOLDUP - after run put the Agent client on the system tray
        HIDE - hide the system tray icon
    AUTOLOGIN
        logins using the last saved credentials. YES is the default
install-component-id
    HostView, PrintView, tWebView
version
    the component version number
CALL_ADMIN
    Requests the WebConnect administrator's assistance
CALL_SUPPORT
    Requests the WebConnect tech-support's assistance
```

Commonly Used PtAgent.exe Parameters

(*) denotes the default value.

[*] if the designated file is not found, then it will be created.

SSL Encryption (ssl-usage)	<p>/NOSSL - disables SSL.</p> <p>/SSL - (*) enables SSL.</p> <p>/SSLCERTFILE[=[*]] - explicitly specifies the SSL certificate filename.</p> <p>/SSLCERTPATH[=[*]] - specifies the path for the SSL certificate.</p>
Login Dialog Display (show-login-dialog-mode)	<p>/C2S_DLG(*) - displays the Connection-to-Server dialog.</p> <p>/NO_C2S_DLG - does not display the Connection-to-Server dialog.</p>
Coordinator Dialog (use-coordinator-dialog-mode)	<p>/COORD_DLG(*) - displays the coordinator pop-up dialog to show event information.</p> <p>/NO_COORD_DLG - hide the dialog</p>
Reconnect Mode (reconnect-mode)	<p>/RM_NONE (*) - will not reconnect an interrupted session.</p> <p>/RM_ON DEMAND - will reconnect only sessions connected through the PowerTerm WebConnect server's gateway.</p> <p>/RM_WIRELESS - will reconnect any session automatically. All wireless sessions use the PowerTerm WebConnect server's gateway.</p> <p>/RM_INTERACTIVE - enables the client to select the mode during login.</p>
/USER=	<p>specifies a fixed value for the User Name field. Placing an asterisk in front of the user name will bypass the login dialog and use the defined credentials</p> <p>Enter ## as the username to use the optionally installed SSO component</p> <p>Enter two backslashes (/USER=\\) to always keep this field empty.</p>
/PASS=	specifies a fixed value for the user's

Password	
/RUN=	requires /RUN to be configured. This parameters specifies additional parameters that can be accepted by the client component, such as /CONNECTION
/EXTRA_PARAMS=	places a shortcut to the Application Zone executable on the user's desktop. If the shortcut is configured for a specific user, it will not be valid when copied to another user's profile (check the <i>Properties</i> of the shortcut for a valid path to the cached client component).
/SHORTCUT=DESKTOP	places a shortcut to the connection in the Windows Startup menu
/SHORTCUT=STARTUP	places a shortcut to the connection in both the desktop and the Windows Startup menu
/SHORTCUT=BOTH	REGULAR(*) – displays the systray icon HIDE – hides the systray icon
/SYSTRAY	HIDE – hides the Application Zone window
/WINDOWSIZE	Allows the user to save credentials to a local encrypted file on the system
/AUTOLOGIN=	

NOTE The FTP and DFT client do not support command-line parameters because they connect directly to the host

Client Failover Configuration

When there are multiple PowerTerm WebConnect servers, the clients can be configured to connect to a list of available servers.

To configure the client HTML file (i.e. ApplicationZone.html) change the parameter value of the PowerTerm WebConnect server (default: <WebServer>) to a list of PowerTerm WebConnect server. Separate the server names using a semi-colon.

EXAMPLE: <PARAM NAME="Parameters" VALUE="192.168.0.100; 192.168.0.101; 192.168.0.102 /RUN=RemoteView">



Admin Console Failover Configuration

- Launch the Administration Tool. The Connect dialog appears.
- Type the WebConnect server names in Host Name.
- Enter other parameters.
- Click Connect.

NOTE Separate the list of servers with semi-colons `;`

Using /AUTOLOGIN=

This allows the user to save credentials to a local encrypted file on the system. The credentials file will be created in the user's application folder (C:\Documents and Settings\\Local settings\Application Data\Ericom\). The credentials are saved in an *encrypted* format that is user and machine specific. Exiting the Application Zone will erase the credentials based on the setting *AGENT_ExitCleanMode*. If the credentials are incorrect, the login dialog will be displayed with the current values pre-entered into the fields, and the *Save Credentials* box checked. When the user clicks *Connect* and the logs on to PowerTerm WebConnect successfully, the new values will be saved to the credentials file, overwriting the exiting one. In this scenario, if the user clears the checkbox, the credentials file is deleted.

To clear saved credentials right-click on the Agent icon in the system tray and select *Clear Credentials*. The possible values for /AUTOLOGIN are:

- *YES* – If the credential file exists, the login dialog will not be displayed. Otherwise, the login dialog will be displayed.
- *NO* - disabled
- *INTERACTIVE* - If the credentials file exists, and the user changed the credentials when the check box is still ON, the user will be asked to save the updated credential information.
- *FIRST INTERACTIVE* – (Default setting) If the credential file exists, the login dialog will not be displayed. Otherwise, the login dialog will be displayed and the Save Credentials check box will be displayed.
- Empty, missing or invalid value - use *FIRST INTERACTIVE*


Using /EXTRA_PARAMS=

This is a list of additional command line parameters that will be passed to the native client via the Application Zone (ptagent.exe). Any valid parameters for ptrdp.exe and ptermx.exe are passed using this setting when the component is launched using ptagent.exe.

NOTE When defining a parameter string with both the /RUN and /CONNECTION parameters - ensure that the connection is supported by the client. If /USER is also defined, make sure that it has access to the specified connection.

Available RemoteView (PtRDP.exe) Parameters

PtRDP.exe /help shows all available parameters:



PtRdp.exe <WebConnect-Server-Host>[:<WebConnect-Server-Port>]
[/USER=<user-name>] [/PASS=<password>] [/SID=<session-id>]
[/ssl-usage] [/WEBSOCKET] [/show-login-dialog-mode]
[/use-coordinator-dialog-mode] [/VAR="<var-name>=<var-value>"
...] [/reconnect-mode] [/CONNECTION=connection]

Where:

- ssl-usage
 - NOSSL
 - SSL (*)
 - SSLCERTFILE[=[*]<files-list>]
 - SSLCERTPATH[=[*]<paths-list>]
- show-login-dialog-mode
 - C2S_DLG (*) or NO_C2S_DLG
- use-coordinator-dialog-mode
 - COORD_DLG (*) or NO_COORD_DLG
- reconnect-mode
 - RM_NONE (*), RM_ON_DEMAND, RM_WIRELESS or RM_INTERACTIVE
- connection
 - a valid WebConnect RemoteView connection name

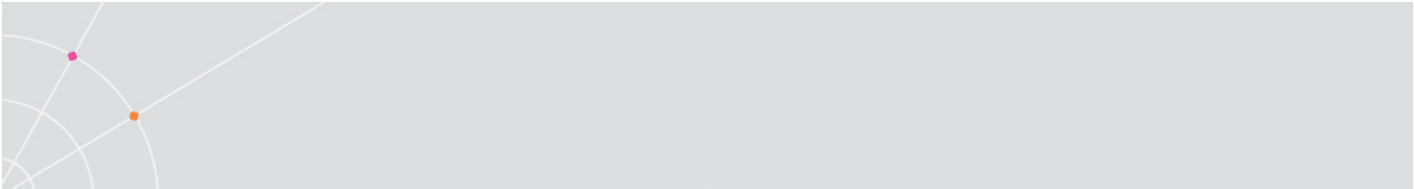
Example

Auto-login with username and password "example". Auto-launches the RemoteView connection named "MyTerminalServer"

```
PT.agentParameters = " -wc-client " + PT.server + " /SHORTCUT=BOTH  
/AUTOLOGIN=NO /USER=*example /PASS=example /RUN=RemoteView  
/EXTRA_PARAMS=/CONNECTION=MyTerminalServer"
```

Launching one Application with AccessNow

PowerTerm WebConnect's Application Portal may be configured to launch just one application using AccessNow. AccessNow does not support the client parameters, so the desired application must be hard-coded into the *main.js*



file (under the AppPortal folder). Back up the original file before making any changes. The sg* pages may also be used to test this functionality.

Multiple sets of the Application Portal pages may be created manually to create access pages for multiple applications.

To configure the Application Portal to always launch a single application, perform the following:

- Open the *main.js* file
- Find this line in the *Loaded()* function:
document.getElementById("ericom").focus();
- (Optional) To open the AccessNow session in the same browser window as the Application Portal, add this line right below the line from step 2:

```
AccessNow_Same_Tab = true;
```

- To specify the application to be launched automatically upon Application Portal login, add this line below that of step 2 or step 3 (case sensitive):

```
Run(null, 15, "Calculator #1", "Calculator Application");
```

- *Calculator #1* represents the unique PowerTerm WebConnect *Connection name* of the desired application
- *Calculator Application* represent the browser tab title that the user will see when the application is launched using AccessNow.

Available HostView (Ptermx.exe) Parameters

Ptermx.exe /help shows all available parameters:



```
ptermX.exe <WebConnect-Server-Host>[:<WebConnect-Server-Port>]  
[/USER=<user-name>] [/PASS=<password>] [/SID=<session-id>]  
[/ssl-usage] [/WEBSOCKET] [/show-login-dialog-mode]  
[/use-coordinator-dialog-mode] [/VAR="<var-name>=<var-value>"  
...] [/reconnect-mode] [/CONNECTION=<connection-name>]  
[/LANGUAGE=language-id]
```

Where:

```
ssl-usage  
    NOSSL  
    SSL (*)  
    SSLCERTFILE[=[*]<files-list>]  
    SSLCERTPATH[=[*]<paths-list>]  
show-login-dialog-mode  
    C2S_DLG (*) or NO_C2S_DLG  
use-coordinator-dialog-mode  
    COORD_DLG (*) or NO_COORD_DLG  
reconnect-mode  
    RM_NONE (*), RM_ON_DEMAND, RM_WIRELESS or  
RM_INTERACTIVE  
language-id  
    EN = English (*)  
    FR = French  
    DE = German  
    IT = Italian  
    ES = Spanish  
    ? = as specified in the Regional Settings
```

NOTE When calling HostView via ptagent.exe, insert desired HostView parameters as EXTRA_PARAMS values

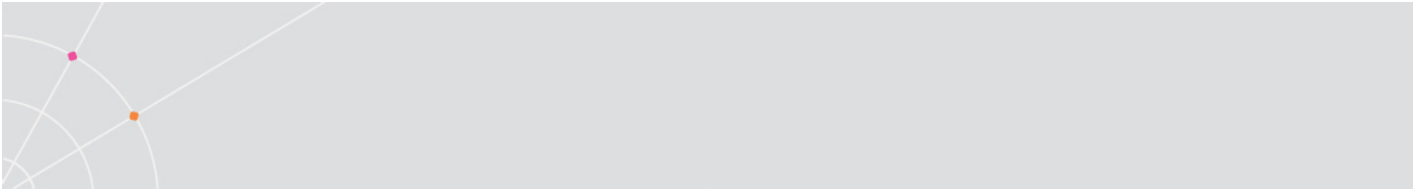
Example

Auto-login with username and password "example". Auto-launches the HostView connection named "Example_VT"

```
PT.agentParameters = " -wc-client " + PT.server + " /SHORTCUT=BOTH  
/AUTOLOGIN=NO /USER=*example /PASS=example /RUN=HostView  
/EXTRA_PARAMS=/CONNECTION=Example_VT"
```

Automatic Server Discovery

PowerTerm WebConnect includes an automatic server discovery mechanism. This is useful when the PowerTerm WebConnect client (e.g. a thin client) does not know where the server is located. In order to use this feature, both



PowerTerm WebConnect Server and the client must be on the local network. The server broadcasts a signal every X seconds so the client can detect its location.

Server-side configuration

- Open the *PtServer.ini* file (PowerTerm WebConnect Administration Tool, *Files | Configuration | Main*)
 - Find *BroadcastConnectionPoint* configure the following:
 - none* (default) – no broadcasting
 - internet* – use the port defined for PowerTerm WebConnect Server in *PtServer.ini* under <server connection point>
 - internal use* – use the port defined for PowerTerm WebConnect Server in *PtServer.ini* under <server connection point>
- BroadcastPort* = <default> (4080)
BroadcastIntervalSecond = 5

Client-side configuration

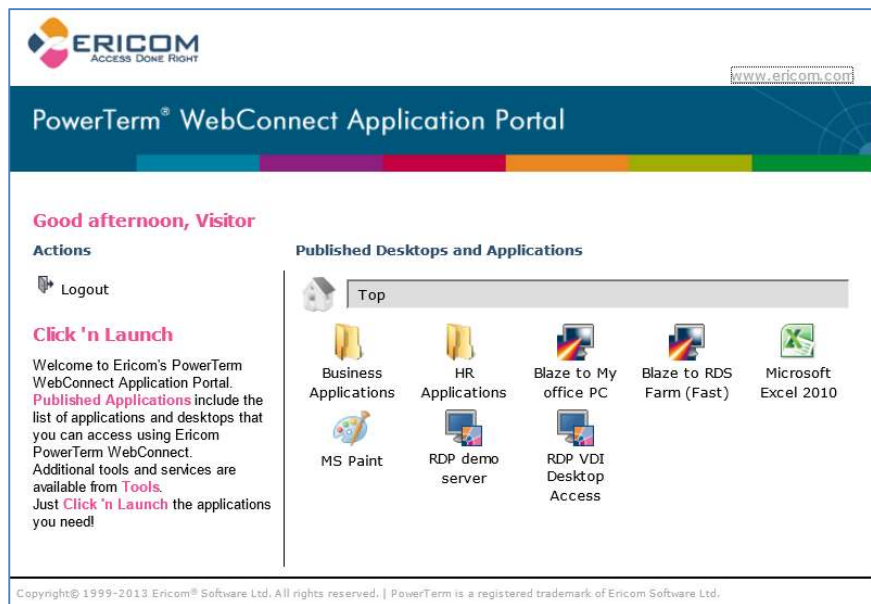
- On the client-side command line add
- */broadcast* – Listen for the server broadcasting and connect to the first discovered server.
- */broadcastlist* – List all the broadcasting servers and let the user select to which one to connect to.
- If the server's *BroadcastPort* is different from the default port (4080), then add **[=listen_port]** to **/broadcast** and **/broadcastlist** for the client.

8. POWERTERM WEBCONNECT APPLICATION PORTAL

The Web Application Portal provides a web based interface to access published applications. Popular web browsers are supported: Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, etc. The purpose of the Application Portal is to give users one easy to use interface to access published resources. Certain Application Zone features are not available, such as Desktop icons, Start menu icons, and the systray agent.

Published applications are launched directly from the browser by means of an ActiveX control or Java applet (the best method is automatically selected based on the client operating system and browser type.) The Application Portal is designed to run on Microsoft's Internet Information Server (IIS) version 5 or higher.

The Application Portal can be deployed on the same system running the PowerTerm WebConnect Server or on a separate server.



NOTE With the introduction of the Ericom Secure Gateway, the need to install Application Portal on a dedicated web server (i.e. in the DMZ) will be reduced or eliminated. In most cases, the Application Portal can simply run in the same server as PowerTerm WebConnect.

Application Portal Configuration

During the Application Portal installation process, a COM (ActiveX) object named *ComPortal* is installed on the Web Server. This COM object is responsible for communication between the Web Server and the PowerTerm WebConnect Server. The ComPortal is also used by AccessToGo. The ComPortal files are installed in the `\ComPortal` directory on the Web Server.

NOTE ASP processing may be disabled by default on Microsoft IIS. The PowerTerm WebConnect installation checks for ASP, and attempts to enable it if it is disabled. If the Application Portal does not work properly, verify that ASP is enabled.

The ComPortal.ini

The PowerTerm WebConnect Application Portal loads the configuration parameters from *ComPortal.ini* file. The ComPortal.ini can be edited using a text editor. However, any changes made to the parameters will not take effect until the ComPortal object is reloaded by the Web Server. To reload ComPortal.ini - reset IIS Server by running *IISReset* using the command prompt.

```
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
C:\Users\Administrator>_
```

ComPortal Parameters

Server=... denotes the properties of a connection to a PowerTerm WebConnect server. Multiple PowerTerm WebConnect Server records can be defined in the Comportal.ini file. This will allow one web server to host multiple Web Application Portals for different PowerTerm WebConnect servers.


```

[General]
MaxLogFileSizeK=<Default>
MaxLogBackups=<Default>
LogFlags=Run Services

[Server=webConnect]
Address=localhost:4000
CustomAddress=
SSL-Certificate=
Min-Instances=1
Max-Instances=10
Initial-Instances=1
Watch-Frequency-Seconds=15
Inactivity-Timeout-Seconds=60

[Server=Production]
Address=192.168.1.105:4000
CustomAddress=192.168.1.105:4000
SSL-Certificate=
Min-Instances=1
Max-Instances=10
Initial-Instances=1
Watch-Frequency-Seconds=15
Inactivity-Timeout-Seconds=60

[Server=vendorRemote]
Address=ptwc-customer:5000
CustomAddress=ptwc-customer:5000
SSL-Certificate=
Min-Instances=1

```

A Server record is reference by the portal's *LoggedIn.asp* page in the *PtUser.Authenticate* function. This allows multiple Portals to reside on the same server and reference a common Comportal.ini. Here is an example of how a server record is configured in a portal's *LoggedIn.asp* page:

```

On Error Resume Next
Set PtUser = Server.CreateObject("PtComPortal.user")
If (Err.Number <> 0) Or (Not IsObject(PtUser)) Then
HandleErrorEx "index.asp", "Failed to create webConnect object. on x64 web server"
Exit Sub
End If
Set Session("PtUser") = PtUser

Result = PtUser.Authenticate("WebConnect", Username, Password, Domain)
If Result <> 0 Then

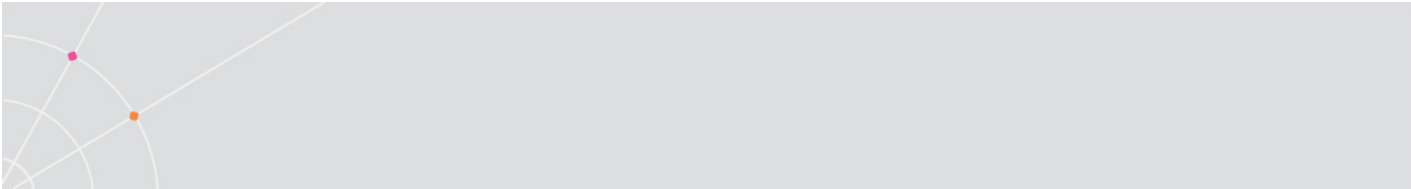
```

For each PowerTerm WebConnect Server, a pool of special portal sessions is maintained by the ComPortal component. Sessions from this pool are used to obtain information from the PowerTerm WebConnect server. These Portal sessions are not associated with any specific user; instead they can retrieve information for any user connected to the Application Portal.

The Portal sessions are stateless and each session that is processing a service is busy until the service is completed. The availability of the Portal services depends on the number of Web sessions that require Portal services as well as the size of the session pool. Increasing the number of sessions in the pool will improve availability, but will also increase the load on the PowerTerm WebConnect Server and the web server.

Address – is the address and port of the PowerTerm WebConnect Server to which ComPortal (web server) will connect to. Default is localhost:4000.

CustomAddress - address and port of the PowerTerm WebConnect Server in *relation to the end-user device* (client). If not specified, then the default IP address of the PowerTerm WebConnect Server will be used.



If there are external clients connecting to an internal PowerTerm WebConnect server via Application Portal, add the PowerTerm WebConnect Server external IP to this list.

If the *CustomAddress=71.86.93.111*, 71.86.93.111 represents the external IP of the PowerTerm WebConnect server

Multiple addresses are separated by semicolons with no spaces. Add the port number to the end of the string as shown below:

```
CustomAddress=66.252.166.135;demo.ericom.com;172.0.1.1:443
```

```
CustomAddress=66.252.166.135;demo.ericom.com;172.0.1.1:4000
```

In this example, there are multiple *CustomAddress* definitions for multiple ports. Note that the port number is added once, only to the end of the string. After changing the settings run *IISRESET* from the command prompt.

SSL-Certificate – the location of the PowerTerm WebConnect Server's SSL certificate, if available. This certificate will be used to authenticate communication between the web server and the PowerTerm WebConnect Server. The default is empty which indicates that there is no SSL certificate and server authentication will not take place.

Initial-Instances – the number of sessions that will be connected to the PowerTerm WebConnect Server at the initial start. Default is 0.

Min-Instances - minimum number of sessions that will be generated and connected to the PowerTerm WebConnect Server. Cannot be less than Initial-Instances. If it is set to a value less than Initial-Instances, then Initial-Instances will be set to Min-Instances. Default is 0.

Max-Instances - the maximum number of sessions that can concurrently be connected to the PowerTerm WebConnect Server. Default is 10.

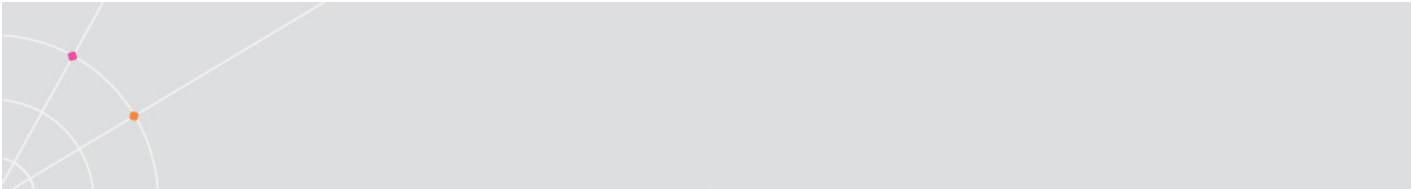
The last three parameters specify the size limits of the pool of sessions connected to a specific PowerTerm WebConnect Server and the pool's initial size.

Watch-Frequency-Seconds - at the end of this period of time, the pool will check that there are at least Min-Instances number of sessions connected to the WebConnect server. If the number of sessions in the pool is less than Min-Instances, the pool manager will create additional pool sessions. There may be more than one [Server=...] record section in order to define more than one PowerTerm WebConnect Servers. Each record corresponds to a session pool. Default is 15.

Logging Parameters

ComPortal can generate a log file to assist in identifying problems. The *ComPortal.LOG* log file resides in the same folder as the *ComPortal.dll* file.

[General] section - this contains the common configuration attributes.



MaxLogFileSizeK—maximum size of the LOG file, in kilobytes.

- <Default> is 1 MB (1024KB).

MaxLogBackups—maximum number of log file backups saved, in kilobytes.

- <Default> is 10.

LogFlags

- *Run* - general software workflow flags.
- All of the following are services provided by the WebConnect Portal client:
 - Authenticate.
 - GetConnectionsList.
 - GetLoginTicket.
 - AddLoginVariable.
 - GetServerAddress.
 - GetPreferenceValue.
 - SetPreferenceValue.
 - GetConnectionIcon.
- All—log all the above services and is equivalent to specifying Authenticate GetConnectionsList GetLoginTicket.

The “< Portal >” Special User

For portal connections PowerTerm WebConnect Server uses a special user named < *Portal* >. This user is used for the communication between the Web Server and the PowerTerm WebConnect Server, regardless of the user actually logged into the Application Portal. < *Portal* > has special attributes and should not be used to manually log in to PowerTerm WebConnect.

To disable Portal access open the Main Configuration file (PtServer.ini) and set [*Server*]UsePortalUser to *False*.

<p>NOTE < <i>Portal</i> > user must not be modified or deleted. If this user is deleted - all PowerTerm WebConnect portal clients that are connected will be shut down. Until the <Portal> user is recreated, Portal clients will not be able to log on. In order to recreate the <Portal> user, the parameter [<i>Server</i>] UsePortalUser must be set to True.</p>
--

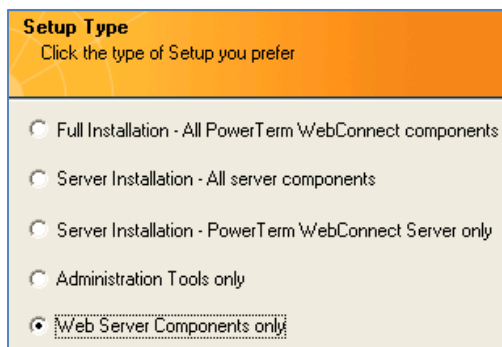
Installing Application Portal on PowerTerm WebConnect Server

The default WebConnect Server installation installs the Application Portal on the same system as the PowerTerm WebConnect server.

In this installation scenario there is no need to modify any ComPortal.ini parameters. The default parameters of the ComPortal.ini point to localhost, which is the PowerTerm WebConnect server.

Installing Application Portal on a separate web server

The Application Portal can be installed on a separate web server from the Ericom PowerTerm WebConnect server. To install, simply run the Ericom installer on the desired web server (Windows only). At the *Setup* type dialog, select *Web server Components only*.



NOTE The Portal can only be used on Windows based web servers because the *ComPortal.dll* is required and needs to be registered on the web server.

Once the installation is completed, go to the **PowerTerm WebConnect Server** and edit the following parameter in the Main Configuration (PtServer.ini) [Portal] section:

- *Machines* - enter the IP address(es) and the name(s) of the web (IIS) server(s). By default this is set to localhost. To specify multiple Web servers separate each address with a semi-colon `;`.

Next, edit the Comportal.ini on the web server and update the following:

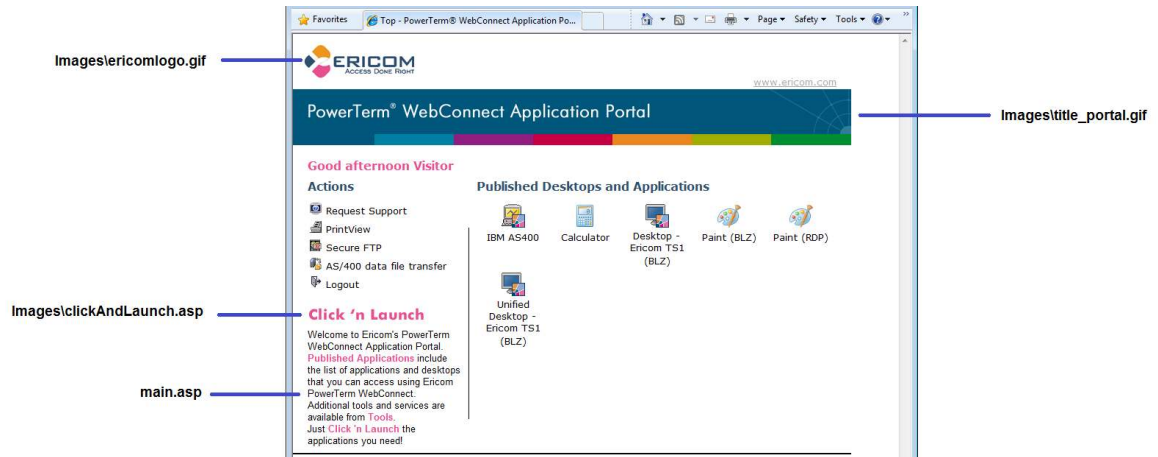
Address=	the address of the target PowerTerm WebConnect server (<i>respective of the web server</i>)
CustomAddress=	the address of the target PowerTerm WebConnect server (<i>respective of the client devices</i>)

Modifying the Portal's Interface

To manually modify the portal settings, navigate to its source folder.

NOTE Before making any changes, backup the current files for easy recovery in case an error is made during editing.

Certain images can be replaced (in the *Images* directory) to modify or brand the Portal. Portal text can be modified under the *index.asp* and *main.asp* files.



Allow Multiple Instances of Application

By default, each time a user clicks on a connection in the Application Portal, only one instance of the application will be launched. If the user clicks on the application again, any active instance of the application appear in the foreground.

To allow multiple instances of the same application, add this configuration:

- Set the Terminal Server to not restrict users to one session
- Modify the Main.js file and change:

```
connections[name] = window.open(url);
```

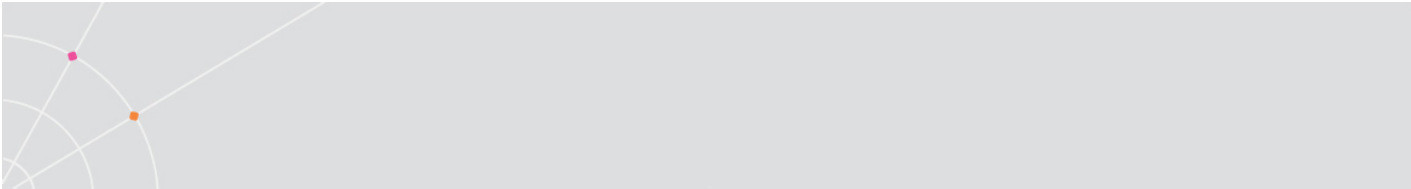
to...

```
var randomnumber=Math.floor(Math.random()*100000001)
connections[name + randomnumber] = window.open(url);
```

Configuring the Session Timeout

To set the Application Portal idle timeout setting:

- Open the Comportal.INI file (..\WebConnect x.y\ComPortal)
- Enter the desire value for Inactivity-Timeout-Seconds
- The value is set in seconds, the default is 60



Troubleshooting

- Examine the *ComPortal.ini* file found in the *\ComPortal* directory for correct settings, in particular the Server name and IP address.
- Verify that the *Comportal.dll* and *OpenSSL.dll* files are present under the *Comportal* directory. If they are not present, launch the batch file *FixComPortal32.bat* (or *FixComPortal64.bat* on x64 servers). After running the batch file, run *iisreset.exe* and then try to login to the Application Portal again.

NOTE On systems with UAC enabled - the batch file must be run as an *Administrator*

- Try restarting the IIS Server by running the *IISreset* command.
- Try to enable 32 bit applications on x64 web servers
 - `cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"`
- If users are receiving a "Service Unavailable" message, re-register ASP.NET using the command prompt:
 - `C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i`
- Examine the *ComPortal.LOG* file found in the *\ComPortal* directory for an indication of where the attempted communication might have failed. Communication failures are indicated by rows starting with ***** ERROR ***** or ***** WARNING *****. Any services showing long elapsed times should be investigated.

LOG file samples

Cannot find WebConnect Server: This error is caused by the *ComPortal.ini* parameters pointing to an incorrect *WebConnect* Server address. An sample of the LOG file showing this error displayed below.

```
*****
06/09/25 09:21:14.259 |      820 | C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll loaded
|      Version: 0.9.7.10
|      Built  : 06/01/15 14:49:48
06/09/25 09:21:25.934 |      820 | Service 'Authenticate' started.
06/09/25 09:21:25.949 |      f28 | Connecting to server 'demo20031', port 4000...
06/09/25 09:21:28.409 |      f28 | *** ERROR *** [1095]
| Cannot connect to server:
| NO_DATA error encountered calling
'gethostbyname' (#11004)
| The requested name is valid, but no data of the
```

Web server is not in Machines list: This error occurs when the Web Server address is not defined in the *PtServer.ini* file. There will also be an entry in the Intruder Record showing "Unknown user <Portal>".

```
*****
```

```

06/09/25 09:25:16.445 |      880 | The login request was sent
06/09/25 09:25:16.476 |      880 | Login rejected:
| State : 5
| Reason: The access of user '< PORTAL >' to is
denied.
| Please contact your system administrator.

```

User <Portal> does not exist: This error is caused when the *UsePortalUsers* in the *PtServer.ini* file is *False*. There will be an entry under *Intruders* showing “Unknown user <Portal>”.

```

*****
06/09/25 09:30:02.832 |      790 | Starting the pre-identification handshake...
06/09/25 09:30:04.381 |      790 | Sending the login request...
06/09/25 09:30:04.397 |      790 | The login request was sent
06/09/25 09:30:04.397 |      790 | Login rejected:
| State : 4
| Reason: The user '< PORTAL >' is not defined

```

Cannot Login to Portal– No Errors

If the *index.asp* page does not allow any logins and the logs do not reveal any information, something may be corrupted and a reinstall will be required. The Comportal log will appear like the following:

```

*****
13/04/26 16:31:42.494 |      1472 | Attaching to C:/Program Files (x86)/Ericom
Software/WebConnect 6.0/ComPortal/ComPortal.dll
|      Built   : 12/05/20 16:10:50
13/04/26 16:31:42.498 |      1472 | Loaded by 'C:/Windows/SysWOW64/regsvr32.exe'.
13/04/26 16:31:42.502 |      1472 | Program arguments:
13/04/26 16:31:42.503 |      1472 | [Run] Loading client pools.
|      INI file: C:/Program Files (x86)/Ericom
Software/WebConnect 6.0/ComPortal/ComPortal.ini
13/04/26 16:31:42.505 |      1472 | [Run] Loading the 'WebConnect' pool.
13/04/26 16:31:42.509 |      1472 | [Run] Client pools loaded.
13/04/26 16:31:44.352 |      1472 | _DllMain( DLL_PROCESS_DETACH )
13/04/26 16:31:44.408 |      1472 | Detaching from C:/Program Files (x86)/Ericom
Software/WebConnect 6.0/ComPortal/ComPortal.dll
|      Built   : 12/05/20 16:10:50
13/04/26 16:31:49.414 |      1472 | _DllMain( DLL_PROCESS_DETACH ) done

```

9. ADMINISTRATION TOOL

The PowerTerm WebConnect Administration Console manages published resources, user sessions, and server configuration.

Launching the Administration Tool

There are several methods to launch the Administration Tool:

- From PowerTerm WebConnect Server's *Start* menu select *Programs | Ericom Software | PowerTerm WebConnect x.x | PowerTerm WebConnect Administration Tool*
- Double-click *PtAdmin.exe*, located in the *bin* directory of the PowerTerm WebConnect application folder.

NOTE You can pass the port number to the Administration Console as a command line parameter, using the following syntax: *-port=port-number*

HINT "C:\Program Files\Ericom Software\PowerTerm WebConnect\bin\PtAdmin.exe" -port=778

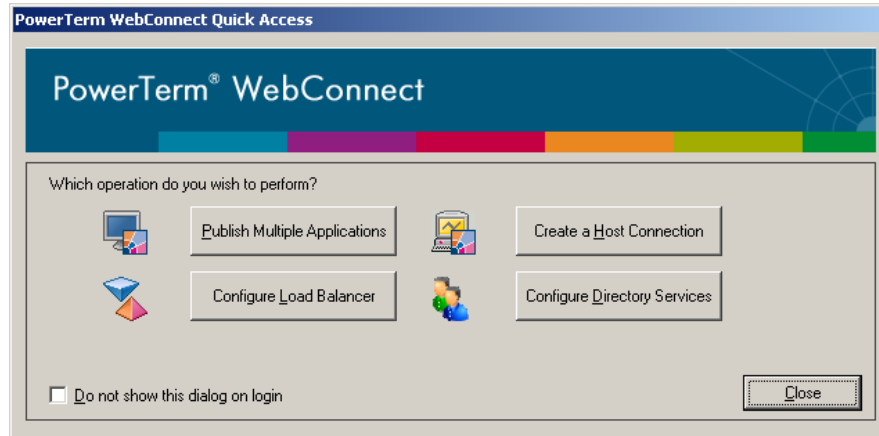
When launching the Administration Console for the first time the *Connection* dialog appears with the user "Administrator" entered as the username. There is no initial password, just click *Connect* to login.

In the *Connection* dialog, the *Host Name* appears as *localhost*. This is correct only if the Administration Console is being launched from the PowerTerm WebConnect server. If the PowerTerm WebConnect server is running from a different machine, enter its IP address/host name.

NOTE If multiple administrators are connecting to the *Administration Tool* from multiple RDP sessions on the same Terminal Server, make sure to go the *Administrator* user's *Properties* and enable *Allow Concurrent Machines*. Each RDP session is counted as a unique session.

Allow Concurrent Machines

Quick Access Screen



- *Publish Multiple Applications*, opens the *Publish Multiple Applications wizard*.
- *Configure Load Balancer*, opens *PowerTerm WebConnect Load Balancer Administration Tool*.
- *Create a Host Connection*, opens the *Add Connection dialog*.
- *Configure Directory Services*, opens the *Directory Services dialog*.

Administration Console Interface

The Administrator Console is comprised of the following components:

Menu bar: used to modify and refresh the information tables, launch wizards to publish applications and desktops, manage objects, etc.

Toolbar: icons to launch commonly used functions.

Information panes: shows properties and real-time information for users, groups, connections, sessions and intruders.

Properties dialogs: used to modify existing object and server settings.

Viewing Users, Groups, and Connections

To display the *Users* pane select *View | Users* or click its icon from the toolbar.



To display the *Groups* pane select *View | Groups* or click its icon from the toolbar.



To display the Connections pane select View | *Connections* or click its icon from the toolbar.



Modifying the View Pane

Most information panes uses a table structure to display relevant information. Useful information panes include:

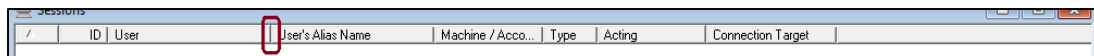
- Client Sessions
- Administrative Sessions
- Intruders
- Users
- Groups
- Connections

Each table row represents an object, queue, or session, while each column represents a property or a piece of runtime information about the object. Additional rows are added when new objects are created. In some views, new rows are added when new queues are generated or sessions established.

Changing Column Width and Order

The width of columns can be changed manually, or automatically expanded to show the entire contents of the column.

Column divider on the column title bar:



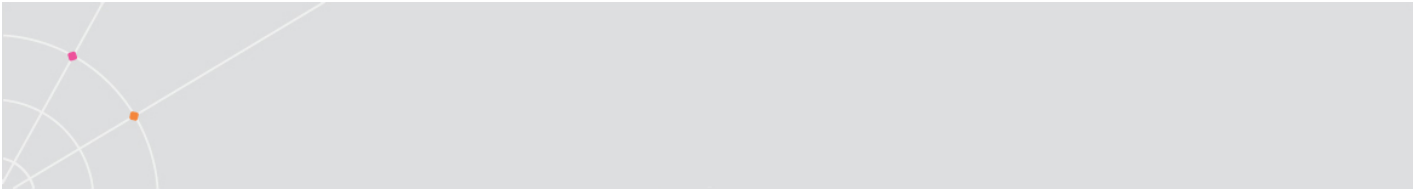
NOTE To see the contents of a column without resizing it, position the mouse over a column title, or a certain line, to see a tool-tip with the full text.

Manually change column width

Mouse-click the column divider and move (drag-and-drop) it right or left to adjust.

Automatically expand a column

Right-click on the column title.



NOTE If the column is empty, the right-click will have the opposite effect: the column will be narrowed to the smallest width

Change the position of a column

Click the column's title and drag and drop it to the desired position.

Hide a column

Certain columns may be hidden so the table only shows desired property settings or status information. Mouse-click the column divider and move (drag-and-drop) it left until the column is hidden. A hidden column may be revealed by clicking the same divider and moving to the right.

NOTE Columns that are not visible are actually set to a width of 0 (zero).

Sorting Tables

Tables can be sorted by clicking the column's title. The column that is clicked will become the primary sorting field. When clicking another column, that field will become the primary sorting field and the previously selected column will become the secondary field. When several objects have the same value for the primary field, those objects are sorted by the secondary field.

The Administrator User

The *Administrator* user is a local PowerTerm WebConnect account. This is not the local system or domain administrator account. The password is initially empty and should be changed immediately. Change the Administrator's password by opening its property page and clicking *Password>>>*.

Initially, the Administrator user can only login to the Administration Console from the PowerTerm WebConnect server. To change this, go to the Administrator's property page and change the *Access Limit Mode to Unlimited*.

HINT It is recommended to launch the Administration Console from a workstation so it does not consume resources from the PowerTerm WebConnect server. Only do this after the Access Limit Mode has been set to *Unlimited*. To allow multiple administrators to login, check *Allow Concurrent Machines*.

Closing the Administration Tool

To close the Administration Console select *Action | Exit*. A confirmation dialog will appear. Click *Yes* to close the application.

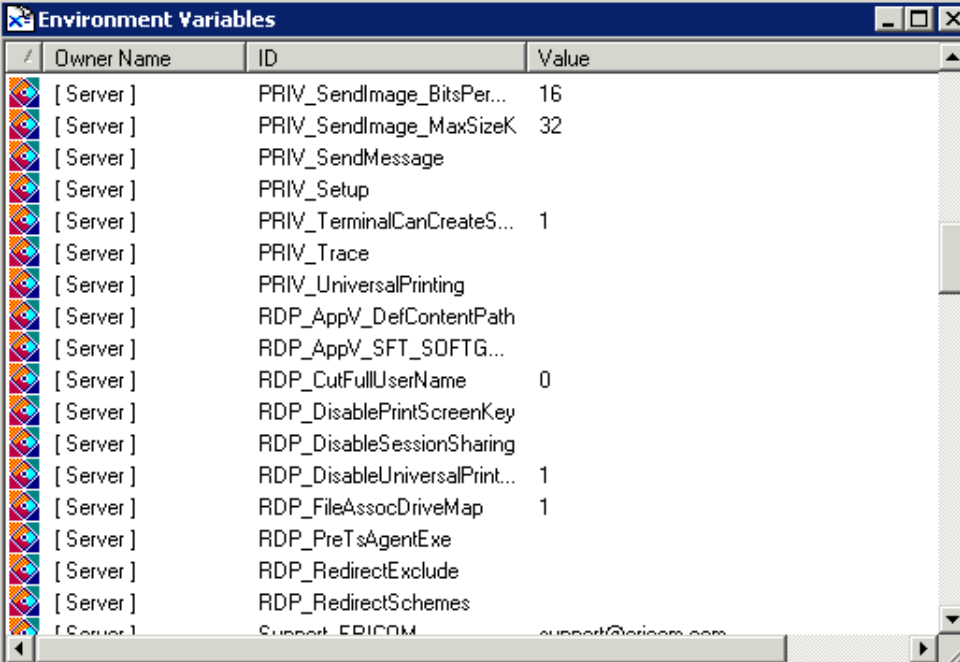
NOTE Closing the Administration Console does not stop the PowerTerm WebConnect Server service.

Useful Functions

Environment Variables


PowerTerm WebConnect provides environment variables to configure advanced features of the server. Environment variables can be defined on for a user, group, connection, or the PowerTerm WebConnect Server.

The *Environment Variables* window shows all defined variables for PowerTerm WebConnect, whether they are defined for users, groups, or the server object. See the Appendix for a full list of available environment variables.



Owner Name	ID	Value
[Server]	PRIV_SendImage_BitsPer...	16
[Server]	PRIV_SendImage_MaxSizeK	32
[Server]	PRIV_SendMessage	
[Server]	PRIV_Setup	
[Server]	PRIV_TerminalCanCreateS...	1
[Server]	PRIV_Trace	
[Server]	PRIV_UniversalPrinting	
[Server]	RDP_AppV_DefContentPath	
[Server]	RDP_AppV_SFT_SOFTG...	
[Server]	RDP_CutFullUserName	0
[Server]	RDP_DisablePrintScreenKey	
[Server]	RDP_DisableSessionSharing	
[Server]	RDP_DisableUniversalPrint...	1
[Server]	RDP_FileAssocDriveMap	1
[Server]	RDP_PreT'sAgentExe	
[Server]	RDP_RedirectExclude	
[Server]	RDP_RedirectSchemes	
[Server]	Support_EPICOM	support@epicom.com

Creating a new Environment Variable

- Double-click or right-click on the desired User or Group and select *Properties*. The Properties dialog appears. Define server values using Server | *Configuration*.
 - Click . The Define Environment Variable dialog appears.
 - Type the new environment variable's name and set its value.
 - Set the encryption type.
 - Click *OK* and the new environment variable will appear in the list.

NOTE Environment variables can be copied and pasted between different user and group properties. However, only one dialog can be open at a time.

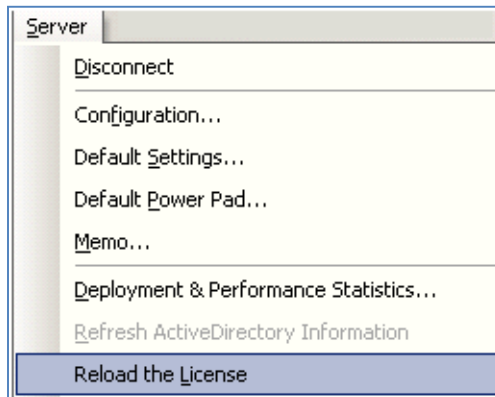
Modifying Existing Environment Variables

Open the Environment Variables Window by selecting View | Environment Variables. Double-click on the variable to be modified. Make any modifications and click OK to apply.

NOTE Non-persistent LDAP user objects cannot have Environment Variables added to them.

Load License (Server menu)

Use this function to load newly entered activation keys.



Refreshing the Information Tables

Information view data can be set to refresh at a fixed interval or manually.

Refresh all information tables manually

Select View | *Refresh I/O Information* or press F5.

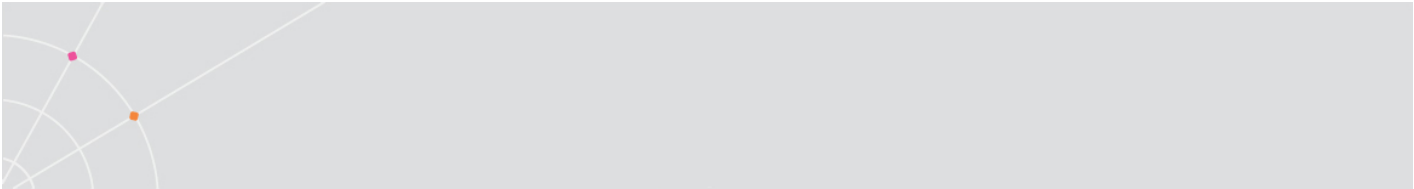
Set the automatic refresh interval

Select Server | *Configuration*. Set the refresh time interval under Administrator | *Auto Refresh Freq.*

NOTE For servers that contain many objects, enabling automatic refresh may result in additional network traffic and reduce the performance of both the server and the Administration Tool. In such cases, increase the automatic refresh interval, or disable the automatic refresh function.

Update WebConnect with Active Directory data

Select Server | *Refresh ActiveDirectory Information*.



Sending/Receiving Files from PowerTerm WebConnect Server

This feature provides file transfer between the WebConnect server and the Administrator's computer (the computer on which the Administration Console is running).

To receive a file from the server select Files | *Get File*. The Get File dialog appears. Browse the Folders for the desired file. Check *Open* to open the local copy using its associated application when received. Click *OK*.

Copied files are placed into a temporary folder under the user's Application Data folder in the Ericom/ptadmin subdirectory.

To send files to the server select Files | *Put Files*. The *Select Files to Put on Server* dialog appears. Select one or more files and click *Open*. The *Put Files* dialog appears. Select the target folder on the server for the file(s) destination. Click *OK* and the files will be transferred to the server.

Administration Console Parameters

The administrator can configure shortcuts to the Administration Console using command line parameters. The parameters are optional.

-user=user-name	User's account name on the PowerTerm WebConnect Server. Enter question mark (?) to sign in with the user currently logged into the system (the account must exist in the Administration Tool). Enter an asterisk (*) to bypass the login dialog.
-pass=password	User's password on the PowerTerm WebConnect Server.
-host=hostname	PowerTerm WebConnect Server's host name.
-port=port=number	PowerTerm WebConnect Server's port number.

```
PATH "D:\Ericom\PtAdmin.exe" -host=117.18.75.89 -port=778 -user="Lee"
```



10. DIRECTORY SERVICES

PowerTerm WebConnect integrates with LDAP based Directory Services (DS) such as Microsoft's Active Directory and Novell's eDirectory. Please consult with Ericom if other LDAP sources will be used.

PowerTerm WebConnect authenticates users by identifying the DS User object and then applying the standard DS User authentication.

The syntax for Active Directory users is `user@domain`.

The syntax for eDirectory users is `user.path.domain`.

When a user logs in to PowerTerm WebConnect:

- The domain specified by the user is used.
- If no domain is specified, the default is used.
- If there is no default, the authentication will fail.

<p>NOTE PowerTerm WebConnect supports both two-way and one-way domain trusts. Untrusted domains are also supported.</p>
--

Local PowerTerm WebConnect Database

PowerTerm WebConnect provides a built-in directory framework in case a third-party directory service is not available. The *Administrator* user is a built-in user.

Administration Console Connection Process

PowerTerm WebConnect requires *read* access to the Directory Service. To enable the ability to change user's password, *modify* access is required. The PowerTerm WebConnect Server can connect to the Directory Service by one of the following:

- Directly to the Domain Controller/Server where the DS is stored.
- Available when the computer running the Administration Console is running on the same trusted network as the host of the DS.
- Via the WebConnect server SSL gateway.
- Used when the computer running the Administration Console is connecting from outside the trusted network.

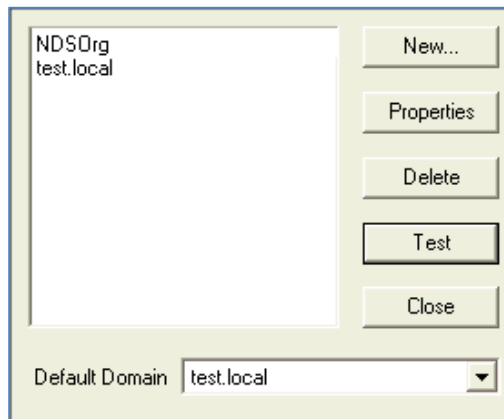
The use of SSL provides enhanced security, but does so at the expense of increased traffic overhead and degradation of the connection response time.

Once the connection to the DS database has been established, the PowerTerm WebConnect Server is able to authenticate Users using the DS.

Connecting to Directory Services

Connect PowerTerm WebConnect to an existing Directory Services:

- Launch the Administration Tool.
- Select Server | Directory Services.
If there is already a default DS identity defined, this will be discovered and displayed in the list automatically.
- Clicking New create a new DS entry. Highlighting one of the existing DS's will allow the administrator to view and modify properties, delete the DS from the list, or test the connection.
- Select one of the Domains from the Default Domain drop-down list which will be used as the default Domain for PowerTerm WebConnect Users to log in. Click Close.



Defining a *default domain* enables users to log in without having to specify the domain name as part of their login user name. PowerTerm WebConnect will automatically use the default domain when no domain is specified as part of the login.

Adding a new Directory Services instance:

- Launch the Administration Tool.
- Select Server | *Directory Services*.
- In the Directory Services window click *New*.

STOP When creating a new DS with the same name as an existing DS, a warning message will be displayed. If the warning is ignored, PowerTerm WebConnect will create a new DS with the existing name with the addition of "_1" as a suffix. To create a new instance of the DS click "Yes", to edit the existing DS click No. The name of the domain is reflected in the name of the User, for example, if the domain name is ericom.local_1, Users will to log in to this domain using a name of the form john@ericom.local_1.

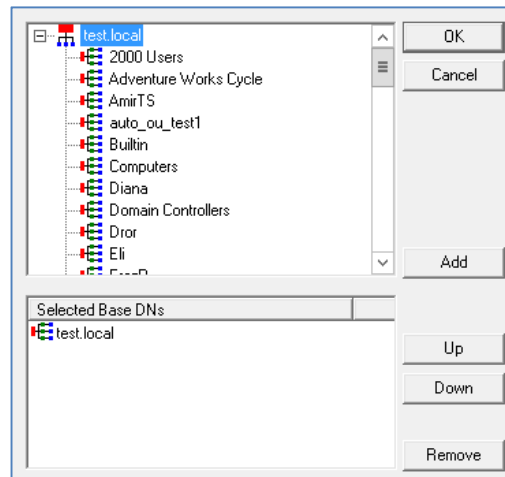
- Enter the address using the server name or IP address, and the TCP port to be used. If SSL is used to connect, this address must be a name and cannot be an IP address.
- Select the connection type from the drop-down list. Selecting *Specify credentials* requires a valid User name and Password that can query the Directory Service. Selecting *Windows authentication (Kerberos)* will log in to the DS using the current Windows credentials.
- Click Connect.

When PowerTerm WebConnect is properly connected to the DS, the Name, Vendor and Base DN (root tree Distinguished Name) of the DS will be displayed.

NOTE Connecting to an *eDirectory* DS anonymously will allow the Administration Console to read the user and group objects. When connecting anonymously to a Microsoft *Active Directory* DS, the Administration Console will not be allowed to browse the DS objects.

Adding Base DN's for use with PowerTerm WebConnect

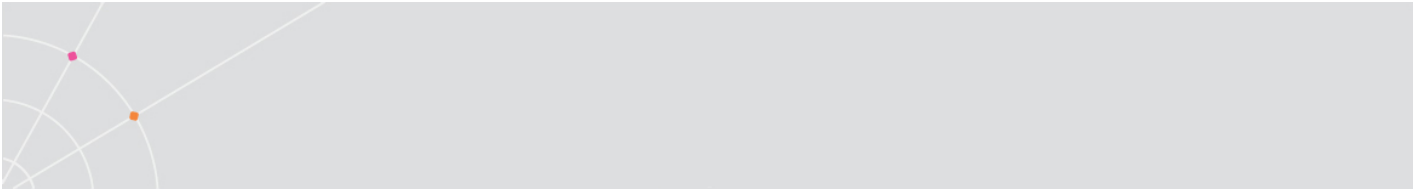
- Click on the Details of the Base DN button to display the resources stored within the DS.



Select desired organizational units (OU) for use with PowerTerm WebConnect. This enables the search for specific users to be faster and also allows PowerTerm WebConnect to reject users that are not a part of the selected OU's.

NOTE The default is to search the entire tree, which may be slow with larger directories

- Highlight desired OU's and click *Add* to add the OU's to the *Selected Base DN's* list. Multiple OU's may be added. Double click on an OU to display the child branches and objects.
- When all required resources have been added to the *Selected Base DN's* list, change the order in which they should be searched by using the *Up* and *Down* buttons. The best practice is to place the most commonly used OU's at the top of the order.



Parameter combinations

The following connection options are available.

Type	Use SSL (Port)	Server Gateway (Port)	Default Port	Use SSL and Gateway
Anonymous	✓	✓	✓	X
Specify credentials	✓	✓	✓	X
Windows authentication (Kerberos)	X	X	✓	X

HINT The default port for LDAP is 389 and the default port for SSL LDAP is 636

Certain Active Directory configurations require that Specify credentials be used. If your user logins are taking longer than expected (i.e. more than 30 seconds) configure the following:

- Use *Specify Credentials* and enter a user account that can query the directory server.
- Open the *Main Configuration* and set *Filter=use_server_cred* under the [LdapDomain=1] section.
- Restart the PowerTerm WebConnect Server service

Using Novell eDirectory

Client Configuration

When there is an Active Directory server and an eDirectory server configured in PowerTerm WebConnect, the Application Zone (ptagent) must run with the parameter */nodomain*.

NOTE */domain* is not required when Novell eDirectory is the only directory services being used.

Defining the Novell eDirectory domain base name

For a user with the following DN:

- cn=user1
- ou=Users
- ou=SalesDepartment
- ou=NDSOrg

If only the root of the tree is referenced (NDSOrg) in the base DN, the user will need to enter *user1.Users.SaleDepartment.NDSOrg* to log in.

If Users.SaleDepartment.NDSOrg is added to the base DN, the user has to enter *user1.NDSOrg* to log in.

If NDSOrg is defined as the default domain name, the user has to enter *user1* to log in.

Integration with Terminal Server

An add-on component is available through Ericom Support to automatically create local Microsoft user accounts on the Terminal Server based on the users' Novell login. Each of these local accounts will be named based on the Novell account and have the same password with the prefix of #ptwc# (for example: #ptwc#P@ssw0rd).

Active Directory (AD) User Configuration (Login Problem)

Active Directory users logging into PowerTerm WebConnect, must have a domain defined in their user account *Properties* or their login may fail. To set the domain, open the user's *Properties* screen in Active Directory and select the *Account* tab. Select the desired domain next to the *User logon name*:



Member Of	Dial-in	Environment	Sessions		
Remote control	Remote Desktop Services Profile	COM+			
General	Address	Account	Profile	Telephones	Organization

User logon name:
RU's

11. UNDERSTANDING USERS, GROUPS, AND CONNECTIONS

PowerTerm WebConnect User Object

The user object represents one person (or entity) in the PowerTerm WebConnect database. There are three types of user objects.

PowerTerm WebConnect User	Defined within the PowerTerm WebConnect database. All credentials and rights are stored in the database.
Non-persistent DS User	Defined from a Directory Services. Only listed in PowerTerm WebConnect while the user is active. All credentials and rights are stored in the directory service.
Persistent DS User	Defined within the PowerTerm WebConnect database by import from a directory service. All credentials and rights are stored in the directory service. Users are periodically synched with the directory service information.

Built-in User Objects

Several built-in PowerTerm WebConnect local user objects are supplied with the Administration Tool.

<Generic Customer>

The attributes of this user cannot be modified.

<Portal>

Used by the PowerTerm WebConnect portal component. The attributes of this user cannot be modified.

<Software Installer>

Used by the Agent to install the PowerTerm WebConnect components. The attributes of this user cannot be modified.



Administrator

Default PowerTerm WebConnect Administrator user. This account is used to login to the Administration Tool. By default there is no password, it is recommended to change the Administrator's password, and not leave empty.

NOTE To allow Administrators to login from machines other than the console, add the IP address of the desired machine to the Allow Access list. Changing the *Access Limit Mode* to *Unlimited* will allow access from any machine.

Default AutoCreated User Template

This user serves as the template for all users that are automatically created from a Directory Service (i.e., Microsoft Active Directory). The attributes of this user can be modified.

Example

A sample local user used for testing. This user's password is *example*.

Guest

Used to allow temporary access. This is a restricted user that cannot request Tech-support or Administrator support. By default there is no password.

Auto-Created users

PowerTerm WebConnect has the ability to generate user objects on the fly when using a directory service such as Microsoft Active Directory. This feature is enabled by default.

Creating Users

To create a user:

Select Actions | New | *User*. The Add User dialog is displayed.

To modify user properties:

- Double-click the desired user or right-click on the desired user and select Properties.
- Modify the necessary properties.
- Click OK.

To delete a user:

- Select the desired user and right-click Delete or select Action | Delete. A confirmation message is displayed.

- 
- Click OK.

To disable a user:

- Select the desired user and right-click Properties or select Action | Properties.
- Clear the Enabled checkbox.
- Click OK.

NOTE If the user's default group is disabled, the user will be disabled as well, even if the user object is set as enabled. However, if the user is disabled, it remains disabled even if the group is enabled.

To enable a user again after disabling it:

- Select the desired user and right-click Properties or select Action | Properties.
- Select the Enabled checkbox.
- Click OK.
- The User's default group must be enabled.

Using the Add User / User Properties Dialog

The User Properties dialog (called the Add User dialog when you are creating a new user) consists of the following:

- User properties fields
- Environment variables table
- Settings button
- Memo button: Opens a text to type notes about the object.
- Sessions button: Shows existing sessions of the user.
- Up and down arrows: Clicking these arrows switches to the previous (up) or next (down) user, as sorted in the Users pane.

NOTE The arrows are not displayed in the Add User dialog, when creating a new user.

- OK and Cancel buttons: Save or discard your changes (respectively), and close the dialog.



Changing User's Settings

To change the user's client settings:

- Select the desired user and right-click Properties or select Action | Properties.
- Click the Settings button. The Settings dialog is displayed.
- Make the necessary modifications.
- Click OK to close the Settings dialog.
- Click OK. The new modifications take effect.

NOTE Client settings that are not configured at the user level are inherited from the user's default group and server settings.

PowerTerm User Object Properties

The user object contains values to define credentials, linked connections, group membership, system permissions, and allowed access methods. Certain user properties can be defined explicitly using the Properties dialog, or they can be inherited from groups or the server group.

NOTE Although these properties apply to directory services users, most do not require configuration. Default values can be used with directory services.

There are four types of User properties:

Standalone properties

These are properties that can only be defined at the user level. They cannot be inherited from the group or server. An example is the User Name property.

Property	Description
User Name	The unique name of the object
Alias	An alternative name or ID for the user for informational purposes
Active Directory Path	Active Directory Path for the user if it exists
Use Network Password	When checked, the directory services password is enabled. When cleared, the Password button is enabled. Click it to enter the PowerTerm WebConnect password.
Password	The user's password. Ignored if Network Password is used.

Free User	(Emulation only) Enables the user to specify the connection properties.
Allow Concurrent Machines	Determines if the user is allowed to log on simultaneously from multiple computers.
Rights	Sets the user type
Access Limit Mode	<p>Unlimited: specifies that the user can access the server from any computer.</p> <p>User: specifies that the user can access the server from a computer specified in Allow Access From.</p> <p>Group: specifies that the user can access the server from a computer specified in User's Group.</p> <p>Both: both the User and Group rules are applied.</p>
Memo	Opens an editor to type notes about the object

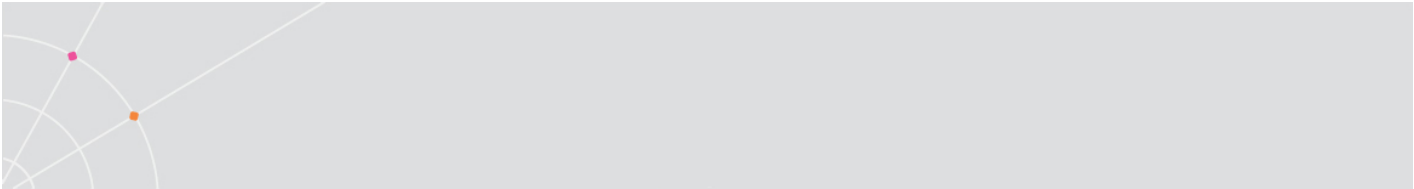
Shared properties

These are properties that are referenced in more than one object. For example, the User's Connections property defines which connections are attached to the user object. When a connection is added, the Owner property in the connection object and user object are changed.

Property	Description	Property shared with
User's Groups (PowerTerm WebConnect Groups Only)	Select a group from the Available Groups box and click the right-arrow to make the user a member of the group. Double click a group in the User's Groups box to make it the user's <i>Default</i> group.	Groups. Once a Group is assigned, the user will appear in the Group's User list.
User's Connections	Select a connection from the Available Connections box and click the right-arrow to make the user the owner of the connection.	Connection. Once a Connection is assigned, the user will appear in the Connection's User list.

Inherited properties

These are properties that can be defined at the user level, but also defined at the group or server level. If they are not explicitly defined at the user level,



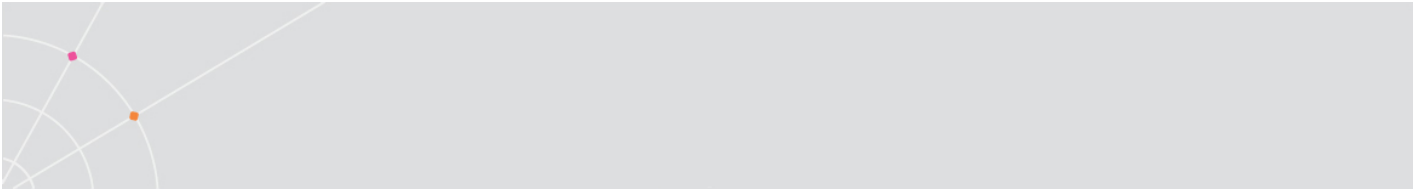
these properties are inherited from the user's default group. If they are also not defined at the group level, they are inherited directly from the Server.

Property	Description
Settings	This button opens a dialog to modify emulation settings
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions. The value '0' will use the value in the group's entry. If the group value is also '0', then the program uses the default value in the MaxUserQuota field located in the [Server] section of the Main Configuration (PtServer.ini).
Highest Reconnect Mode	Specifies the rule according to which the user is allowed to reconnect to the PowerTerm WebConnect server: None: Reconnect disabled Default: Use the default group setting OnDemand: reconnect is only performed via the Gateway Wireless: reconnect is performed via the Gateway
Environment Variables	Advanced PowerTerm WebConnect settings

General properties

These are always inherited from the user's group and/or from the server, regardless of what is defined in the user object. The user-level setting does not override the properties explicitly set at the group/server level.

Property	Description	Inheritance
User's Connections	In addition to the connections that are explicitly defined for the user, Group connections are permitted to the user as well.	Connections
Enabled	If the default group is disabled (the Enable checkbox in the Group Properties dialog is not selected), the user object inherits this setting and becomes disabled as well.	Group
Allow Access From	In addition to the connection sources explicitly define here, the user object inherits computers and addresses from its groups as well.	Group
Environment Variables	Environment variables that are not explicitly defined for the user are	Group and Server



	inherited from the groups and server.	
Client Inactivity Timeout (server object)	Specifies the inactivity timeout for all clients. Does not appear in the User Properties/Add User dialog, as it cannot be defined per-user. This property is defined using the Server Configuration dialog.	Server
Max. Sessions (server object)	Specifies the maximum number of PowerTerm sessions that can be opened simultaneously. Does not appear in the User Properties/Add User dialog, as it cannot be defined per-user. This property is defined using the Server Configuration dialog.	Server: the user's Max. Concurrent Session parameter must be lower than the Max. Sessions defined on the server.
Max Intrusion Attempts* (server object)	Maximum number of unsuccessful login attempts before the user is locked out.	Always inherited from Server
Intruders Disable Timeout* (server object)	The amount of time the PowerTerm WebConnect Server will refuse a login after detecting an intruder.	Server
Background Bitmap File	(Emulation only) Sets background image of HostView.	Server: if the user runs the HostView client, this image will be displayed as the background.

Adding a User to a Group and Setting its Default Group

Every user must belong to at least one group. Users inherit general properties from the groups to which they belong. Users optionally inherit properties from their default group, unless they have these properties explicitly defined.

NOTE The server object's Default Group parameter defines a default group for users who do not have one selected. If you do not explicitly select a default group for a user, it will acquire the Default Group defined at the server level (see chapter 0).



Assign Users to Groups

In the User Properties dialog

- Select the desired user and right-click Properties or select Action | Properties. The User Properties dialog appears.
- Select the desired group that the user will be affiliated with and click the right-arrow.
- Click OK.

In the Group Properties dialog

- Select the desired group and right-click Properties or select Action | Properties. The Group Properties dialog appears.
- Select the members to be included in this group from the Available Users list: Highlight the desired member and click the right-arrow or click the multiple right-arrows to select all the members.
- The desired member(s) appear in the Group User's list.
- Click OK.

Remove Users from Groups

In the User Properties dialog

- Select the desired user and right-click Properties or select Action | Properties.
- Select the desired group from which the user will be disaffiliated, and click the left-arrow.
- Click OK.

In the Group Properties dialog

- Select the desired member to be excluded from this group from the Group's Users list.
- Click the left-arrow. The desired member appears in the Available Users list.
- Click OK.

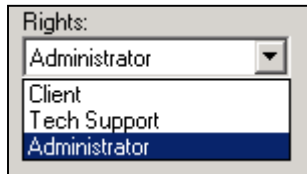
Set a default group for a user

- Select the desired user and right-click Properties or select Action | Properties. The User Properties dialog appears.
- Double-click on the group that you want to be the default group. An red arrow appears adjacent to the selected group signifying default group.

NOTE Double-click to clear the default designation.
--

PowerTerm WebConnect User Rights

A PowerTerm WebConnect user object will be one of three types: Client, Supervisor, and Administrator.



The following table explains the differences between each type:

Components/User Rights	Client	Supervisor	Administrator
Access PowerTerm WebConnect clients: HostView, RemoteView, etc.	Yes	Yes	Yes
Request support from other Administrators or Supervisors logged on to PowerTerm WebConnect	Yes	Yes	Yes
Provide support to other PowerTerm WebConnect users	No	Yes	Yes
Add/Modify/Delete user profiles via the Administration Tool	No	No	Yes
Support Active Directory/LDAP	Yes	No	No

Testing a User

The Administration Console allows you to connect as a user, and test the access options, client settings, and available connections. The user's password is required to test a connection. While you can view the user's settings using the Properties dialogs and the information panes, it is sometimes useful to test the user experience for yourself, either directly after creating a user object, after making changes to a user object, or in response to a user's request or complaint.

- Select the desired user and right-click Test. The Login dialog appears.
- Type in the Password, if required.
- Select Reconnect Mode, if required.
- Click Login. The PowerTerm emulation appears and connects to the desired host.



Connection Object

The connection defines a resource on a host server. A connection object contains information on the host type, protocol used, target application, etc. PowerTerm WebConnect supports three distinct areas of hosts: Terminal Services, VDI and legacy access.

To access a connection, it must be assigned to a user or group object. This object becomes the connection's owner. A connection can only be owned by one object at a time, so a connection intended for multiple users should be assigned to a group, which contains the desired users.

NOTE A connection can be assigned to the <i>Server</i> which will give any user access to it.
--

A connection can also be owned by another connection (which becomes its parent connection). When the parent connection is executed, the child connection is launched automatically. Child connections do not inherit settings from the parent connection.

Group Objects

The group object contains a group of users with similar permissions (for example, members of the same department). This makes it easier to classify and find similar users. When a user object belongs to a group, it will inherit some or all of its properties from the group. Any property not explicitly defined in the user object is taken from the user's group. Settings defined at the user level will override the settings at the group level.

EXAMPLE – Configuration Inheritance

Group A is defined to allowed concurrent sessions. If parameter was not defined explicitly for each user, all group members will inherit this setting. If User A of Group A is defined to not allow concurrent sessions, the user-level setting overrides the group setting. User A is not allowed concurrent sessions.

Similar to the User object, the Group object contain values to define: credentials, linked connections, group membership, system permissions, and allowed access methods. Certain group properties can be defined explicitly using the Properties dialog, or they can be inherited from the server group.

Standalone properties

These are properties that can only be defined at the group level. They cannot be inherited from the server. An example is the Group Name property.

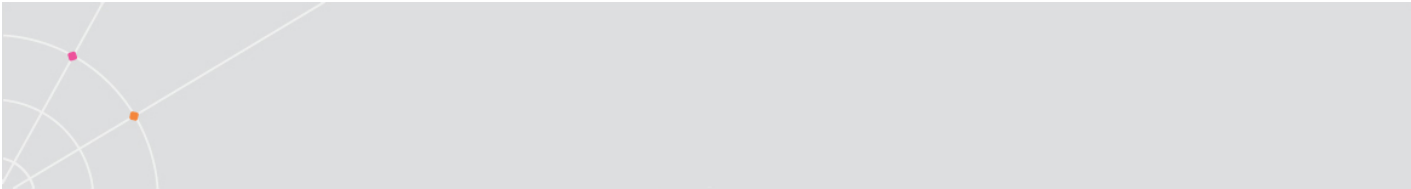
Property	Description
Group Name	Unique identifier for the object

Alias	An alternative name or ID for the user for informational purposes
Enabled	Specifies whether the group is active
Highest Reconnect Mode	Specifies which Reconnect mode to use
Allow Access From	Specifies the machines from which the user is allowed to access to PowerTerm WebConnect. Format – IP address, IP Scope, User Name, all entries are separated by semi-colons.
Access Limit Mode	Unlimited: specifies that the user can access the server from any computer. User: specifies that the user can access the server from a computer specified in Allow Access From. Group: specifies that the user can access the server from a computer specified in User's Group. Both: both the User and Group rules are applied.
Memo	Opens a text editor to type notes about the object

Shared Properties

Shared properties are reference by more than one object at a time.

Property	Description	Property shared with
Group's Users	Select a user from the Available Users box and click the right-arrow to make the user a member of the group. Use the multiple right-arrows to add all the users.	Users
Group's Connections	Select a connection from the Available Connections box and click the right-arrow to make the group the owner of the connection. Use the multiple right-arrows to associate all the unaffiliated connections to this group. The group's members can select one of the connections shown here (or one of the connections inherited from other groups and the server) when logging in.	Connections



Optionally-Inherited Properties

Optionally-inherited properties can be defined at the group level, but also at the server level. If they are not explicitly defined at the group level (using the Add Group or Group Properties dialog), these properties are inherited from the “master group” – the server object.

Property	Description	Inheritance
Settings	This button opens a dialog to modify settings for the group's users	If settings are not defined here then all settings will be inherited from the server.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions that this has. The value '0' instructs the program to use the value specified (maximum number of concurrent connections) in the User's default group. If this value is also '0', then the program uses the default value in the MaxUserQuota field located in the [Server] section of the PtServer.ini file. Other values will override the default value.	Enter '0' to inherit this property value from the server object's Default Sessions property.
Max. LPD Queues	Stipulates maximum number of LPD queues that this user will be allowed to have at any particular time. Enter '0' to revert to the default group's setting (or the server's setting).	Enter '0' to inherit this property's value from the server's object's Default LPD Queues property.
Environment Variables	This table allows you to create and edit free-text variables that have numerous uses. Environment variables added here are defined on the group level.	Environment variables that are defined both here and in the user's default group (or on the server) are optionally inherited. If you do not define them explicitly here, they are inherited from the group.



Groups and Connections

A group, like a user, can own a connection object. When a connection is affiliated to a group, all of the group's members can use that connection object to connect to the host.

Every connection is owned by a specific user, a group of users or by the server object (see below). When a connection is owned by a specific user, only that user is allowed to use that connection. When a connection is owned by a group only users belonging to that group can use that connection. In other words, you define how a user communicates with a host, and which remote applications that user can access, by affiliating the user object to a connection object. Another way to do this is to affiliate a connection to a group of users to which the specific user belongs.

Using Built-in Group Objects

Several default group objects are predefined in the PowerTerm WebConnect server. These groups may be modified based on the administrator's needs.

- Novice Users (Default) – least permissions
- Advanced Users
- Expert Users
- Super Users – most permissions

Disabling a Group

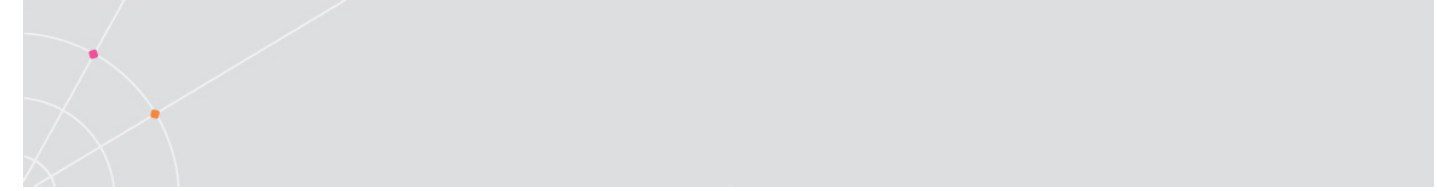
When disabling or deleting a group object, all the users of the group will be blocked from accessing PowerTerm WebConnect. In order to re-enable users from a deleted group, a new default group must be assigned to them.

<p>NOTE If a group is disabled, all its users are inherently disabled. However, disabling a user does not affect anything on its groups.</p>

- Right-click the desired group and select *Properties*. The Group Properties dialog appears.
- Check the Enable checkbox to enable, clear the checkbox to disable. Click *OK*.

The Server Object – the "Master Group"

The server object has a dual function: to define PowerTerm WebConnect server-related settings, and to set the defaults for all objects. Groups settings that are not explicitly defined are inherited from the Server Configuration. The server object can be set as the owner for specific connections. Such connections become available to all the users.



NOTE If a setting is not explicitly defined at the group level, the group's users inherit the default settings from the server object. Settings defined at the connection object level override the settings at the server levels. However, if the setting is explicitly defined at the user level, the user's setting overrides all the other settings.

General Properties at the Server Level

Certain properties are defined at the server object and are automatically inherited by all users.

For example: the Max. Intrusion Attempts parameter defines the number of times a user can enter a wrong password before being blocked, is defined at the server level and is automatically inherited by all users in the system. You cannot modify this parameter for specific users or groups.

The Server Object as a Fallback Option

The server object is a "master group" to which all groups and users belong. By default, the server's properties effect the entire system and all the users. However, this is often not the case. Groups do not inherit server options if they have these options explicitly defined, and users can also have explicitly defined properties that override the server defined properties.

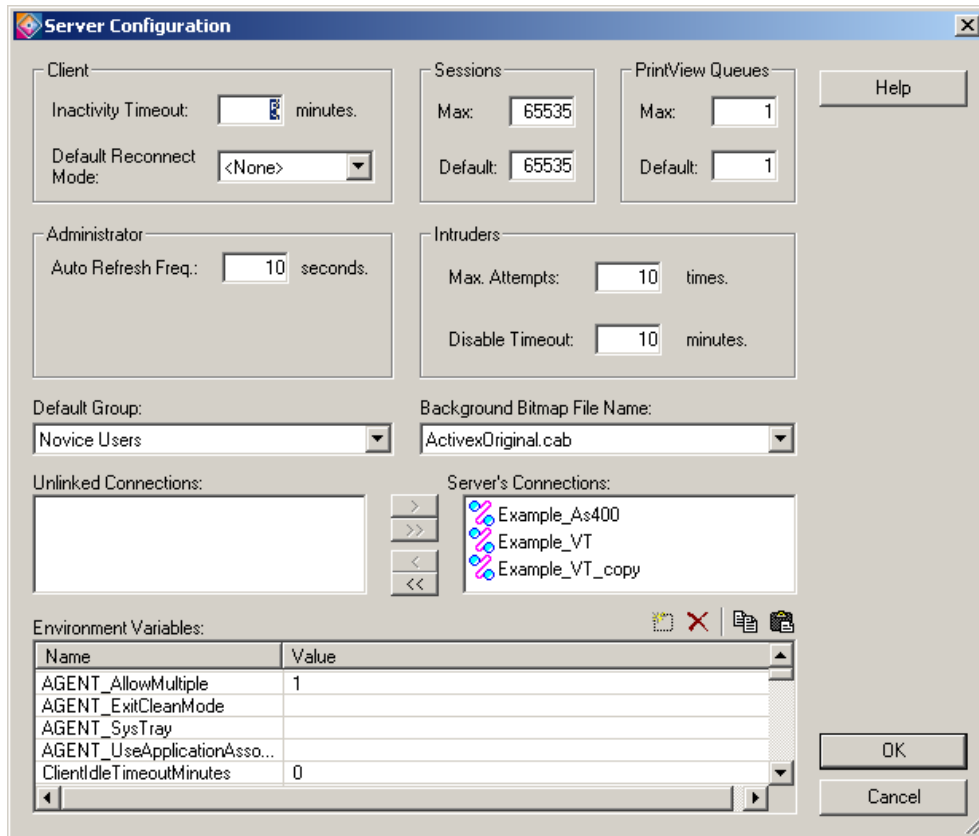
Essentially, this means that the server object is a fallback option. Any "optionally inherited" properties you neglect to define in a group or user – either intentionally or by mistake – will be taken from the server.

The consensus is that server properties should be as widely applicable as possible. Try to define settings that will be the most appropriate for most users because most users are likely to inherit at least some of them during their system lifetime.

Server Object Properties

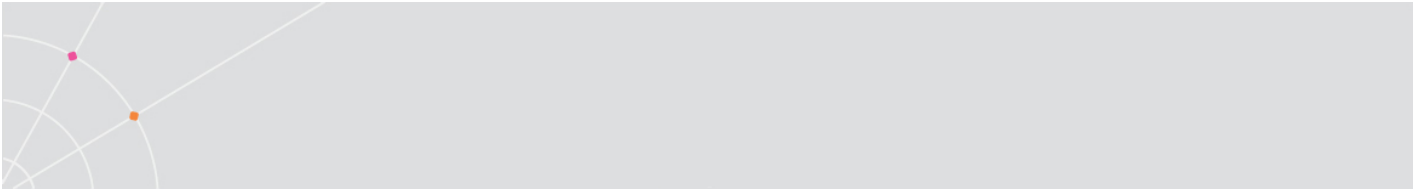
The server object has properties that define linked connections and allowed access methods for users. These properties can be divided into two types:

- **Optionally-inherited properties:** Groups and users inherit these properties unless you specify otherwise. Settings explicitly defined in a group or user object override these server-level settings.
- **General properties:** Groups and users always inherit these. These properties cannot be defined per-group or per-user (i.e. they can only be defined in the server object, using the Server Configuration dialog).



The following table lists and explains the server object's properties. The "Type" column details how each property is inherited by groups and users.

Property	Description	Type
Client Inactivity Timeout	Specifies the time limit for any client's inactivity after which the server closes the connection.	General
Max. Sessions	Specifies the maximum number of concurrent sessions that a user can open	General
Max LPD Queues	Specifies the maximum number of registered LPD queues that a user can define.	General
Administrator Auto Refresh Freq.	Specifies the interval in which the Administration Tool's <i>AutoRefresh</i> will refresh the screen.	-
Intruders: Max. Attempts	Specifies the maximum number of login attempts the user can perform to the PowerTerm WebConnect server before being regarded as an intruder and be	General



	locked out for a set time duration.	
Intruders: Disable Timeout	Specifies the amount of time (in minutes) that the PowerTerm WebConnect server refuses to login a valid user after detecting an intruder.	General
Default Group	Initial Default Group	Users who do not have a default group defined will use this value.
Background Bitmap File	Sets a background bitmap for clients that support this feature.	General
Server's Connections	Connections available to the server.	General. All users can access the server's connections.
Environmental Variables	Server related Environment Variables. These Environment Variables can be accessed from the login scripts.	Environmental variables that are not defined in any group or user object act like general properties, and are inherited by all users.

Object Hierarchy

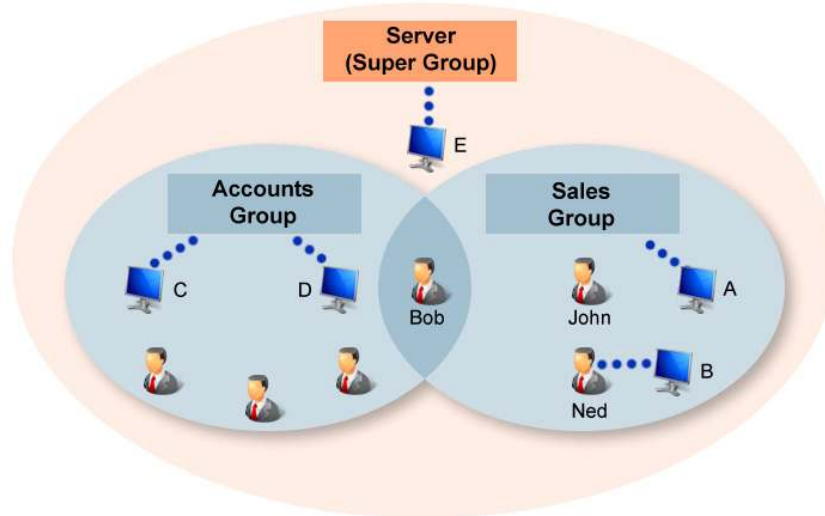
Server (Master Group) settings are applied first upon login.

Group settings are applied next

Connection settings are applied next

User settings are applied last and these will overwrite any previous settings that were configured.

Example: Object relationships and hierarchy



In the example above there are two users belonging to the *Sales* group, three belonging to the *Accounts* group, and one user, Bob, belonging to both. All users belong to the *Master Group* – the server. There are five connections with different owners (indicated by dotted lines). Connection A belongs to the “Sales” group, B belongs to the user Ned, C and D belong to the “Accounts” group, and E belongs to the server. In this scenario:

- *John* has access to the following:
 - connection A, because he belongs to the “Sales” group
 - connection E because he belongs to the “Master Group” (the server)
 - John inherits his default settings from the “Sales” group and “Master Group”.
- *Ned* has access to the following:
 - connection B because he owns it.
 - connections A as a member of the “Sales” group
 - connection E because he belongs to the “Master Group” (the server).
 - Ned inherits default settings from the “Sales” group and “Master Group”.
- *Bob* belongs to two groups and to the server and has access to the following:
 - all connections shown (except B, which ONLY Ned owns).
 - Bob inherits default settings from his default group, which can be either “Accounts” or “Sales”.



Implementing Access Policy

When designing the PowerTerm WebConnect infrastructure consider these questions:

- Which users should have access to PowerTerm WebConnect resources?
- Do all the users have similar needs, or are there groups of users with distinct access needs?
- How will changes in personnel and their groups affect the access policy?
- What type of applications will be published?

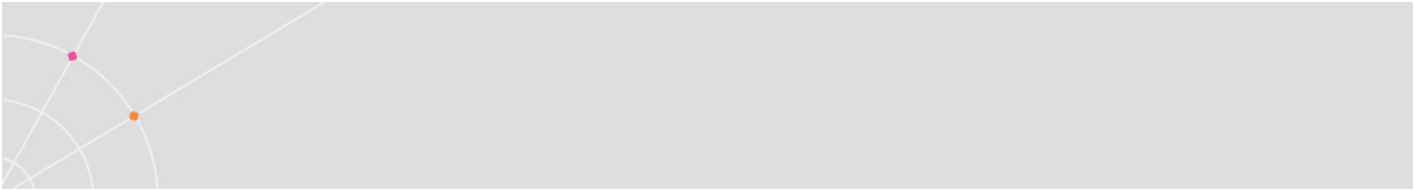
Initial Configuration

The following procedure is a general guideline that explains how to define users and groups at the initial configuration

- Define administrator's attributes and privileges. Create any additional administrator users.
- Determine if PowerTerm WebConnect built-in groups will be used. Modify them if needed.
 - Create additional groups as needed.
- Assign built-in users to desired groups
- Determine if Directory Services will be used.
 - Directory Services users will always be assigned to the PowerTerm WebConnect Default Group (Server | Configuration| *Default Group*).
- Assign any PowerTerm WebConnect users to desired groups
- Create connections and applications
- Assign connections and applications to groups or users

Generic Users

In some cases authentication into PowerTerm WebConnect is not required. For example, the published application has its own authentication system, and an additional login is not desired. By using generic users, all users will connect to the PowerTerm WebConnect environment with the same "generic" account. Any applications and desktops published to the generic user will be accessible without a login. The generic user credentials are configured in the client HTML parameter line as */USER* and */PASS*.



HINT When using generic users, to ensure single sign-on between WebConnect and the Terminal Server, ensure that the generic user also has an account on all Terminal Servers (same username and password).

User Object Properties: To Define or Not?

When to Define User Settings

Specific users who need different settings from the others in their group must have user-defined settings. When user groups are fairly heterogeneous, and users need unique configuration, define settings in the PowerTerm User account and create notes using the Memo function. User defined settings have the highest precedence and will follow the user regardless of its group assignments.

When to Inherit Properties from Groups/Server

If users have no properties explicitly defined, simply add them to a group and they assume the properties of the group. Defining settings at the Group level will reduce administrative overhead and settings only need to be defined for a few groups rather than many users.

HINT Directory Services users should be configured inherit settings from its Default Group and the *Server*.



12. DEPLOYING APPLICATIONS AND DESKTOPS WITH TERMINAL SERVICES

Overview

AccessNow and the RemoteView native component of PowerTerm WebConnect enables access to sessions running on Windows Terminal Servers or any desktop accepting RDP connections. Three protocols are available for RemoteView connections: *RDP*, *Blaze* (accelerated RDP), and AccessNow (HTML5 access). Two modes of access are available:

Full Desktop – the user connects to the entire remote desktop of the host. This mode is useful for these scenarios:

- End users connecting from a thin client to a remote desktop to do all work.
- End users connecting to a remote desktop that is locked down and regulated by the corporate IT department.
- Administrators connecting to a server to manage it.

Seamless applications – the user only sees the application that is selected, without the entire desktop. *Ericom Access Server* must be installed on any Terminal Servers that will be used with PowerTerm WebConnect Seamless windows. Seamless applications are useful when:

- End users only need access to a specific application

Administrators want to hide the remote desktop and restrict access to certain OS functions on the host (i.e., restarting the server).NOTE Seamless windows are not available for 16 bit applications.

On each RDP Host (i.e., Terminal Server), install the following components to get the most out of PowerTerm WebConnect:

- *Ericom Access Server* is required for HTML5 access and accelerated Blaze RDP connections. Also includes the Ericom TSAgent.
- Net2Printer/triCerat Server is required when using one of these universal printing enhancement options (see chapter on Printing for more information on this offering). This is only supported by the Windows native client.

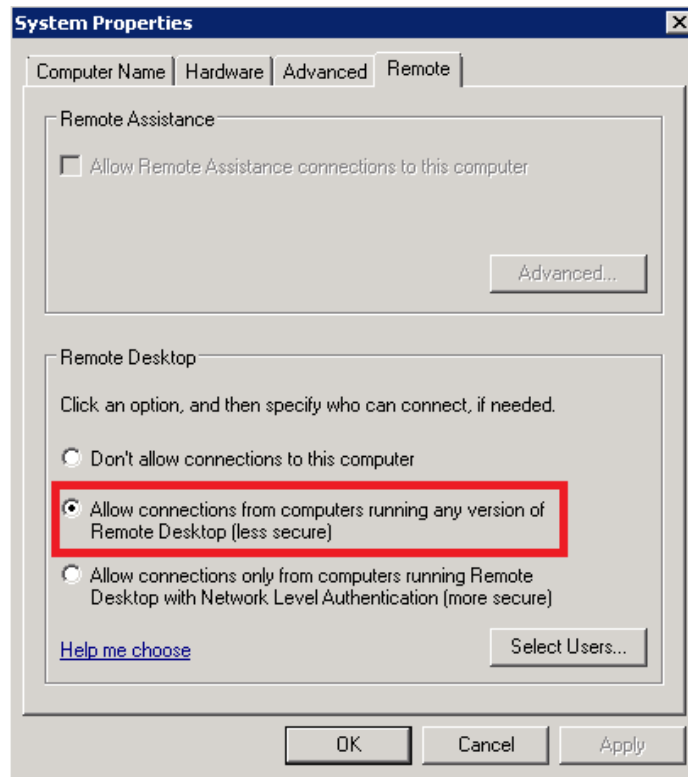
Disable RDP NLA Support

PowerTerm WebConnect clients do not fully support NLA. For best results, disable NLA on all Terminal Servers (Session Hosts). On Windows 2008, 2008R2, and 2012 go to *Control Panel | System | Remote* tab.

Windows 2008R2

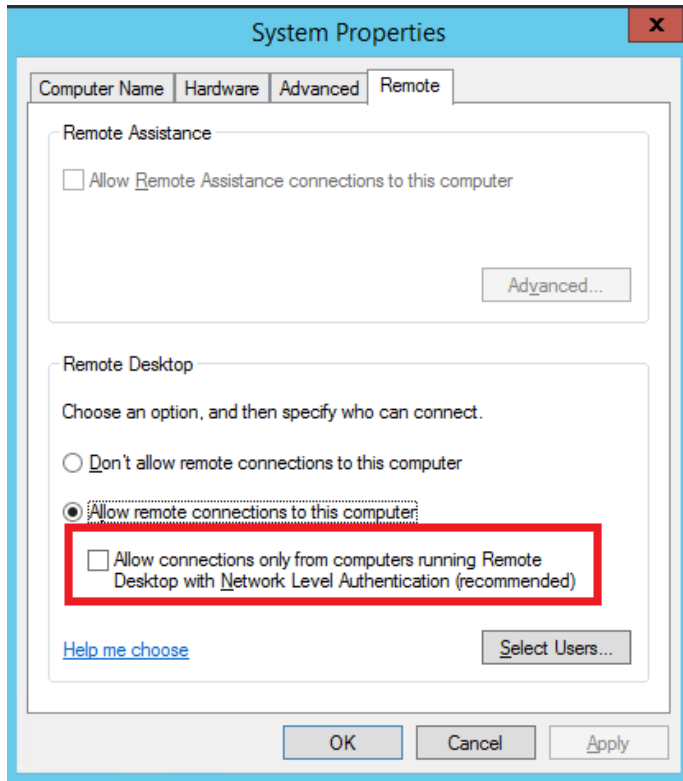
Check *Allow connections from computers ...*

Do not select *Allow connections only from computers running ...*

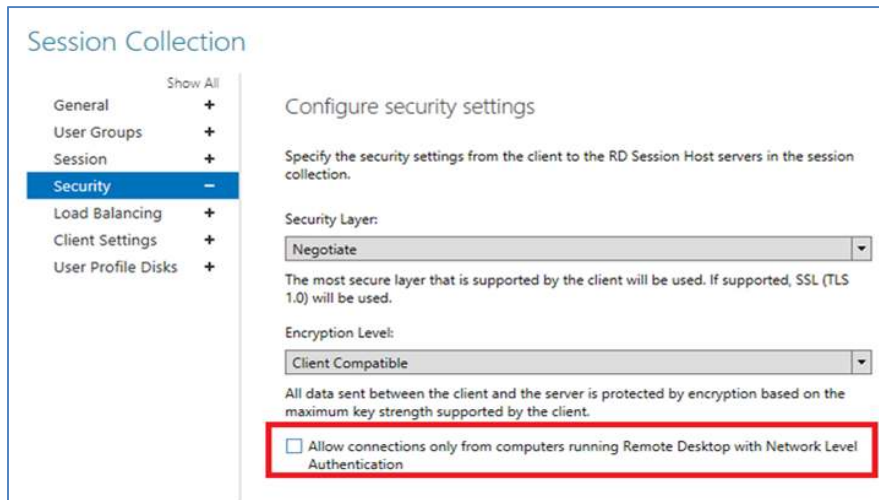


Windows 2012

Uncheck the checkbox to *Allow connections only from computer running...*



To manage this setting in a collection of Session Hosts, go to the Collection's Security tab and uncheck the box.



Ericom Blaze RDP Acceleration

The Ericom Access Server is required to enable Blaze RDP Acceleration. The Access Server installer is found under the AddOns directory. Install this on each Terminal Server that is planning to host Blaze sessions.



Ericom AccessNow HTML5 Client

The Ericom Access Server is required to enable HTML5 access. The Access Server installer is found under the AddOns directory. Install this on each Terminal Server that is planning to host AccessNow sessions.

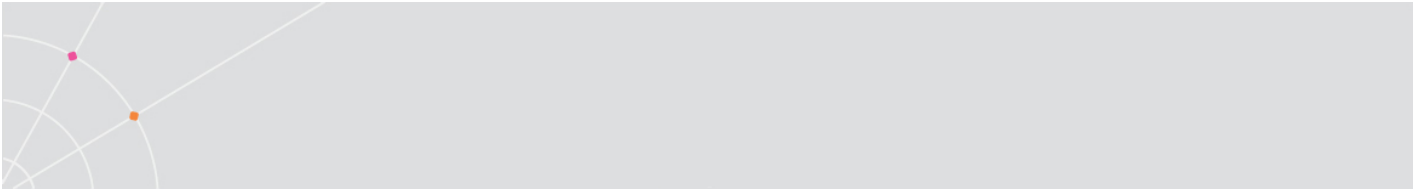
Ericom Terminal Server Agent

The Ericom Access Server includes the Terminal Server Agent (TSAgent). This must be installed on every Terminal Server that will be managed by PowerTerm WebConnect.

The behavior of the TSAgent can be modified using settings in the registry or via PowerTerm WebConnect environment variables. Some values can be defined only using the registry, some only using environment variables, and some using both. The order of precedence is:

- Registry under HKEY_CURRENT_USER \SOFTWARE\Ericom Software\PtTSAgent (highest)
- Registry under HKEY_LOCAL_MACHINE\SOFTWARE\Ericom Software\PtTSAgent
- PTWC environment variable at user level
- PTWC environment variable at group level
- PTWC environment variable at connection level
- PTWC environment variable at server level (lowest)

<p>NOTE On x64 servers, the Ericom PtTSAgent key is under HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Ericom Software\PtTSAgent</p>



List of all possible TSAgent settings and their respective options				
Env Var Name	Reg Name	Reg Type	Default Value	Description
-	LogFolder	String	%USERPROFILE%	Default location where log is written. Log is always PtTSAgent.log
-	LogUser	String	""	Logging only for set user
RDP_RedirectSchemes	RedirectSchemes	String	""	A delimited list of protocols to redirect
RDP_RedirectExclude	-	String	""	Domains and IP ranges to exclude from redirection
RDP_ScriptFolder	-	String	.\Scripts	Folder of event scripts
-	SkipStartup	DWORD	0	Set to 1 to skip Windows startups in True Seamless
RDP_LogoffDisconnected	LogoffDisconnected	DWORD	0	Set to 1 to logoff disconnected sessions
RDP_LogoffDelaySeconds	LogoffDelaySeconds	DWORD	300 (5 * 60)	Timeout interval to end a session (min value = 3 ATG/AN and 30 RemoteView)
-	NoLoadBalancerAgent	DWORD	0	Set to 1 to not connect to local LB Agent
-	LoadBalancerAgentPort	DWORD	4040	Port to connect to local LB Agent
RDP_PerformanceFlags	PerformanceFlags	DWORD	0	Performance flags bitmask: 1 – higher priority for foreground app 2 – make see-through windows opaque

RDP_BehaviorFlags	BehaviorFlags	DWORD	0	Behavior flags bitmask: 1 – Don't disable screen-saver 2 – Change bring window to foreground behavior
RDP_MacFlags	MacFlags	DWORD	0	Mac client flags bitmask: 1 – No window shadow 0x10000 – hide background owned windows
-	LogLevel	DWORD	0	Logging flags bitmask: 1 – events 2 – msgs sent 4 – msgs received 8 – debug

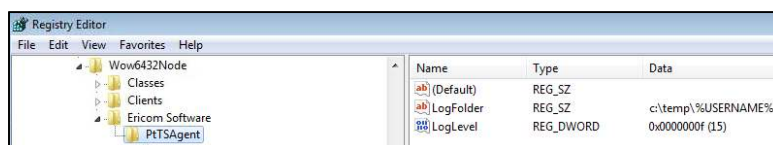
Troubleshooting the TS Agent

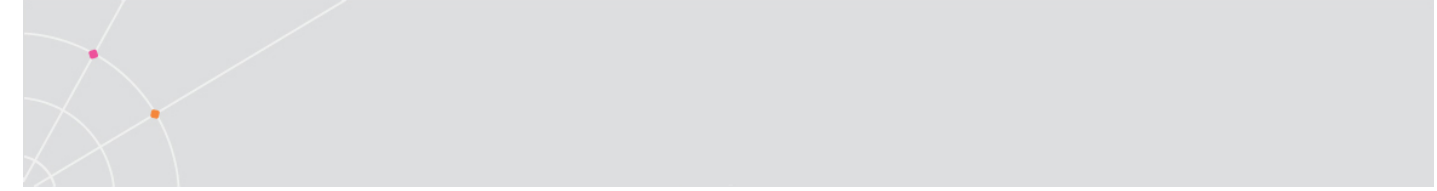
In the event of problems related to the TS Agent (i.e., seamless windows are not appearing properly) a debug log is required for Ericom Support to diagnose the issue.

To create the debug log, the following Registry keys must be updated:

- *LogLevel* – set to 'F'
- *LogFolder* – by default this key is not present in the Registry and is set to %USERPROFILE%.

NOTE To make the log files easier to find, set the *LogFolder* to C:\Temp\%USERNAME%. Make sure that all users being logged have write access to C:\Temp or the configured directory.





At the point where the problem appears, copy/paste the log and send it to Ericom. Ending the log at the point where the problem occurs will expedite the troubleshooting process. Send the log and a description (i.e., screenshot) of the problem to *tech.support@ericom.com*.

Ericom Remote Browser

This feature is installed as part of the Access Server installer. The Application Publishing wizard requires *Ericom Remote Browser* to be installed on at least one Terminal Server. The Remote Browser is a service that passes information on browsed files, display names, icons, and link parameters to the PowerTerm WebConnect server. The Remote Browser is included with the PowerTerm TS Agent installer.

Session Sharing

To streamline Terminal Server license and resource usage, multiple seamless applications can share the same RDP session. When sessions are shared, a user does not have to login multiple times to run multiple seamless applications. The login process is one of the most resource consuming operations of Terminal Services and should be reduced where possible, so session sharing is enabled by default.

Session Sharing is enabled when these settings are the same between launched connections: *Server setting*, *User credentials*, and *Domain setting*.

The *Connection Type* setting of connection is not taken into account. Therefore, if a connection using *Direct* connection is launched, and then another connection defined as *Gateway* is launched, session sharing is performed using the *Direct* mode (the *Connection type* of the second connection is ignored during *Session Sharing*).

Similarly, when *Session Sharing* is enabled, the color depth of the first application launched is used. Subsequent applications will use the first application's color quality regardless of its own setting. To ensure that a certain color quality is always used for a certain connection, disable *Session Sharing*.

To improve the use of *Session Sharing*:

- All Terminal Servers should have the same applications installed. This ensures that the Terminal Server that is already active will have additional applications that will be launched.
 - The Load Balancer will track which Terminal Servers host which applications. If the user selects an application that is not available on the active Terminal Server, it will be launched using the Load Balancer's selection.

- The address of the Terminal Server has to be specified in exactly the same format for all the published applications. This will happen automatically if the Load Balancer is used.
- The user has to login to the Terminal Server with the same credentials (username and domain), specified in the same format. This will happen automatically for published applications that are configured to use the PowerTerm WebConnect credentials.
- A difference in the *Drive Mapping* setting does not disable Session Sharing, but this setting is not shared between applications.

To disable Session Sharing set the environment variable *RDP_DisableSessionSharing* to 1.

NOTE Session Sharing is not available for AccessNow and AccessToGo clients.

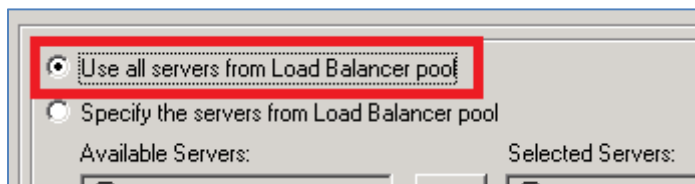
Session Following

Terminal Server sessions can be configured to “follow” users when they move to different workstation. This feature is useful for users that need to access their Applications and Desktops while roaming to different locations (i.e., doctors moving from one patient room to another.) When Session Following is enabled, sessions will follow users based on their WebConnect user name. This feature works across different clients (i.e. AccessNow, AccessToGo, etc.)





NOTE If the connection is not configured to use WebConnect credentials, and the user has manually logged on the TS’s with different credentials, Session Following will not work, and a new session will be opened instead.

This feature is configured globally by modifying *RDPTerminalSessionFollowMe* in the Main Configuration file (*PtServer.ini*). To enable the feature, set the value to *True* (default).

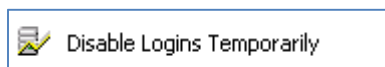
Next, for each *Connection* that will use this feature, set the Connection’s *Servers* setting to “Use all servers..”



The Terminal Server(s) should be configured to *Restrict each user for one session only* (this is the Windows default). This is configured in the *RDP Configuration* settings.

Edit settings	
General	
 Delete temporary folders on exit	Yes
 Use temporary folders per session	Yes
 Restrict each user to a single session	Yes
 User logon mode	Allow all connections

If the Terminal Server where the user's session resides is disabled for logins in the Load Balancer, the existing session will not follow the user at the next connection.



Using LogOffDelaySeconds

Remote desktop sessions are explicitly logged off using the logoff option in the remote desktop's *Start Menu*. When this option is selected, the sessions are logged off immediately. Remote seamless application sessions – sessions in which only specific applications are run – cannot be logged off in this way. Instead, these sessions are automatically logged off when they no longer contain any visible windows, for example when all application windows are closed.

In some cases, applications may not display anything on the screen for short periods during normal operation, for example while loading. To prevent such sessions from logging off prematurely, the automatic logoff is delayed. If during this delay new windows are created or existing windows become visible then the logoff is canceled and the session remains active. The default delay duration is 300 seconds for RemoteView and Blaze and 3 seconds for AccessNow and AccessToGo. In addition, sessions will not be terminated during the first 30 seconds from their creation.

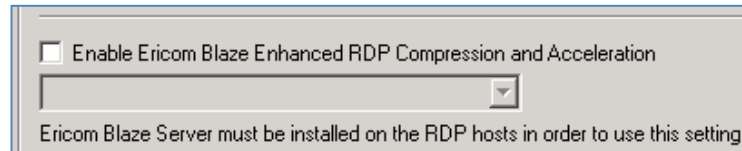
The 300/3 second delay period can be adjusted using the PowerTerm WebConnect *RDP_LogoffDelaySeconds* environment variable. The value specified in this setting will be used for all client types. Note that the 30 seconds delay from session creation cannot be adjusted.

The reason that RemoteView and Blaze use a much longer delay by default is that the client can reuse existing sessions for additional applications (Session Sharing feature). This means that if a new application is launched during the logoff delay, this application can reuse the existing session instead of creating a new one. Session Sharing is not available for AccessNow and AccessToGo.

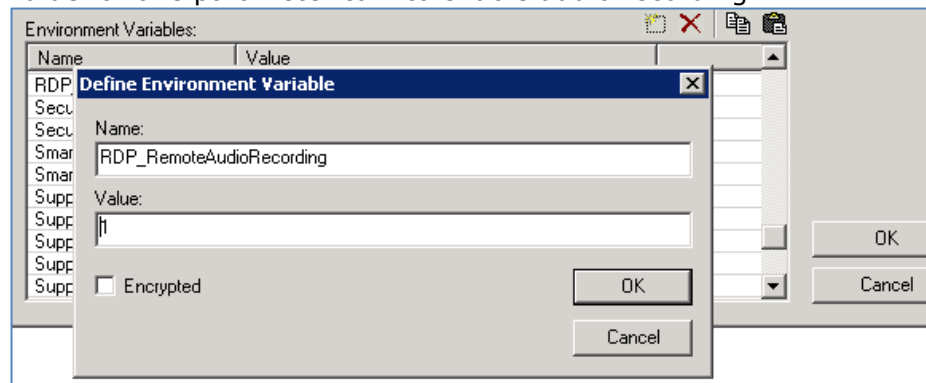
Audio Recording (supported operating systems required)

Modern Windows operating systems (such as Windows 7, 2008 R2, and 2012) support audio recording in RDP. This feature is supported through PowerTerm WebConnect. To enable audio recording redirection, perform the following:

- Publish a connection with *Blaze disabled*. The session must use RDP.



- Add the environment variable *RDP_RemoteAudioRecording* to the connection's *Properties*, or to the *Server Configuration*. Set the value for this parameter to *1* to enable audio recording.



- When the connection is launched, the user will be able to record audio into the RDP session.

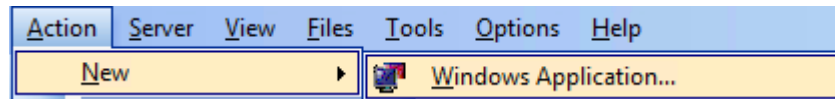
NOTE If the user is having difficulty recording audio into the RDP session, verify that the functionality is working with *mstsc.exe* first. The operating systems on both sides must support audio recording; Windows XP and 2003 do not support this feature.

Publishing

There are three types of publishing modes. All follow similar steps through the publishing wizard; however, some will have more configuration options than others. This chapter will explain how to publish a single application and then explain which steps to follow for Multiple Application Publishing and Full Desktop Publishing.

Publish a single Windows application

From the Administration Tool, select Action | New | *Windows Application*. This wizard will publish one application at a time.



Publishing Wizard Steps

Step 1: Determine the application publishing target

A screenshot of the Publishing Wizard Step 1: Determine the application publishing target. The wizard is titled 'ERICOM ACCESS ONE POINT'. It has three main sections: 'What to Publish', 'Application Installation Type', and 'Publish from'.
- 'What to Publish': Radio buttons for 'Application' (selected), 'Document', and 'URL'.
- 'Application Installation Type': Radio buttons for 'Preinstalled Application' (selected) and 'Streamed Application'. A dropdown menu below 'Streamed Application' is set to 'Microsoft App-V'.
- 'Publish from': Radio buttons for 'Terminal Server' (selected), 'Virtual Desktop / Blade PC', and 'Local Desktop'. A checkbox for 'Prefer Local Desktop' is unchecked.
At the bottom, there are buttons for '< Back', 'Next >' (highlighted), 'Finish', 'Cancel', and 'Help'.

What to Publish

- Application – publish an application
- Document – publish a document, the default application (on the host) will be used to launch the document.
- URL – publish a URL, the default web browser (on the host) will be used to launch the document.

Installation Type


- *Preinstalled* – an application that is already installed on a host.
- *Streamed* – an application that will be delivered to the host from a Microsoft App-V streaming server

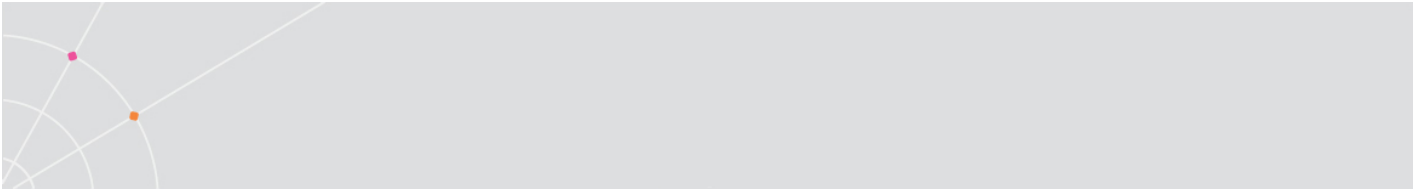
Publish from

- *Terminal Server* – the host is a Terminal Server (select this)
- *Virtual Desktop* – the host is a Virtual Desktop
- *Local Desktop* – the host is the end-user’s workstation (Microsoft Windows XP and higher only)
 - Prefer Local Desktop – the selected application will be launched from the end-user’s local desktop. If the application is not available on the local desktop, then it will be launched from the Terminal Server as a seamless application.

Step 2: Configure the Application properties

The screenshot shows a configuration window for ERICOM. On the left is a logo with the text 'ERICOM ACCESS DONE RIGHT' and a graphic of colorful blocks. The main area contains five input fields with labels: 'Application:', 'Working Directory:', 'Parameters:', 'Name Displayed to User:', and 'Place Icon in Folder:'. The 'Application:' field has a small browse button to its right. At the bottom of the window are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- *Application* - Enter the path of the application to be published (i.e., C:\Windows\notepad.exe.)
- If necessary, configure the *Working Directory* and *Parameters* settings. *Parameters* are command line values that can be passed to the configured application.
- To assign this application to a sub-folder, enter the *Place Icon in Folder* name. Sub-folders are separated with a '\'
 - EXAMPLE: If the administrator enters "Accessories\System", the published application will be placed in a folder named Accessories and a subfolder under Accessories named System.
- To select an application using a graphical interface click the browse button . This will launch a dialog to connect to a server running the PowerTerm Remote Browser.



- The Remote Browser will display applications available via the Terminal Server's Start Menu. After selecting the browse button enter the *Terminal Server's IP* address and *Port number* of the system running the Remote Browser.

A dialog box with the following fields and buttons:

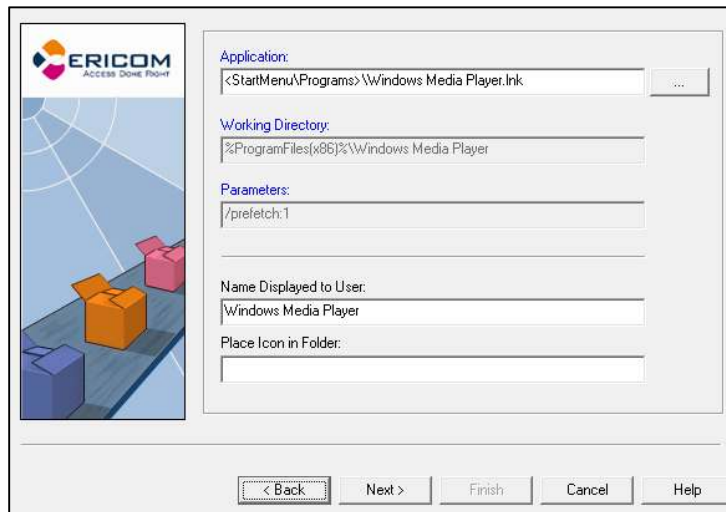
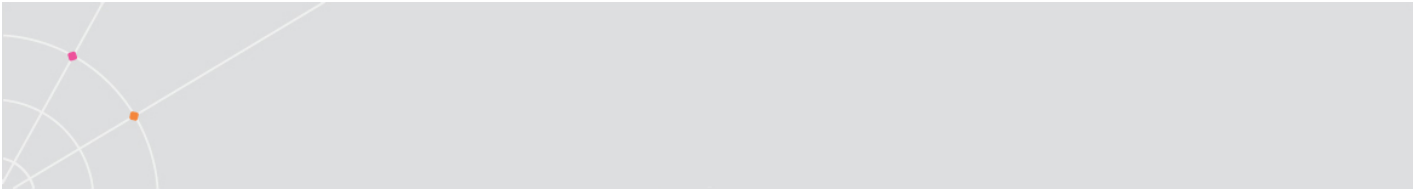
- Server Address: [US-BL2008R2] (dropdown menu)
- Port Number: [4030] (text input)
- OK (button)
- Cancel (button)

- At the application selection dialog, either navigate to the application by clicking on a drive letter or select the application from the *Programs* menu.

A file selection dialog box with the following elements:

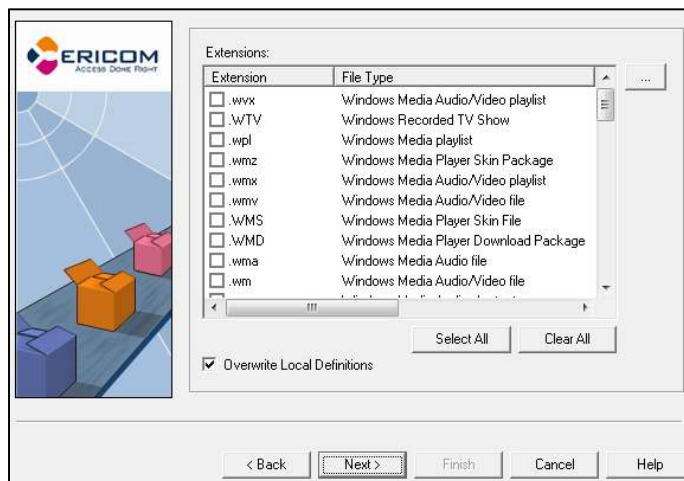
- Navigation pane showing "Programs", "C:", and "D:".
- File name: [] (text input)
- Files of type: [Executables (*.exe;*.com;*.lnk;*.bat;*.js;*.vbs;*.wsf;*.hta)] (dropdown menu)
- Open (button)
- Cancel (button)

- After selecting an application, all relevant files will be automatically completed.
- EXAMPLE: Resulting screen after selecting Microsoft Windows Media Player:



Step 3: Set *Extensions* redirection for the application

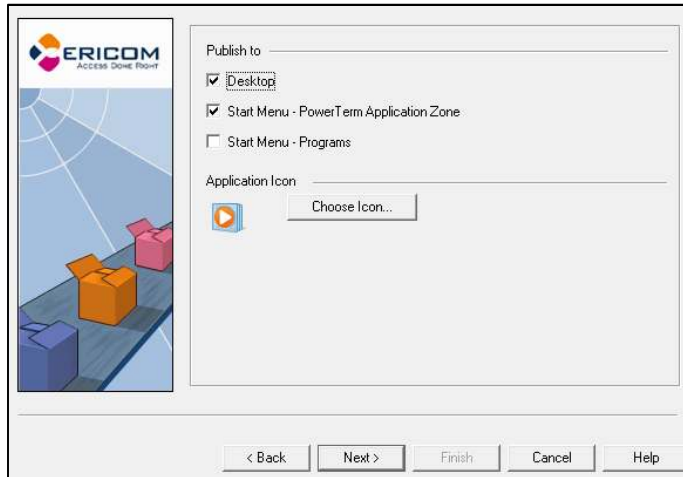
When a user launches a local file with an associated published extension, the published application will be used to open the file. To configure extension redirection, select all desired extension formats and check *Overwrite Local Definitions*. This feature is only available from Windows-based clients.



NOTE Checking *Overwrite Local Definitions* will overwrite the definitions for that file extension if it exists on the local system. This behavior may not always be desired when publishing applications (such as Microsoft Word). For example, users working from a home system may not want to overwrite the local definitions if they cannot save files from the published application back to their local hard drive.

Step 4: Set User Access

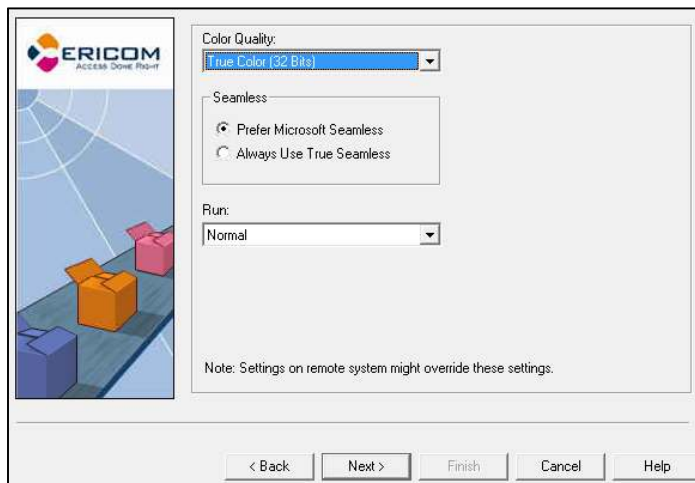
Shortcut icons for the published application will be placed in the locations that are checked.

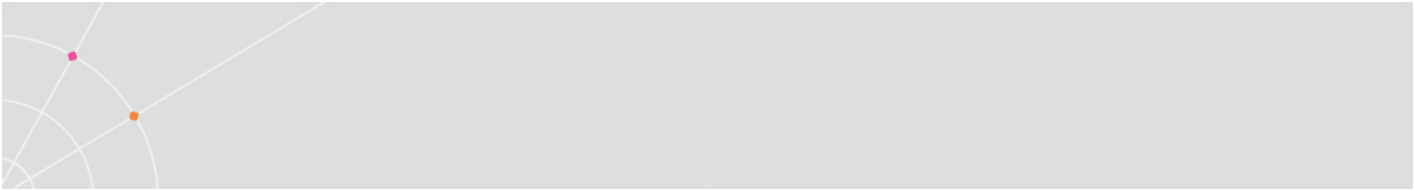


- *Desktop* – Places published shortcut icon on the end-user’s desktop.
- *Start Menu* - Places published shortcut icon on the end-user’s Start Menu, under a folder named *PowerTerm Application Zone*.
- *Start Menu/Programs* - Places published shortcut icon on the end-user’s Start Menu, under the Programs folder.
- To use a custom icon, click *Choose Icon* and select the desired icon. Select *Browse* to display icons from a different file.

Step 5: Set Appearance Properties

The dialog sets appearance characteristics of the published application.



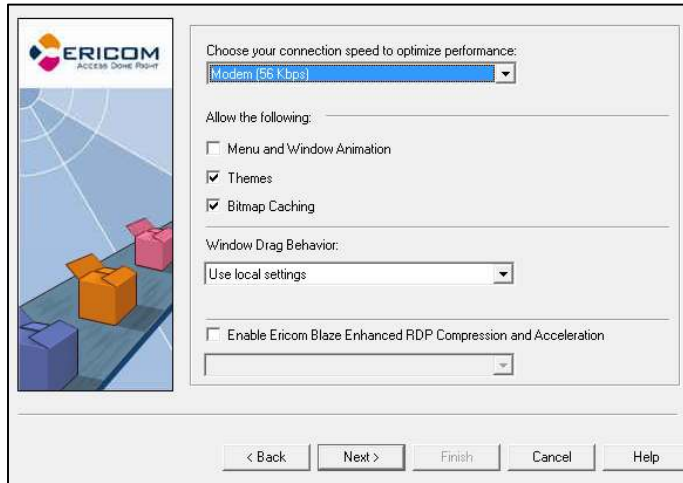


- *Color Quality* – sets the desired color depth of the published application. Seamless type
 - *Prefer Microsoft Seamless* – where possible, use Microsoft’s seamless engine. If not available, Ericom’s seamless engine will be used. Microsoft’s seamless requires Windows XP SP3 or higher on the client end and Windows Server 2008 or higher on the Terminal Server.
 - *Always Use True Seamless* –uses Ericom’s seamless engine.

NOTE Ericom Seamless does not support systray icon redirection for published applications (i.e., Communicator systray will not appear in the local systray). Ericom Seamless is generally more stable than Microsoft Seamless.

- When running applications that require administrative privileges on Windows Vista / 7 / 8 / 2008 / 2008 R2 / 2012 - an elevation screen is displayed. Microsoft seamless will display the elevation screen for the first application in the session if it is required. However, it will not display the elevation screen for other applications in the same session (where session sharing is enabled). Ericom *True Seamless* will properly display the elevation screen for any application launched during the session. For this reason it is recommended to use Ericom True Seamless when publishing applications that require elevation.
- *Run mode* determines the state of the window when the application is first launched. Available settings are: *Normal, Maximized, Minimized.*

Step 6: Performance



- *Connection speed* - choose the value that matches the slowest connection on the network. This will automatically determine the optimization settings. Preset settings can be manually adjusted.
- *Windows Drag Behavior* - Select *Show outline only* for better performance (since window content is not displayed during dragging, there is less network overhead.)

NOTE If *Show window content* is selected, it will also need to be enabled on the RDP host. The configuration varies based on the operating system, search the Internet for "*Show window content*" to find instructions.

- *Enable Ericom Blaze* - Check this setting to enable Ericom Blaze RDP WAN acceleration (see chapter on Ericom Blaze). Select the desired Blaze setting from the drop down menu.

STOP When enabling *Blaze* for a connection, verify that the destination host (Terminal Server or VDI desktop) has Access Server running. Access Server must be manually installed on the host operating system. The Access Server installer is found in the *WebConnect 6.X | AddOns* directory (i.e., \Program Files\Ericom Software\WebConnect 6.X\AddOns\Blaze\EricomBlazeServer.msi)

Step 7: Requirements

This dialog sets redirection settings of local resources. Resources available for redirection are sound, printers, serial ports, Smart Cards, and disk drives.

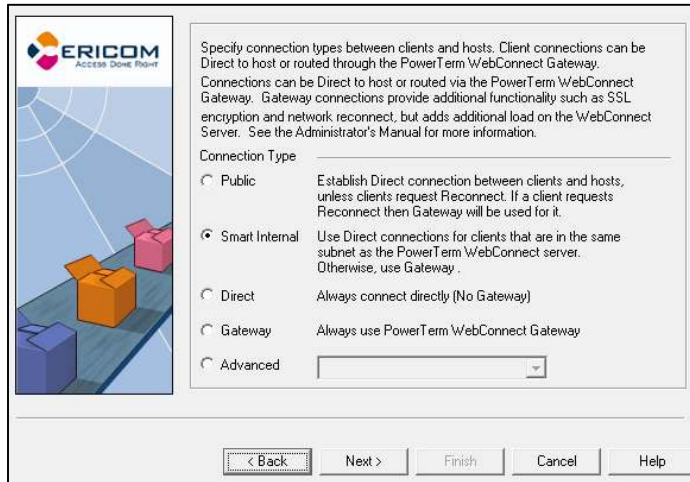
NOTE Ericom Blaze does not support Serial Port and Smart Card redirection

Step 8: Set the Connection Types

The most commonly used connections types are explained on the dialog box.

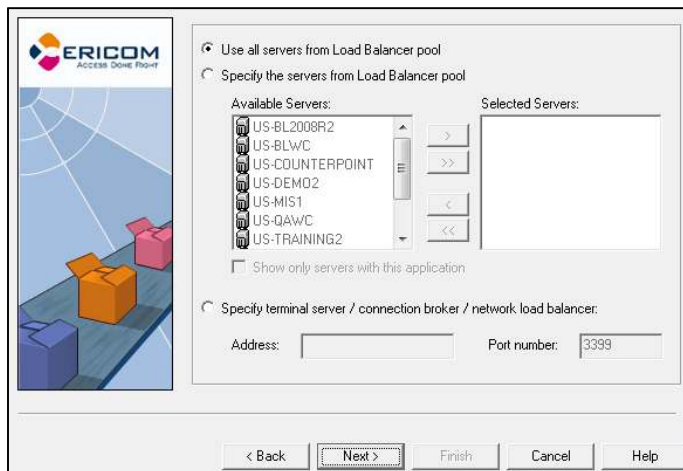
The *Advanced* setting presents a list of built-in and custom *Connection Points* that can be used as the connection type for the published resource.

The *SmartExternal* setting is not commonly used. When this setting is enabled, clients on the internal network (same subnet as the PowerTerm WebConnect server) will use *Gateway* mode, while clients connecting from external locations will use *Direct* mode.



The screenshot shows the 'Connection Type' configuration window in the ERICOM Access Gate Point software. The window title is 'ERICOM ACCESS GATE POINT'. The main text explains that connections can be direct to the host or routed through the PowerTerm WebConnect Gateway. The 'Connection Type' section has five radio button options: 'Public', 'Smart Internal', 'Direct', 'Gateway', and 'Advanced'. The 'Advanced' option is selected, and a dropdown menu is visible next to it. At the bottom, there are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Step 9: Set the Server source



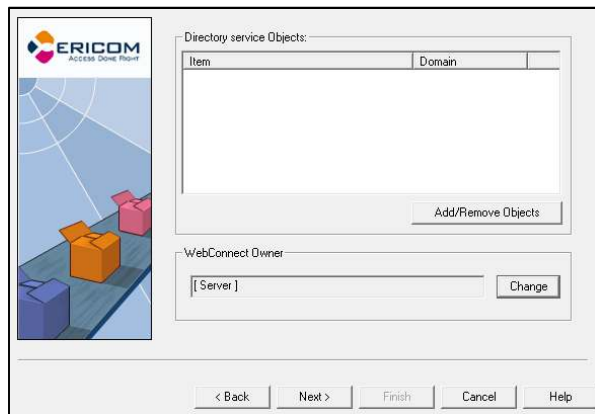
The screenshot shows the 'Server source' configuration window in the ERICOM Access Gate Point software. The window title is 'ERICOM ACCESS GATE POINT'. The 'Use all servers from Load Balancer pool' radio button is selected. Below this, there is a list of 'Available Servers' with checkboxes: US-BL2008R2, US-BLWC, US-COUNTERPOINT, US-DEMO2, US-MIS1, US-QAWC, and US-TRAINING2. To the right of the list are buttons for adding and removing servers. Below the list is a checkbox for 'Show only servers with this application'. At the bottom, there is a section for 'Specify terminal server / connection broker / network load balancer' with fields for 'Address' and 'Port number' (set to 3399). Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- *Use all Servers* (default) – the published application will be launched from any Terminal Server managed by the Load Balancer. Ensure that the application is installed properly on each Terminal Server configured under the Load Balancer.
- *Specify Servers* - select from a list of servers available in the Load Balancer. Only selected servers will be included as part of the load balancing process.

- Selecting *Show only servers with this application* will show the servers where the application is installed.
- To bypass the Load Balancer, select *Specify* and enter the address and port number of the desired Terminal Server to launched the application from.

Step 10: Select Owner(s) for the published application.

The *Owners* dialog assigns the connection to users or groups. The user and group may be a PowerTerm WebConnect object or Directory Service object.



- To assign the connection to a Directory Service object, click the *Add/Remove Objects* button.

NOTE Ensure that the Directory Service is properly configured or an error message will be returned:

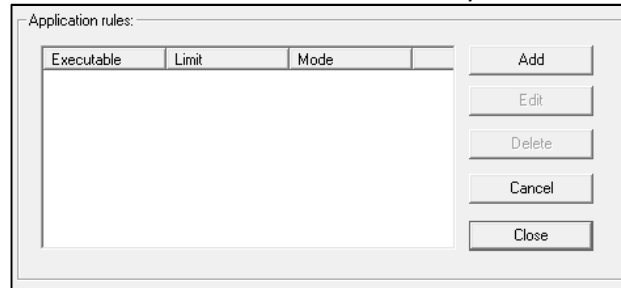


- The *Add/Remove Objects* dialog will appear. Navigate through the domain and select the desired objects to add. Click the *Show users* setting to display users under a selected OU. Click the *Add* button to add selected objects. Click *Close* when complete.
- Once Directory Services objects are selected, the *PowerTerm Owner* will automatically change to *Directory Services Access Only*.
- Applications may be published to OUs, Groups or Users.
- Groups may be members of one or more Groups, whereas OUs may belong to only one OU.
- To assign the connection to a WebConnect Owner, click the *Change* button. Select the desired WebConnect object to assign as the owner (only one per connection).

Step 11: Set the Execution Rules

Execution Rules limits how many instances of the published application can be run (also known as application limiting or metering). This is useful in preventing more than allotted licenses of a certain application from being launched.

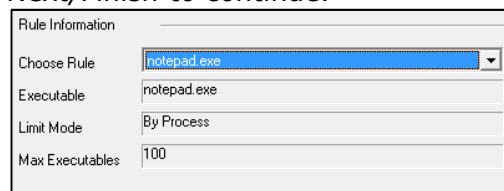
- Click *Edit Rules* to create or modify rules.



- Click *Add* to add a new rule
- Configure the rule
 - *Executable*: enter the executable to be managed
 - *Mode*: enter the criteria used for counting
 - *Limit*: enter the limit of running processes/users

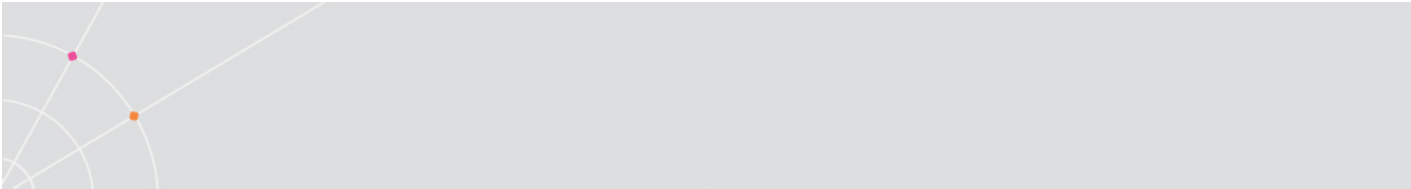


- To apply the rule, select it from the drop down list and click *Next/Finish* to continue.



Step 12: Information

The Information screen displays a summary of the configuration. Click the *Advanced* button to configure advanced functions for the connection. By default, the user's credentials and password are passed from pagent to the remote host (i.e., Terminal Server). Passing of credentials can be modified under the *Advanced* dialog.



- To disable credentials pass-thru from pagent, uncheck *User WebConnect User Credentials*.
 - To pass predefined credentials, enter the desired username/password.
- To disable the passing of the Domain information, uncheck *User Default Domain*.
 - To pass a predefined domain, enter the desired domain name.

Credentials

Username: Password:

Use WebConnect User Credentials

Domain:

Use Default Domain

- To disable the published connection uncheck *Enable*. Note that when a connection is copied, the duplicated connection will be disabled by default (unchecked).

Enable this Application

- Enter any environment variables that will be specific for this connection.

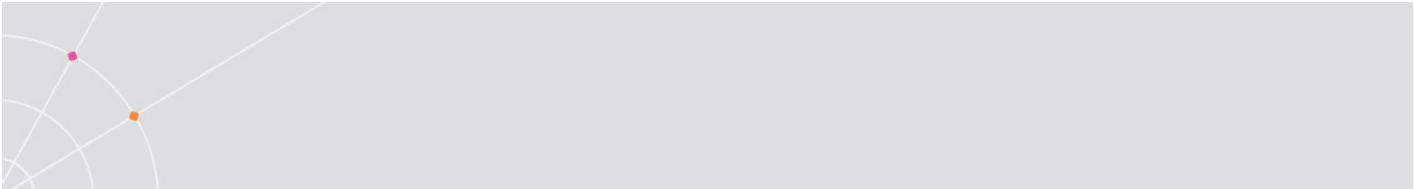
Environment Variables:

Name	Value
------	-------

- Click *Finish* and the published application will automatically appear in the Connection list and in the Application Zone for any active user that has access to the published resource.
- An authenticated user's username is represented by the environment variable %u

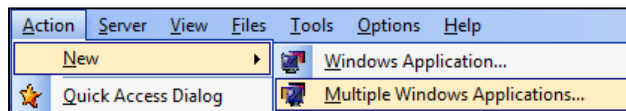
NOTE To authenticate to Windows 2012 (non R2) RDS servers, the following environment variable needs to be defined for the connection: Define *BLAZE_SETUP_PARAMS* and add: **username:s:<domain>%u**

This will append the user's domain to the username as the prefix as this is required to login to 2012 RDS servers (e.g. acmetest%u)



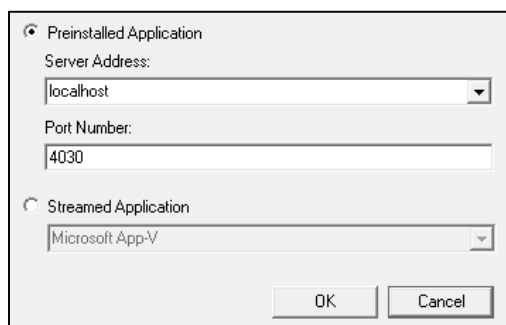
Publish Multiple Windows applications

This wizard will publish multiple applications at the same time. Use this feature to save time when publishing similar applications (i.e., applications part of the Microsoft Office suite).

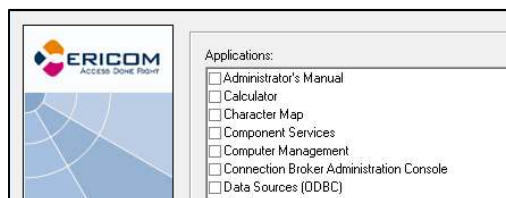


Step 1: Select the Browsing Source

- *Preinstalled* – applications that are already installed on a host.
- *Streamed* – applications that will be delivered to the host from a Microsoft App-V streaming server



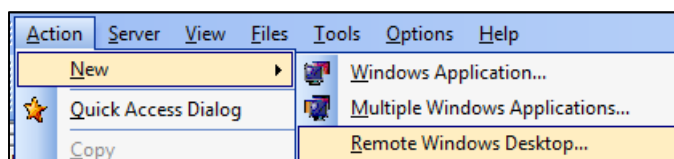
Upon selecting Preinstalled Application, an application selection list will be displayed. Select the applications to be published and click *Next* to continue.

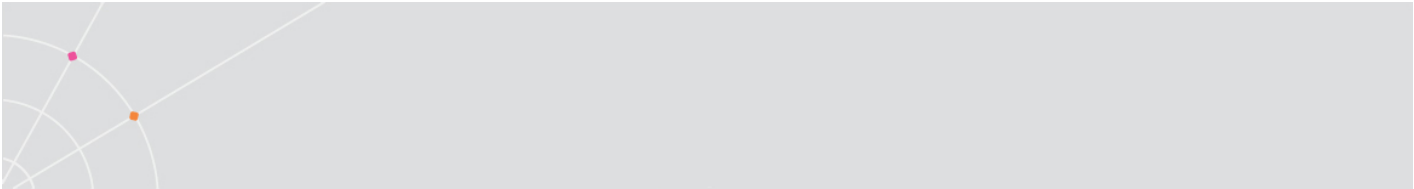


The wizard will display these steps from the *Publishing a Single Application* section: 4, 5, 6, 7, 8, 9, 10, and 12.

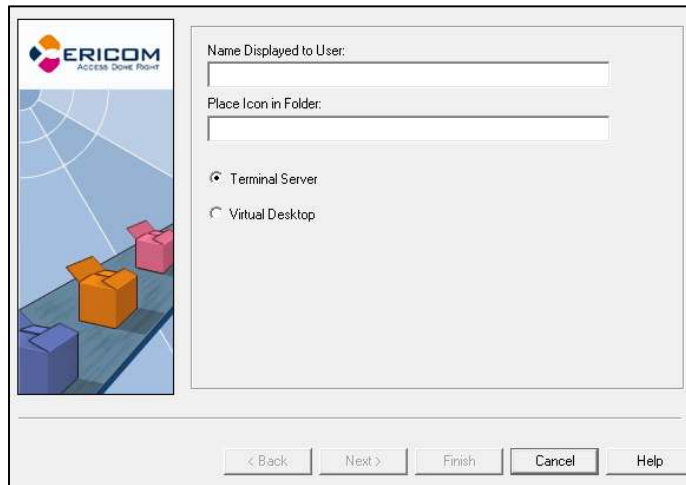
Publish a Full Desktop

This wizard will publish a Full Desktop session. To begin publishing: select Action | New | *Remote Windows Desktop*.





At the next prompt, enter the Target and Description



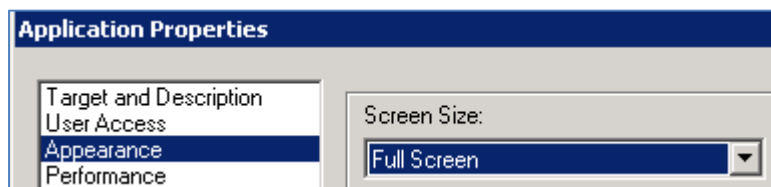
- *Name Displayed* – this is the name for the desktop connection that will be displayed to the user.
- *Place Icon in Folder* - To assign this application to a sub-folder, enter the *Place Icon in Folder* name. Sub-folders are separated with a '\\'.
- *Terminal Server* – select this to publish a desktop session from a Terminal Server
- *Virtual Desktop* – select this to publish a desktop session from a Virtual Desktop

The Remote Desktop wizard will display these steps from the *Publishing a Single Application* section: 4, 5, 6, 7, 8, 9, 10, and 12.

At the *Appearance* screen (5), select the desired screen size.

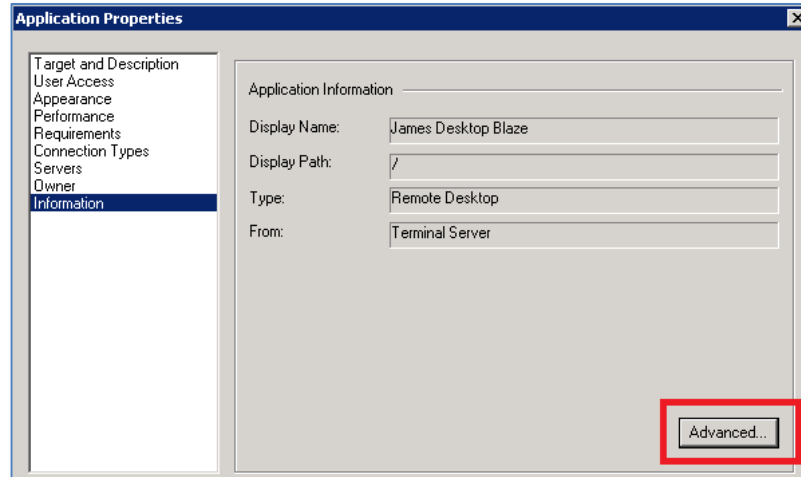
Multi-Monitor Support

When publishing a Full Screen Desktop session, the native clients will support multi-monitor functionality. Based on the RDP host operating system version, the session will span (Windows XP and 2003) across all monitors, or handle the multiple monitors natively (Windows 7 and higher & 2008 and higher).

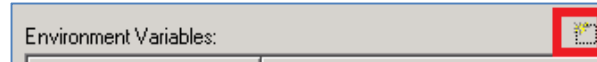


Full screen sessions may also be locked down to one monitor in a multi-monitor configuration. To limit the connection to display only on a certain monitor, perform the following:

- Open the Desktop Connection's *Properties* page.
- Click the Information tab and then the "Advanced" button



- In the "Environment Variables" section, add a new variable.



- Enter the following in the *Name* field: *RDP_FullScreenMonitor*
- The value can be one of the following:
 - 0 = Display on all monitors (Default)
 - 1 = Display only on monitor 1
 - 2 = Display only on monitor 2
 - 3 = Display only on monitor 3
 - X = Display only on monitor "x"

NOTE This value may also be set for all connections by adding it to the Server's configuration. This can be found by selecting *Server -> Configuration* from the Admin Tool's menu bar.

Publish a Desktop Session using an LDAP Attribute

One published Desktop connection may be used to publish unique desktop sessions for individual users. PowerTerm WebConnect can extract a configured LDAP attribute that represents the respective user's computer name or address. Follow these steps to use the %L variable to retrieve an LDAP attribute and then use it as the RDP host address:

- Publish a Full Desktop connection
- At the Server's dialog, select "*Specify terminal server ...*".

- Enter %L and then the attribute name in quotes. For example:

Specify terminal server / connection broker / network load balancer:

Address: %L"pager"

- In this example, %L will extract the value of the "pager" attribute from Active Directory (LDAP).
- This is how the pager value would be defined on the Active Directory (LDAP) server:

General | Address | Account | Profile | Telephones | Organization

Telephone numbers

Home: [] Other...

Pager: MyComputerName Other...

Mobile: [] Other...

Fax: [] Other...

IP phone: [] Other...

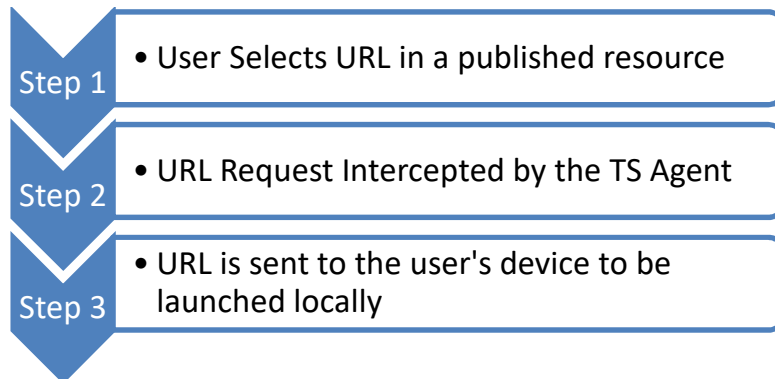
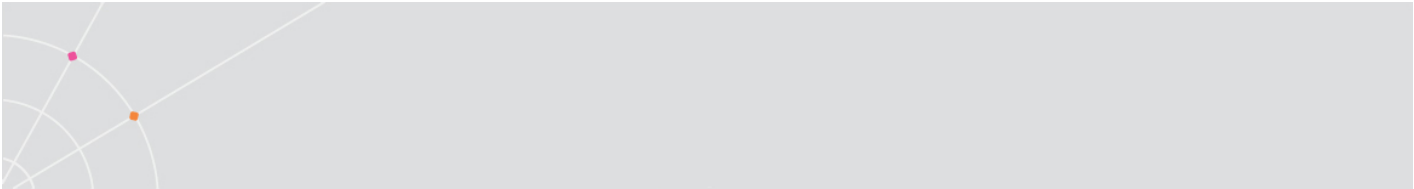
- The value of *MyComputerName* will be used as the address of the RDP host. This may also be defined using an IP address.

NOTE Custom LDAP attributes are also supported.

URL Redirection

URL redirection is a feature that intercepts URL requests on the Terminal Server, and redirects that request to the client device. This feature is compatible with RemoteView, Blaze, and AccessNow.

When a user clicks a URL in a document running on a Terminal Server, by default the browser would be launched from the Terminal Server. With URL redirection enabled, the browser will open on the client device instead.



Use URL redirection to:

- Reduce server load - running the browser on the client offloads the resource usage from the server. This is especially useful for web pages that contain streaming video or audio.
- Improve performance - Data streams flow directly between the client and URL source. RDP (which is not ideal for streaming content) is bypassed.
- Allow access - The Terminal Servers may not have access to the desired content. Some types of content downloads may be more appropriate for the client rather than the server (i.e., downloaded music files).
- Better security – Prevent malicious web content from being downloaded onto the Terminal Servers.

NOTE Windows 2012 RDP session hosts and Windows 8 RDP hosts are currently not compatible with the URL redirection feature.

Configuration

Any URL type may be redirected. A URL is a standard method to denote resource locations, and has the format: *host/resource-path*

URL Redirection supports the following schemes:

http	Hyper Text Transfer Protocol (web content)
https	Hyper Text Transfer Protocol Secured (via SSL)
ftp	File Transfer Protocol
telnet	Open an interactive terminal window with a telnet server
gopher	File transfer with gopher server.
news	Usenet newsgroups

nntp	USENET news using NNTP
mms	Microsoft Multimedia Messaging Service
rtsp	Real Time Streaming Protocol
itms	iTunes Music Store (Apple Music downloads)

NOTE AccessNow HTML5 only supports http and https URL redirection

By default, URLs are not redirected. In order to enable redirection, the *RDP_RedirectSchemes* Environment Variable must be defined on the PowerTerm WebConnect server. This Environment Variable contains a delimited list of the schemes to redirect. Only URLs that uses schemes specified in *RDP_RedirectSchemes* will be redirected. *RDP_RedirectSchemes* can be defined for a specific user, a group of users, a connection, or the entire server.

Excluding a URL from redirection

In some cases certain URL's should not be redirected (i.e., an intranet site). Add an Environment Variable *RDP_RedirectExclude* to specify which URLs should be excluded. *RDP_RedirectExclude* is a delimited list of the host addresses to exclude.

Host names specified in *RDP_RedirectExclude* are compared to the URL addresses from right to left (i.e., if "ericom.com" is specified in *RDP_RedirectExclude* it will match http://ericom.com, but also http://www.ericom.com and ftp://ftp.ericom.com).

IP addresses are compared left to right so 126.0.1 will match http://126.0.1.10 and also http://126.0.1.20.

NOTE Exclusion based on IP address is performed only if the IP address is explicitly specified in the URL. IP Exclusion is *not* performed if the host name is used in the URL instead of the corresponding IP.

Restrictions and Limitations

Installing a web browser or mail client on the Terminal Server *after* the Access Server agent has been installed may disrupt the redirection mechanism. In such a case, uninstall both the Access Server agent and the new browser or mail client and reinstall the new browser or mail client *before* the Access Server agent.

Restricting the user from making any changes in the registry on the Terminal Server, even in HKEY_CURRENT_USER, may cause the redirection mechanism to redirect *every* URL, regardless of the values in *RDP_RedirectSchemes* and *RDP_RedirectExclude*. (For standard Windows configurations, even restricted users have permissions to modify certain sections of the registry).

The redirection mechanism *does not verify* that the client supports a particular URL type or has Internet connection. Before redirecting a URL ensure that users will have access to it from their local devices.

URLs that are opened inside an application's browser control or using Internet Explorer's COM interface will not be redirected.

Viewing Application Publishing Properties

To view the properties and status of a published resource on PowerTerm WebConnect - double-click the desired connection (published application or desktop) from the *Connections* view. The *Application Properties* dialog will be displayed. The *Application Properties* dialog will display all settings that were configured during the publishing wizard (i.e., *Display Name*, type of connection, the host source, etc.)

Microsoft App-V Integration

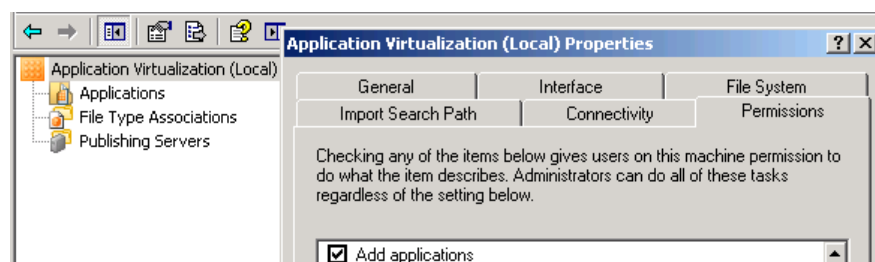
PowerTerm WebConnect supports application streaming and application virtualization through tight integration with Microsoft App-V. PowerTerm WebConnect enables easy publishing of App-V packages and supports streaming to end-point devices, Terminal Servers, virtual desktops and Blade PCs. The packaged applications can be launched from a web interface (Application Portal), a rich client interface (Application Zone), and from Desktop and Start Menu shortcuts.

PowerTerm WebConnect enhances App-V with features such as two-factor authentication, desktop integration with remote clients, centralized management, usage reporting and remote support.

PowerTerm WebConnect supports Microsoft App-V **4.5**.

Requirements

- The App-V Client must be pre-installed on the Terminal Server or end-user system running the streamed application. PowerTerm WebConnect does not deploy or update the App-V client.
- Configure the App-V client with *Add Applications* permission for all machines (Properties | *Permissions* tab of the App-V client).

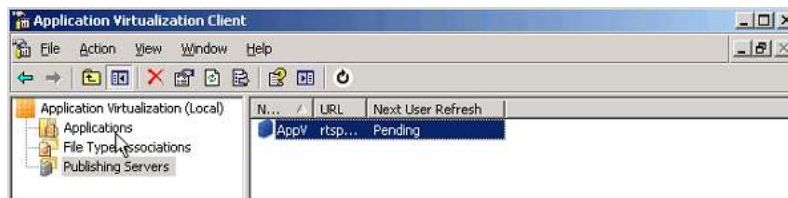


- Verify that App-V is working properly by itself before integrating with PowerTerm WebConnect. This will make it easier to identify and resolve App-V specific issues.

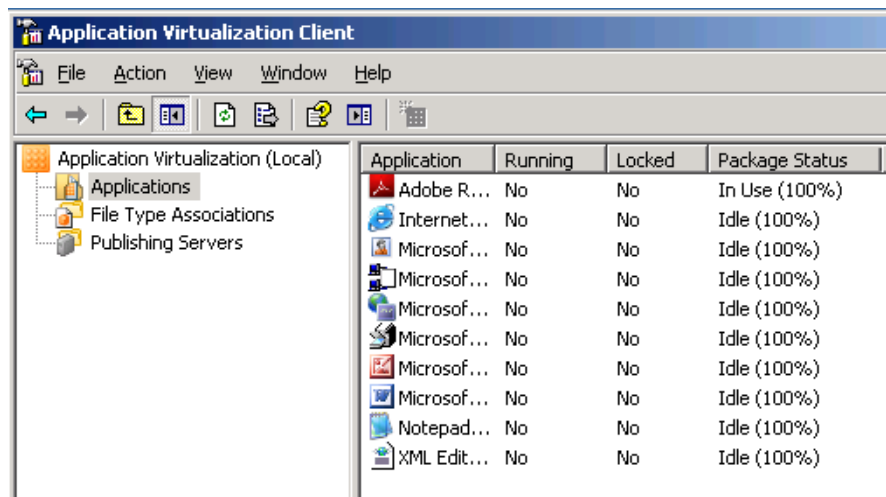
App-V Client Configuration on Terminal Servers

Perform the following when planning to stream applications from App-V to Terminal Servers. Streaming applications to Terminal Servers expedites deployment and standardization of applications.

Once the App-V client is installed, define the publishing servers.



Applications that appear in the Applications list of the App-V client will be streamed to the Terminal Server ready for publishing and usage.



Associations are published in one of two ways:

- Defining a Publishing Server and configuring App-V client to poll the configuration (upon user login / auto-refresh interval)
- Defining a Publishing Server and configuring App-V server to push the configuration (upon user login / auto-refresh interval)

File associations that were created during the App-V sequencing process will be automatically updated on the Terminal Server.

Extension	Description	Application
acrobats...	Adobe Acrobat Secu...	Adobe Reader 9 9.1.0.163
doc	Microsoft Word Docu...	Microsoft Office Word 2003
dochtml	Microsoft Word HTM...	Microsoft Office Word 2003
docxml	Microsoft Word XML ...	Microsoft Office Word 2003
dot	Microsoft Word Tem...	Microsoft Office Word 2003
dothtml	Microsoft Word HTM...	Microsoft Office Word 2003
fdf	Adobe Acrobat Form...	Adobe Reader 9 9.1.0.163
mdi	Microsoft Office Doc...	Microsoft Office Document In
pdf	Adobe Acrobat Docu...	Adobe Reader 9 9.1.0.163
pdfxml	Adobe Acrobat PDFX...	Adobe Reader 9 9.1.0.163
pdx	Acrobat Catalog Index	Adobe Reader 9 9.1.0.163

On the client-side machine, it is also possible to update the clients file associations to launch the published application when a user double-clicks on a local file. This is achieved by setting the required file associations during the publishing wizard.

Extension	File Type
<input type="checkbox"/> .acrobatsecurity	Adobe Acrobat Security Settings Document
<input type="checkbox"/> .fdf	Adobe Acrobat Forms Document
<input type="checkbox"/> .pdf	Adobe Acrobat Document
<input type="checkbox"/> .pdfxml	Adobe Acrobat PDFXML Document
<input type="checkbox"/> .pdx	Acrobat Catalog Index
<input type="checkbox"/> .xdp	Adobe Acrobat XML Data Package File
<input type="checkbox"/> .xdf	Adobe Acrobat Forms Document

App-V Client Configuration on End User Systems

Streaming applications to the end-user's device expedites standardization of applications and may result in better performance.

When working in this manner, the App-V client MMC GUI will be in read-only mode: no shortcuts are created and file associations are managed by the App-V client. This ensures that there will be no conflicts with PowerTerm WebConnect. Publishing servers do not have to be defined.

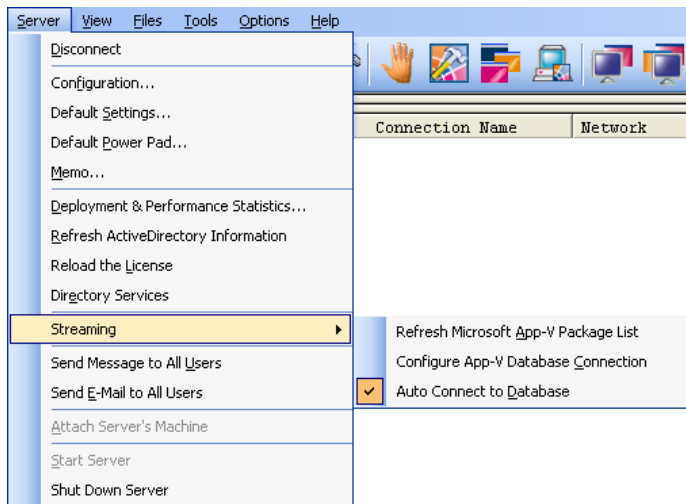
Configuring the App-V Server in PowerTerm WebConnect

Open the Administration tool and go to Server | *Streaming*. There are three options:

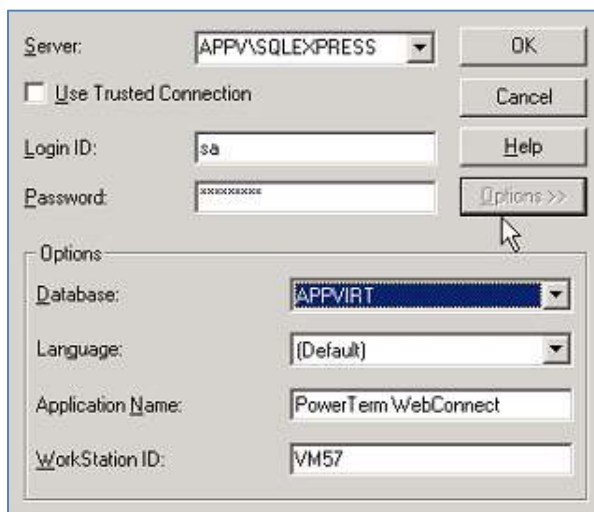
- *Configure App-V Database Connection*: opens Windows ODBC wizard for configuring the connection string to the App-V database. This setting will be saved into the PowerTerm WebConnect server environment variable *AppV_DatabaseConnectionString*.

- *Refresh App-V Package List*: forces an immediate refresh with the App-V database
- *Auto Connect to Database*: If enabled, the connection (and the retrieval of the package list) will be performed automatically each time the application publishing wizard is opened.

NOTE PowerTerm WebConnect Administration Tool must have network access to App-V database in order to view the available packages and publish App-V applications.



Select *Configure App-V Database Connection* and enter the parameters for the App-V server. Expand the options section and select the name of your App-V database (the default is "APPVIRT"). Once the server is configured, the *AppV_DatabaseConnectionString* will be automatically populated.

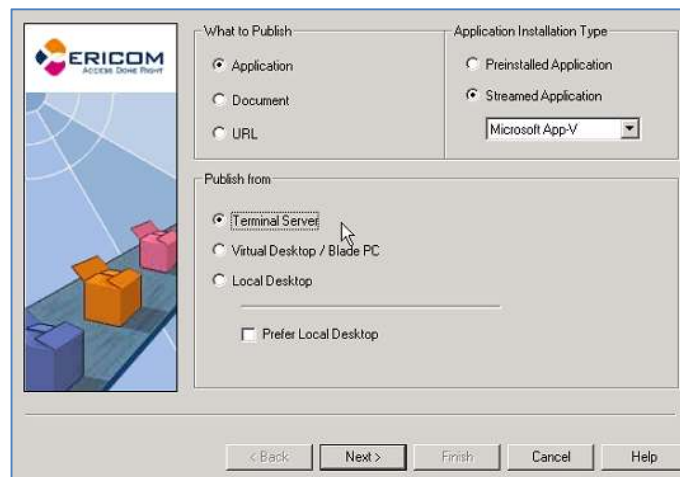


Publishing an App-V application

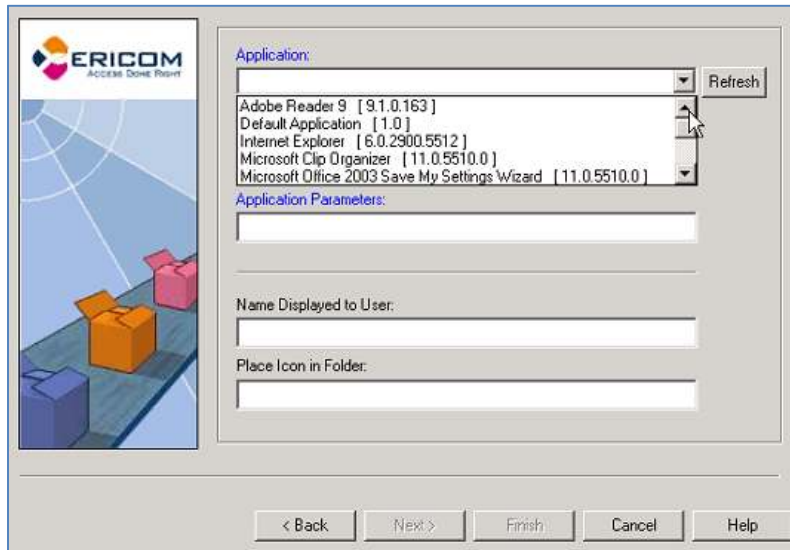
Use the Administration Console's publishing wizard to publish an App-V application.

At *Step 1*, select *Streamed Application* and select *Microsoft App-V*. Next, set the *publish* source:

- Terminal Server: the App-V application is streamed to a Terminal Server, which can then be published to the end user.
- Virtual Desktop: the App-V application is streamed to a virtual desktop, which can then be published to the end user.
- Local Desktop: the App-V application is streamed to the end user's system directly. The streamed application can run in off-line mode, however, PowerTerm WebConnect is required to launch the streamed application.



At *Step 2*, specify the App-V application to be published by selecting from the drop down list. Click the *Refresh* button to obtain the current application list. The name for the application will be automatically populated from the App-V database, what the user will see on the shortcut can be changed by changing the display name. Enter a subfolder name if desired.



If the drop down list is empty, click the refresh button, if this fails check your App-V connection settings.

At *Step 3* a list of extensions will be displayed. The extension list is obtained from the App-V server. This list will only be visible for App-V applications that are streamed to a Terminal Server or virtual desktop.

NOTE App-V applications that are streamed to the Local Desktop have their extensions managed by the App-V client.

Publishing App-V applications require Session Sharing so complete the remaining of the steps of the wizard similarly for all App-V applications.

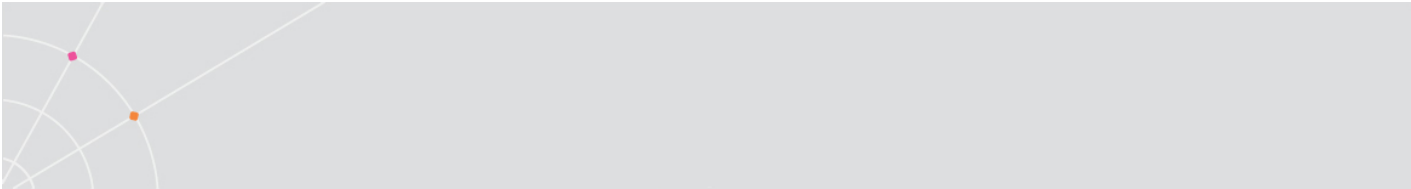
Launching App-V published applications

Launching published App-V applications are just like launching Terminal Server based applications. The user simply has to point and double-click the desired application.

Streaming applications to the end-user's device

App-V applications may be streamed directly to the end-user's device using any of the Ericom user interfaces, such as Application Zone. For users who are working on the internal LAN, applications may be streamed using the RTSP protocol.

For users connecting over the Internet, configure App-V streaming to use HTTP or HTTPS. If packages were created using RTSP, use the WebConnect variable *RDP_AppV_DefContentPath* to override the setting in the App-V database. The OSD files will need to be manually changed to HTTP/HTTPS.



The process of streaming applications from the App-V server to the client is performed solely by App-V, the PowerTerm WebConnect Gateway is not used.

Related Environment Variables

AppV_DatabaseConnectionString – contains the connection string to the AppV Database. This value is automatically populated by configuring Server | Streaming | *Configure App-V Database Connection*.

RDP_AppV_DefContentPath (optional) - This allows an administrator to override the path specified in the App-V database for OSD files (ignore what is specified in the App-V database.) This value defines the path to App-V content folder and gives the Administrator the flexibility to override the path contained in the existing packages without the need to change them.

The variable can be defined using a UNC path, this is the default setting for App-V known as RTSP (applicable if all users are within the organization) or an HTTP path (applicable for users located outside the organization).

For example, setting this to: *RTSP://AppV:554/content/* will override the location specified in the App-V database and look in the above location instead.

RDP_AppV_SFT_SOFTGRIDSERVER – When the App-V client is installed, it creates a variable named *AppV_SFT_SOFTGRIDSERVER*. This value contains the name of the App-V server. Once set, this variable is automatically passed to the client when the user logs into Application Zone. By default, App-V Package Sequencer uses the “SFT_SOFTGRIDSERVER” Windows variable inside the package which represents the address of the streaming server or load balancing device. App-V requires that this variable will be configured on all App-V client machines. This WebConnect variable is the equivalent of the Windows environment variable. RemoteView will set the SFT_SOFTGRIDSERVER variable on all App-V enabled machines for internal and external users. Setting this environment variable requires administrator privileges.

NOTE After this variable is set, the user's machine must be restarted.
--

Copy a connection based on an existing one:

- Select a Connection to be copied and right-click it; then select *Copy*. The Copy Connection dialog will appear.
- Type in a new *Connection Name*. This will be a unique identifier for the connection. Once it has been set, it cannot be changed later on. If you wish to change the ConnectionName, simply copy the existing Connection, enter the desired name, and delete the one that will no longer be used.

- Click *OK*. The new connection will be created and the *Connection Properties* dialog will appear.
- Make necessary modifications. Verify that the *Display Name* is unique and then enable the connection.
- Click *OK*. The new connection appears with its own unique properties in the *Connection* pane.

NOTE A copied connection is initially disabled. It must be manually enabled for users access it. Go to the Connection's Properties | Information | *Advanced* button to *enable* the application.

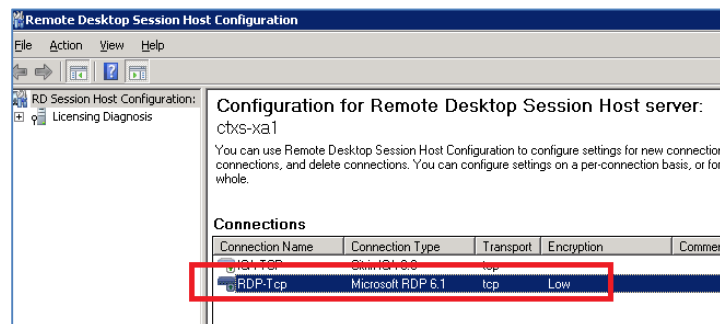
Enable this Application

Publishing Applications/Desktops from a Citrix XenApp Server

Existing Citrix XenApp servers may be used as Terminal Servers (or RDS Servers) in an Ericom Terminal Server "farm". Two configuration changes need to be added to the XenApp server in order to allow incoming RDP connections.

Enable RDP on the XenApp Server (i.e. Windows 2008 R2)

- Open the Remote Desktop Session Host Configuration
- Select Create New Connection
- Select RDP for the Connection Protocol



- Click *Next* and complete the configuration. Go to the protocol's *Properties* to perform any additional configuration for RDP.

Allow Application and Desktop Access

Citrix XenApp Servers prevent users from launching applications directly over RDP. This restriction can be removed by performing the following on the Citrix XenApp (6.0) server that will be used as a Terminal Server:

NOTE This information is taken from the Citrix website and may vary for different versions of Citrix Presentation Server or XenApp. Website link: <http://support.citrix.com/article/CTX124745>

Changing the Default Unfiltered User Policy Settings for ICA in the DSC

To change the default unfiltered User policy settings for ICA in the DSC, complete the following procedure:

1. Select **Policies**.
2. Activate the **User** tab (you notice the default unfiltered policy).
3. To access the default policy settings, activate the **Settings** tab in the lower pane.
4. Click **ICA** on the Categories window.

Allowing Non-administrative Users to Connect to the Server Desktop

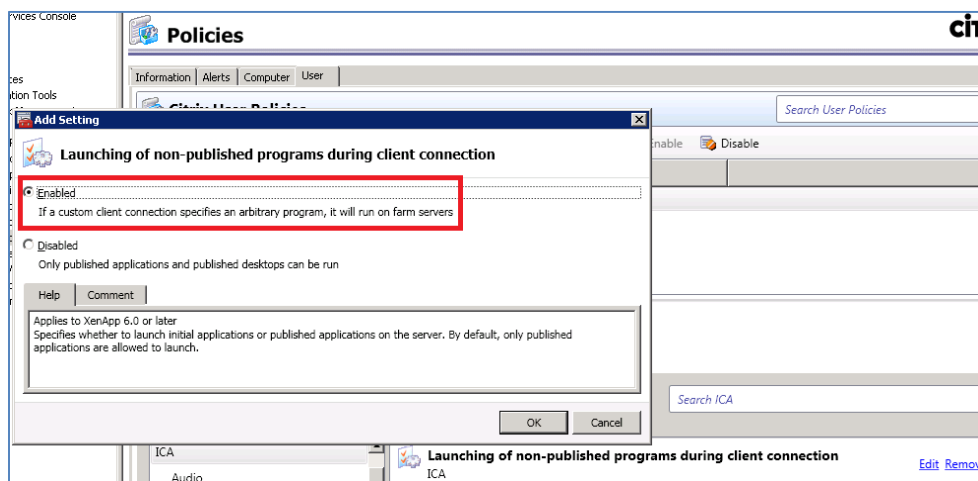
To allow non-administrative users to connect to the server desktop, complete the following procedure:

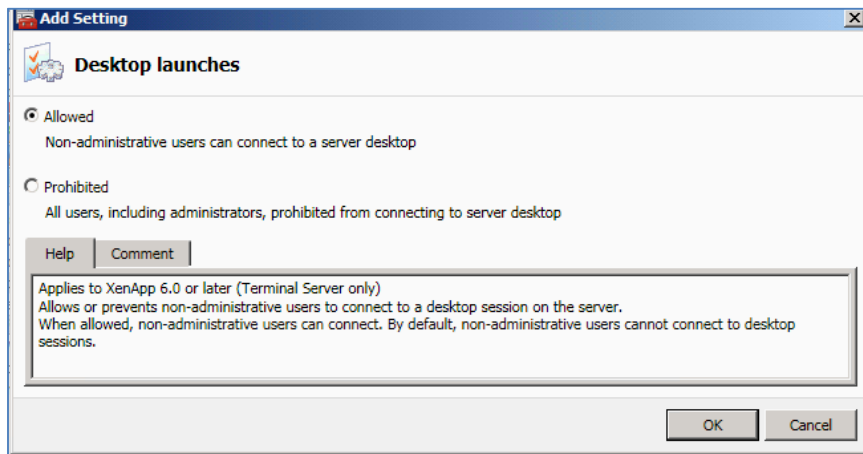
1. Click the **Add** link for starting the Desktop.
2. Select **Allowed**.
3. Click **OK**.

Allowing Non-administrative Users to Start Any Application during Client Connection

To allow non-administrative users to start any application during client connection, complete the following procedure:

1. Click the **Add** link for starting the non-published programs during client connection.
2. Select **Enabled**.
3. Click **OK**.

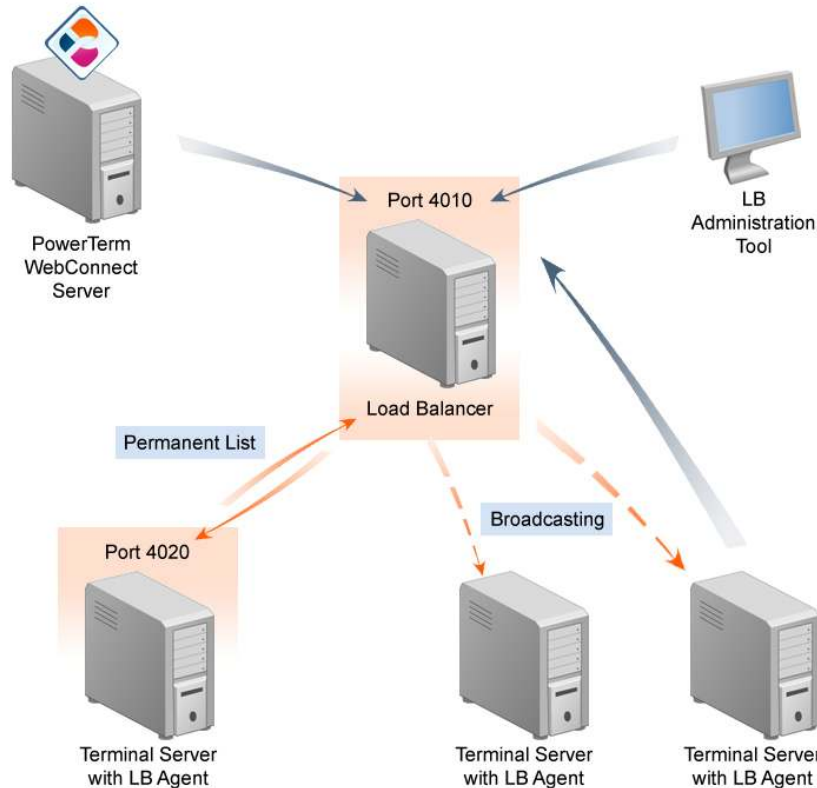




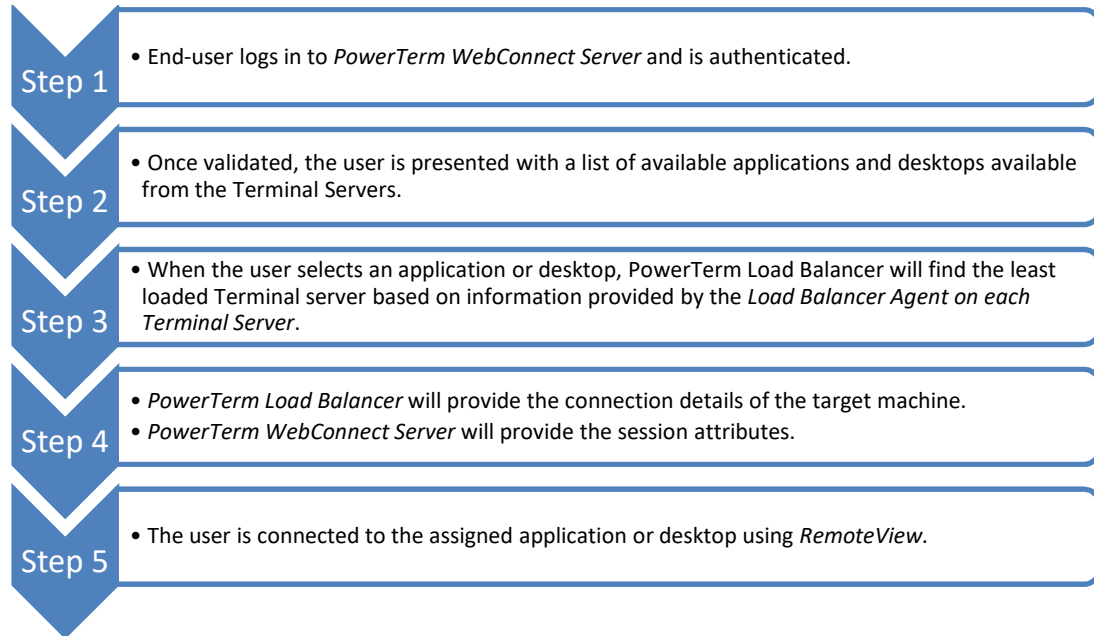
13. CONFIGURING POWERTERM LOAD BALANCER

The PowerTerm WebConnect Load Balancer is designed to distribute user requests evenly in an Ericom Terminal Server farm and avoid resource bottlenecks. The Load Balancer is comprised of three components:

- PowerTerm WebConnect Load Balancer Server gathers real-time information from the Terminal servers and routes incoming users requests to the least loaded server.
- PowerTerm WebConnect Load Balancer Agent provides the Load Balancer with resource usage information of the server it is running on.
- PowerTerm WebConnect Load Balancer Administration Console manages settings associated with the Load Balancer. All settings are stored in a XML formatted configuration file (LoadBalancer.xml).



Load Balancing Process Overview



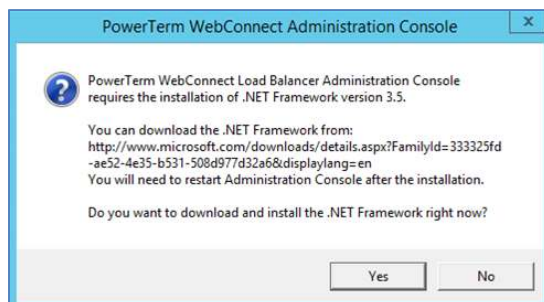
Installation

PowerTerm WebConnect Load Balancer is automatically installed with the *Full Installation* option of the installer.

To install *PowerTerm WebConnect Load Balancer Administration Console* after *PowerTerm WebConnect Server* has already been installed, go to *<PowerTerm WebConnect Installation Folder>\WebConnect 5.X\AddOns\LoadBalancerAdmin\LoadBalancerAdmin.msi*.

The *Load Balancer Server* may also be installed independently by running *PTLBServer.exe* that is included with the original installation media (same location as the installer for *PowerTerm WebConnect*).

On Windows 2012 servers, enable *.Net 3.5* when installing *the Application Server* role. If *.Net 3.5* is not installed, the following error message will appear when the *Load Balancer admin console* is launched:



PowerTerm Load Balancer Server

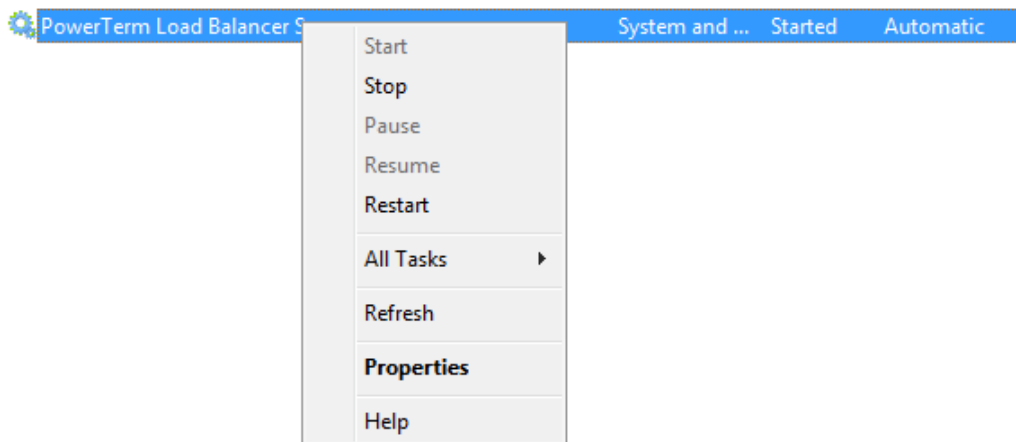
The PowerTerm WebConnect Load Balancer server runs as a Windows service. By default, PowerTerm WebConnect Load Balancer server listens over TCP port 4010. This can be modified using the command line or XML and cannot be changed via the PowerTerm WebConnect Load Balancer Admin Tool.

The PowerTerm WebConnect Load Balancer Agent is periodically collecting information about the server it is loaded on and reports the gathered data to the Load Balancer server at a pre-determined interval. If no information is received from a Terminal server within a five minute interval, the Terminal Server is classified unavailable in the PowerTerm WebConnect Load Balancer.

Starting/Stopping the Load Balancer service

The PowerTerm WebConnect Load Balancer runs as a service and can be started and stopped using the Services MMC plug-in (`services.msc`).

From the server running the PowerTerm WebConnect Load Balancer Server run `services.msc`. Next, right-click on the *PowerTerm WebConnect Load Balancer Server*, and select the desired operation.



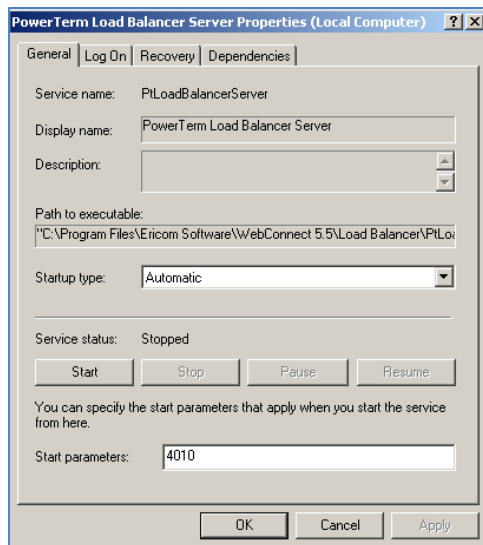
Modifying PowerTerm WebConnect Load Balancer's Port

The Load Balancer's port can be modified under the service's properties.

From the server running the PowerTerm WebConnect Load Balancer Server run `services.msc`. Right-click on the *PowerTerm WebConnect Load Balancer Server*, and select *Properties*. Modify the Load Balancer's port by entering the desired port number in Start parameters.

Backing up the Load Balancer configuration

All settings are saved into the LoadBalancer.xml file. To back up the configuration, simply copy this file to an alternate location. To restore/import saved load balancer settings, simply copy this file back to the Load Balancer folder and restart the service.

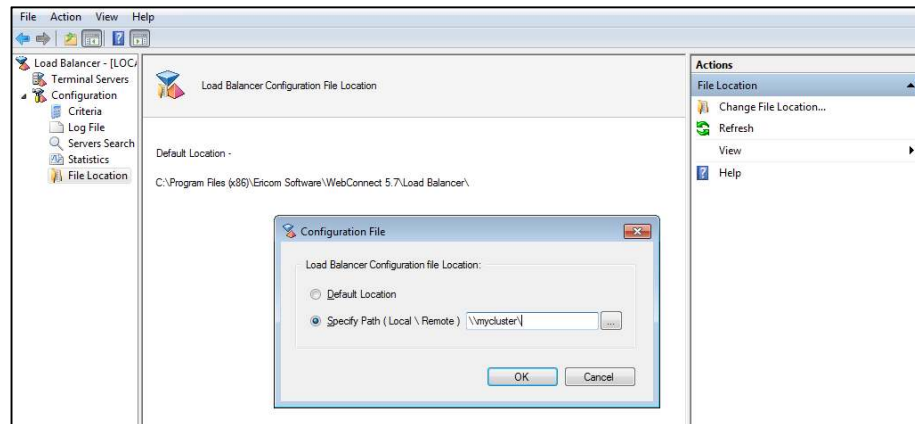
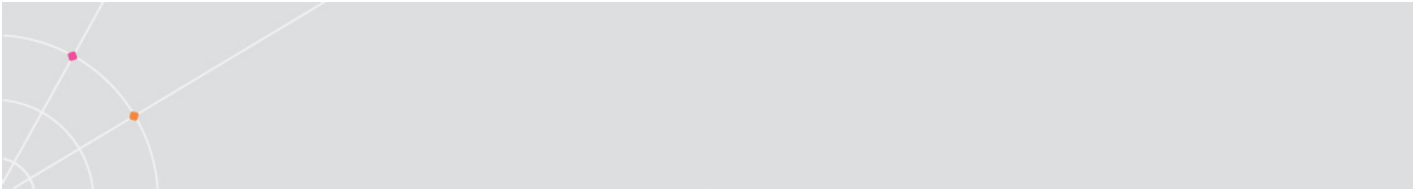


Clustering the Load Balancer

For the Load Balancer to operate in Cluster mode, use the Load Balancer Administration Console to specify the path of the cluster (shared) database. All servers that will use the shared database need *Full* permissions to access the Configuration file path.

Configuring the Cluster Path

- Open PowerTerm Load Balancer Administration Tool.
- Go to Configuration | *File Location*. Under the Actions pane, select *Change File Location*.



- Select Specify Path and enter the location of the centrally shared directory of the database (XML file).
- Click OK.

NOTE Cluster mode can only be enabled if the full network path is defined in the PtServer.ptr file; and the PtServer.ini file is defined with the *local* path to the license file.

If the full network path is defined in the PtServer.ptr file, but the PtServer.ini file is defined with the *network* path to the license file, the PowerTerm® WebConnect Server will operate in Failover mode.

PowerTerm Load Balancer Agent

PowerTerm WebConnect Load Balancer Agent (PtLoadBalancerAgent.exe) is installed along with the *Ericom Access Server*. *PowerTerm WebConnect Load Balancer Agent* runs as a Windows service and must be installed on every Terminal Server that will be part of the Ericom PowerTerm WebConnect farm.

PowerTerm WebConnect Load Balancer Agent sends resource information to the Load Balancer Server at least once every 5 minutes, or when there is a 5% or greater change in any of the Load Balancing Criteria. All related activity is tracked in the log file (*PtLoadBalancerAgent.log*). The ten most recent logs are saved (named as *PtLoadBalancerAgent.bck-XX.log*).

NOTE A new log is created each time the service is started, or when the log size exceeds 1MB.

PowerTerm WebConnect Load Balancer listens over TCP port 4020, but the port can be changed either via the command line or via the registry.

Support

To diagnose problems related to the Load balancer Agent, a log is required.

Perform the following to enable logging for the Load Balancer Agent (this is different than the TSAgent log).

- Open *Regedit.exe* and go to HKLM | SOFTWARE | WOW6432NODE | ERICOM SOFTWARE | PTLOADBALANCERAGENT
- Change the value of CREATELOGFILELEVEL to F
- Restart the *Load Balancer Agent* service
- A log file will be created under C:\Program Files (x86)\Ericom Software\PtTsAgent named *PtLoadBalancerAgent.log*

Please send this log to Ericom Support once the issue with the Load Balancer Agent is observed.

PowerTerm Load Balancer Administration Tool

PowerTerm WebConnect Load Balancer Administration Console (PtLoadBalancerAdmin.exe) is used to view and set all of the Load Balancer's parameters and attributes. The Load Balancer Administration Console is an MMC snap-in module

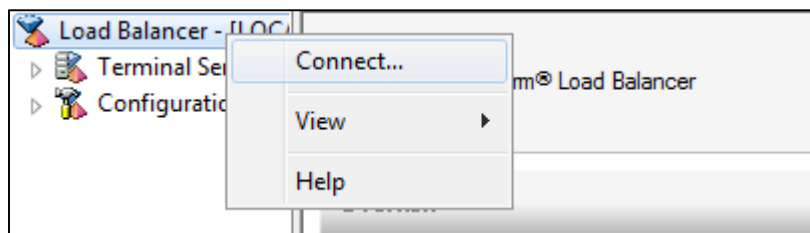
Using the PowerTerm WebConnect Load Balancer Administration Tool, the administrator determines the how the balancing criteria is applied across the Terminal Server farm. The Load Balancer Admin Console may be launched from the Start | Programs | Ericom Software | PowerTerm WebConnect | *Load Balancer* folder or by click its icon from the Administration Tool.



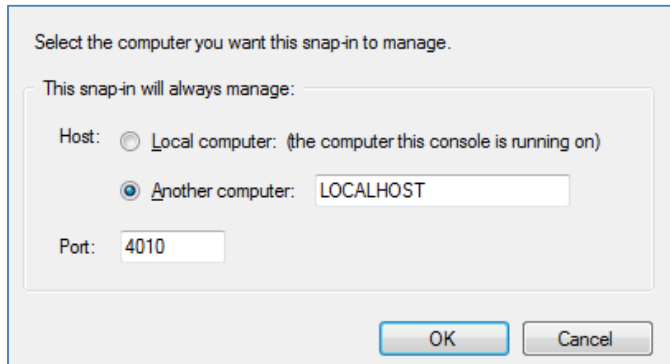
NOTE When launching the Load Balancer Admin console from the PowerTerm WebConnect Admin tool, it will use *gateway* mode, if a gateway is configured. This is so the admin console may be launched securely from a remote location using the Ericom Secure Gateway.

Connecting to Load Balancer

To connect to a Load Balancer Server launch the Load Balancer Tool Administration Console and right-click *Load Balancer* and select *Connect*.



A Connect dialog will appear.

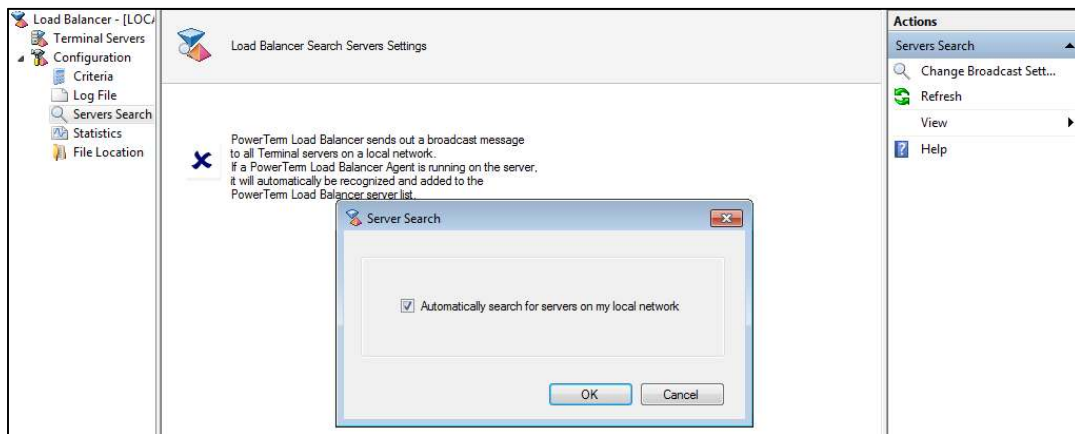


Enter the address and port of the Load Balancer Server and click OK to connect.

Adding Terminal Servers

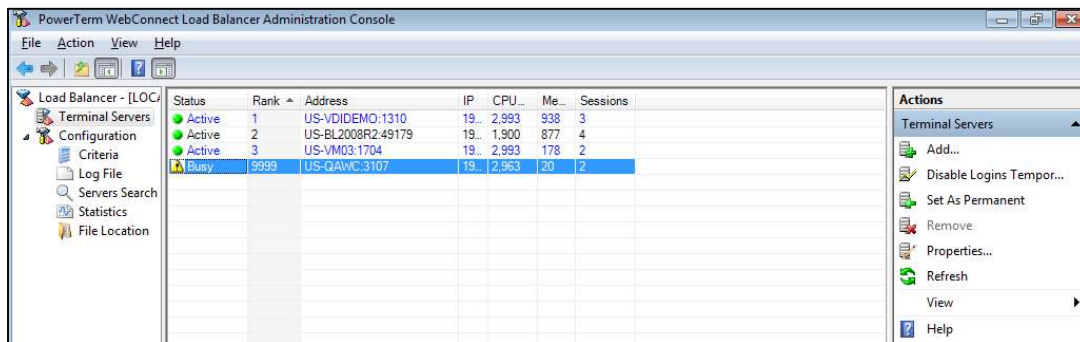
Automatic Discovery

PowerTerm WebConnect Load Balancer Server sends broadcast messages to all Terminal servers. If a Load Balancer Agent is running on a server, it will be detected and added to the PowerTerm WebConnect Load Balancer server list if the *Automatic search* is enabled under *Server Search*.



NOTE Clearing the setting will remove any active server from the load balancer list that was added with the discovery feature

Terminal servers that have been found via automatic search will be displayed in blue text, as shown here:



NOTE PowerTerm WebConnect Load Balancer broadcasts do not work across subnets

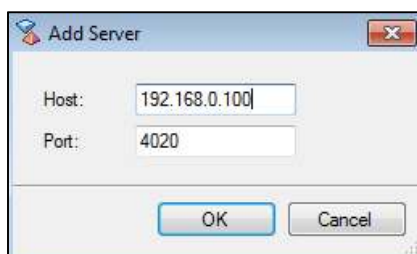
Permanent Mode

A server added via automatic discovery can be converted to permanent mode. A permanent server is one that is not managed by automatic discovery. If automatic discovery is disabled, permanent servers will not be removed. If a server is *permanent*, but not connected, PowerTerm Load Balancer will try to reconnect every 30 seconds.

NOTE Automatically discovered servers cannot be removed manually from the list unless it has been set to *Permanent*.

Manually Adding Servers

Additional servers can be manually added to the PowerTerm WebConnect Load Balancer list by selecting *Add*. Enter the server address when prompted to add a new server. All manually added servers are *permanent* mode.



If any added server does not have the Load Balancer Agent running, it will be displayed as *Not Connected*. Not Connected | N/A


Viewing Server Properties

Double click on any Terminal Server in the load balancer list to view its properties:

Address:	US-VDIDEMO:1320
IP:	192.168.35.77
Operating system:	Windows 2003 Server
Number of CPUs:	1
CPU (MHz):	2.993
Physical memory (MB):	1.499
<input type="button" value="Close"/>	

Disable Logins


To prevent logins to any server in the list, highlight the desired server and select *Disable Logins*.

 Disable Logins Temporarily

A Terminal Server that is disabled will be set to Busy and displayed in gray.

 Busy 99999 US-DEMO2-1826


To enable logins in a disabled Terminal Server, click *Enable Logins*.

 Enable Logins

Removing Manually Added Servers

To remove a server from the load balancer list - highlight the desired server and select *Remove*.

The administrator will be prompted to confirm removal of the server. Select *Yes* to remove the server. The server can be added back in the future.

 Are you sure you want to remove server 192.168.0.100:4020?

NOTE When a server is removed from the Load Balancer, it will also be removed from ALL connections that explicitly use it.

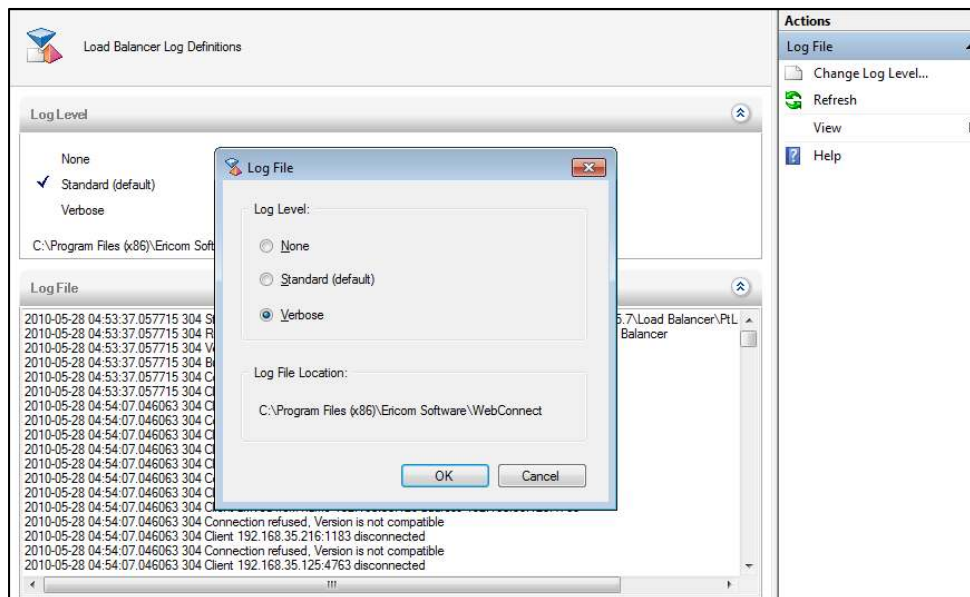
Logging

There are two different types of Load Balancer log files:

Standard - traces how the different servers connect and disconnect to PowerTerm WebConnect Load Balancer.

Verbose - traces all activity on PowerTerm WebConnect Load Balancer, such as connection history, packet sizes, etc.

To enable logging, Launch the PTLB Administration Console and select Configuration | *Log file*. The current log file will be displayed. To change the logging setting, select *Change Log Level*.



PowerTerm WebConnect Load Balancer server generates a log file in the current directory (PtLoadBalancerServer.log). The last ten log files are saved and named PtLoadBalancerServer.bck-01.log, PtLoadBalancerServer.bck-02.log etc.

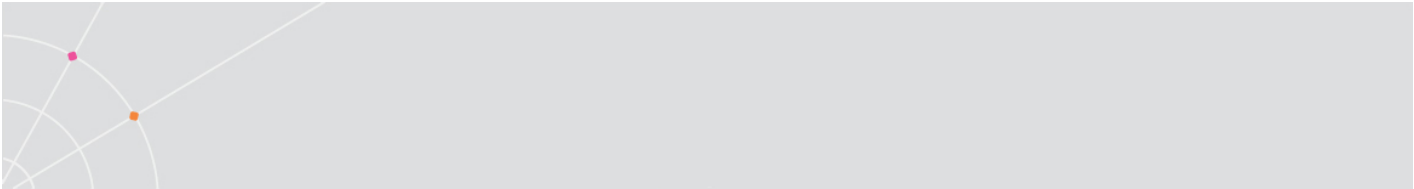
NOTE Every time the service is started or the log size of 1MB is reached, a new log is created.

Optimizing the Load Balancer

Onrush Blocking

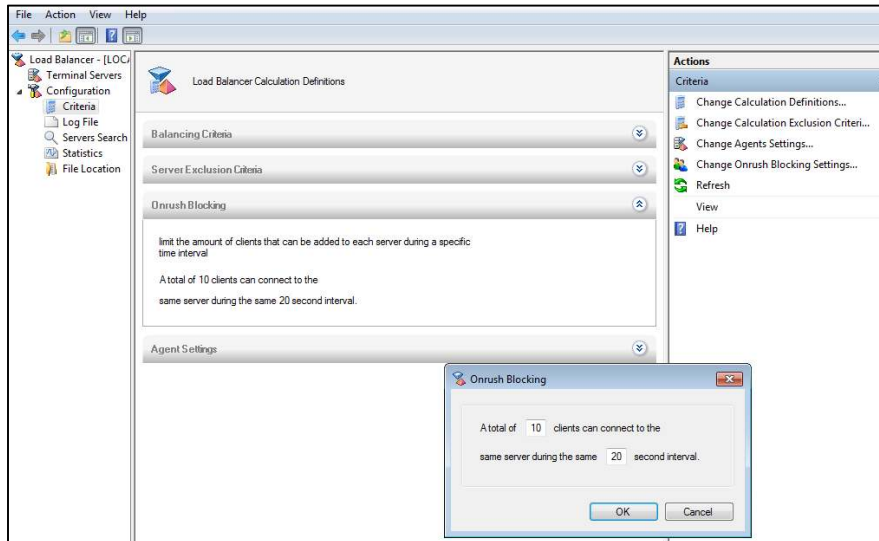
When a fresh server is brought online into a load balanced environment, the tendency is to send all user logins to the new server as it is the least loaded. The onrush of logins will overwhelm the new server and cause a "black-hole" effect. An onrush situation is where users will be unable to connect to the Terminal Server, and the server may even crash.

To avoid onrushing, PowerTerm WebConnect Load Balancer can be configured to only allow a specific number of clients to connect during a set interval. This will balance the amount of logins directed toward any specific server and eliminate access problems associated with onrush activity.

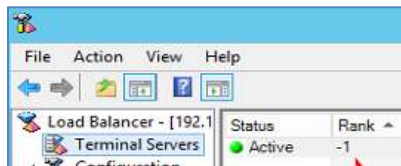


Configuring Onrush Blocking

Select *Criteria* from the Configuration menu and select *Change Onrush Blocking*. Enter the values for the total amount of users that can connect during any given interval.



When a server has Onrush Blocking activated, it will be ranked with a **-1**.



Setting the Balancing Criteria

The Balancing Criteria is a set of parameters that defines the most eligible Terminal Server for user access. To change the criteria calculation go to Configuration | Criteria | *Change Calculation Definitions*.

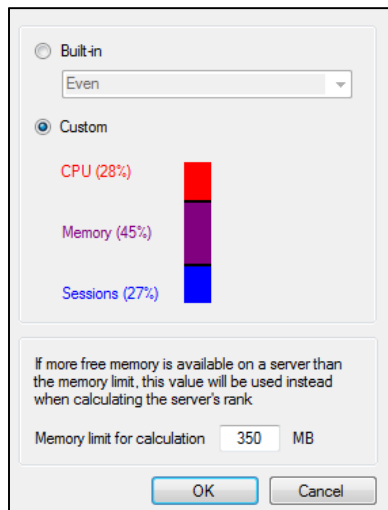
Built-In Load Balancing Options

Value	Definition
Memory Driven (default)	Memory is given the most emphasis among the criteria
CPU Only	CPU is the sole emphasis among the criteria
Memory Only	Memory is the sole emphasis among the criteria
Sessions Only	The number of sessions is the sole emphasis among the criteria

Custom Balancing Configuration

The administrator can decide (by adjusting the two bars) what percentage of the Memory, CPU and Sessions will be used to set the load balancing criteria.

The *Memory Limit for Calculation* balances the memory calculation between all Terminal Servers. If one server has a much more memory than others in the list, this setting does not give it an advantage over the other servers. This value is substituted for the machine's memory size when calculating the server's rank. The result is better user distribution between all listed servers.



Built-in
Even

Custom

CPU (28%)

Memory (45%)

Sessions (27%)

If more free memory is available on a server than the memory limit, this value will be used instead when calculating the server's rank

Memory limit for calculation MB

OK Cancel

Server Exclusion Criteria

A server is disqualified from user access if it exceeds any of the specified values in CPU usage or Sessions, or does not reach the required Available Memory level. This is in contrast to the Balancing Criteria which determines the eligibility of a server to accept requests.

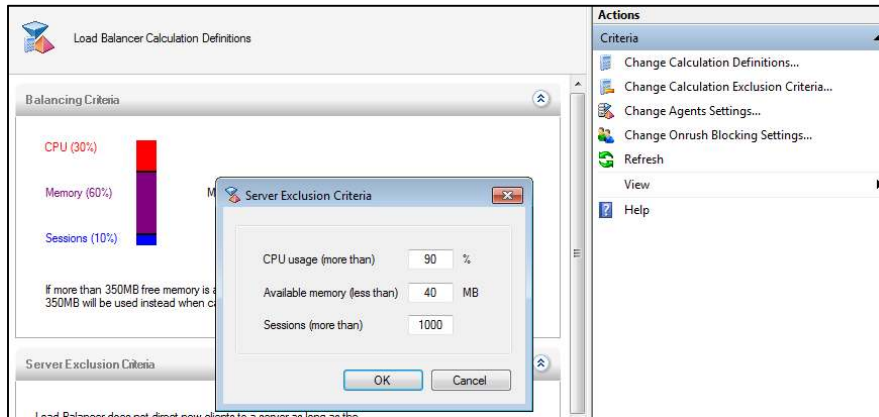
Configuring Server Exclusion Criteria

Select Configuration | Criteria | *Change Exclusion Criteria*.

Specify the *CPU usage* (in percentage) that when exceeded will disqualify the server from receiving user connections.

Specify the minimum *Available Memory* (in MB) that when reached will disqualify the server from receiving user connections.

Specify the *Concurrent Session count* that when exceeded will disqualify the server from receiving user connections.



Agent Sampling Settings

The Load Balancer Agent on each Terminal Server collects sampling data (CPU, Memory, or Number of Sessions) for transmission to the Load Balancer Server. An average of these samplings is calculated for the specified duration of the *Sampling Period*.

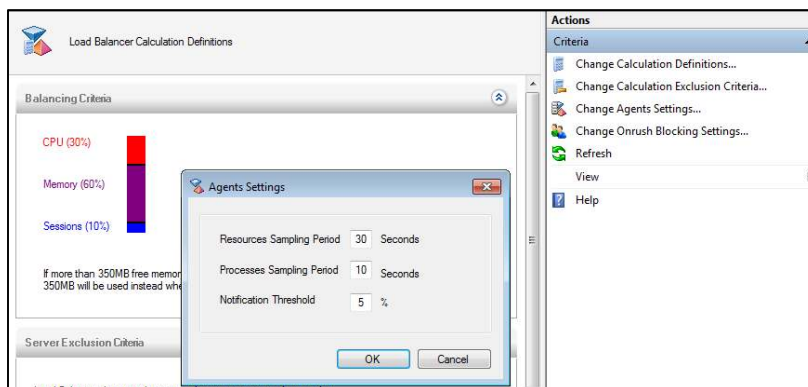
Configuring the Sampling Settings

Select Configuration | Criteria | *Change Agents Settings*. Specify the amount of time (in seconds) in for *sampling period* on which the average will be based on.

Notification Threshold

This is the percentage in the server's criteria that must change (between the previous and current sampling) before a notification is sent to the Load Balancer server. If there is a significant change in the Threshold percentage since the last sampling period, a notification is sent to the Load Balancer.

NOTE If no notification is sent within five minutes from a Terminal Server, the Load Balancer Server will classify it as unavailable.



14. DEPLOYING DESKTOPS WITH VDI

PowerTerm WebConnect DeskView is the built-in VDI connection broker for users to access remote desktops over PowerTerm WebConnect. With Presentation Virtualization, all users have access to applications and desktops on a multi-user operating system provided by a Microsoft Terminal Server. Desktop Virtualization is the concept of delivering applications and desktops from a dedicated (private) operating system hosted on virtual machines and physical machines. The connection broker grants each user access to his or her own desktop session. Each session is an isolated environment, so, if a failure should occur on one machine (physical or virtual) it will not affect any of the other machines. DeskView also provides the ability to create custom pools of desktops for flexible deployment possibilities.

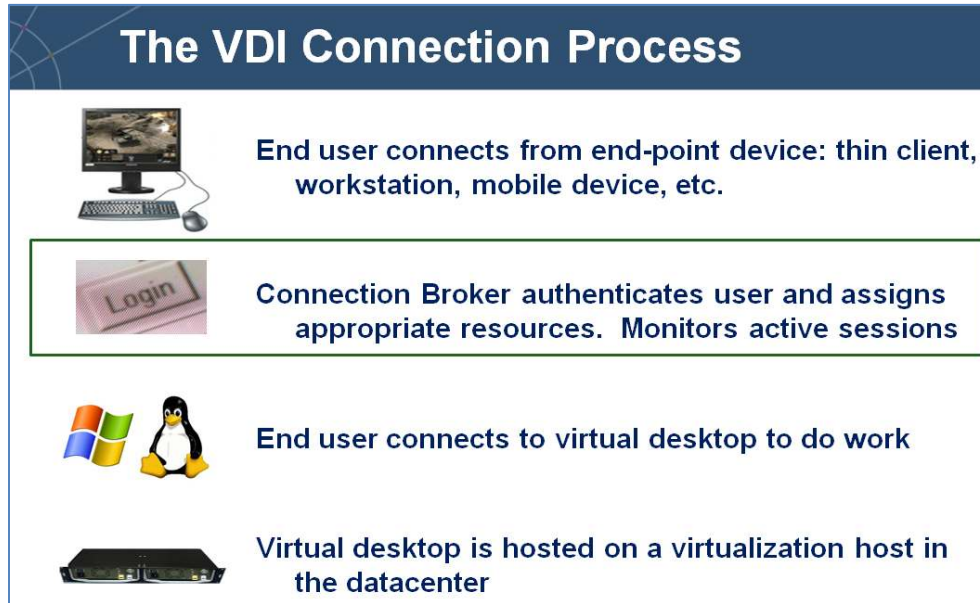
PowerTerm WebConnect DeskView consists of the following components:

- *PowerTerm WebConnect DeskView Server* is the connection broker service that interfaces between *PowerTerm WebConnect Server* and the servers hosting the desktops.
- *PowerTerm Connection Broker Administration Console* is the administrative interface for configuring PowerTerm WebConnect DeskView Server.
- *PowerTerm WebConnect Server* provide necessary functions for DeskView related to licensing, authentication, and publishing characteristics.

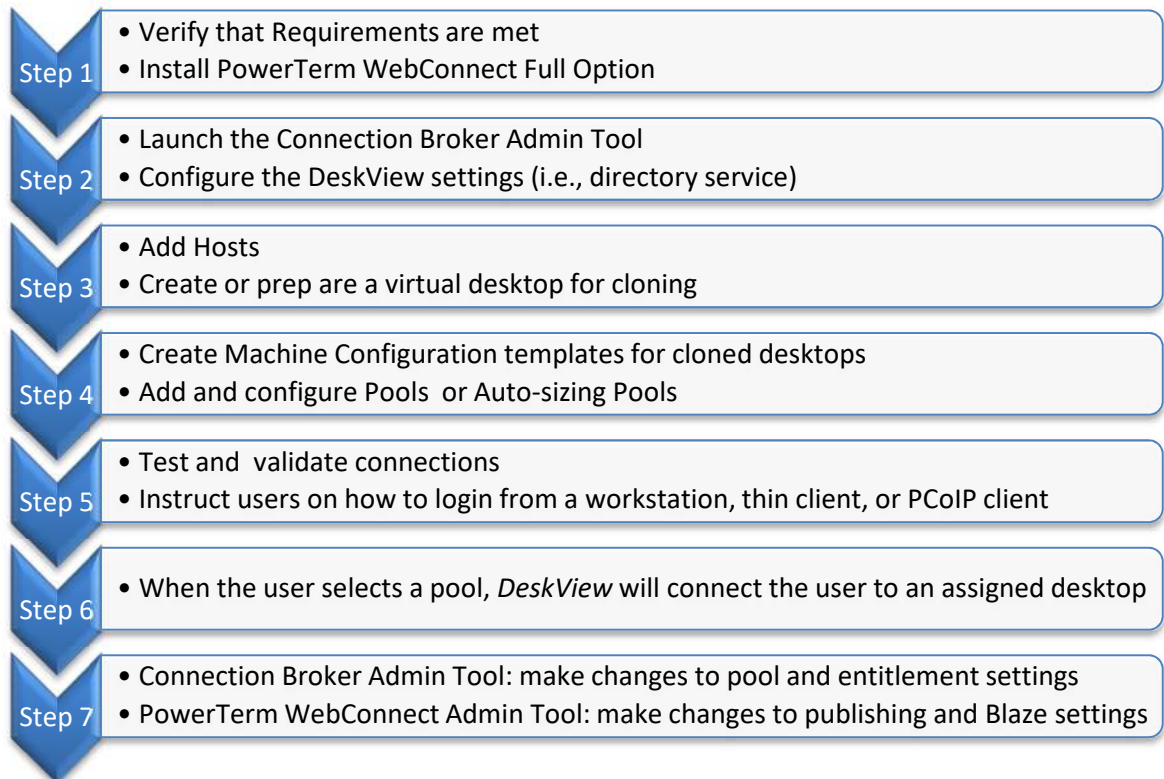
Definitions

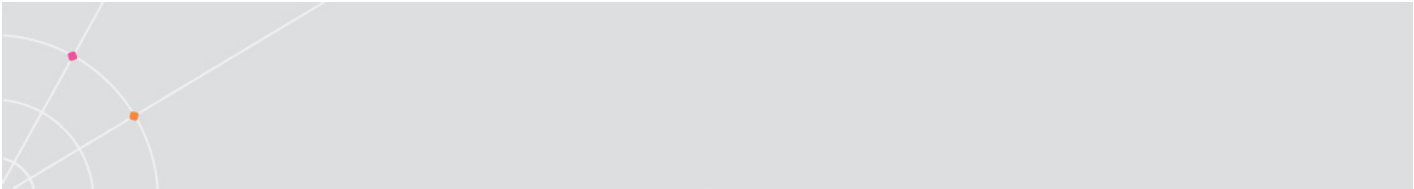
Pool	A collection of desktops with similar traits (i.e., similar applications installed on each, same OS, etc.).
DeskView	PowerTerm WebConnect’s built-in connection broker
Virtual Desktop	Any instance of a user workstation. This can be a VMWare virtual machine, Hyper-V virtual machine, Parallels Virtuozzo container, PCoIP desktop, etc.
Ericom Tools	An agent that is installed on each virtual or physical machine. It communicates with the DeskView server.
PCoIP	PC over IP protocol by Teradici

The VDI Connection Process



Getting Started with PowerTerm WebConnect





PowerTerm Connection Broker Administration Tool, is used to configure settings related to VDI and managed systems (including PCoIP devices). This console manages the PowerTerm WebConnect DeskView service. Use this console to manage functions related to user entitlements, virtual desktop configuration, and PCoIP device administration.

PowerTerm WebConnect Administration Tool, manages publishing of applications and desktops. Manual deployment of VDI pools may be performed using this tool.

Installation

Requirements

The server hosting DeskView and PowerTerm WebConnect must be running Windows 2003 or higher. 800 MB of free hard-disk space must be allocated to PowerTerm WebConnect Server and 256 KB of RAM for each active session

- Microsoft .NET Framework 4 Full edition must be installed on the PowerTerm WebConnect server.
- For Web Portal Access: Enable IIS role on the server
- The server's *Computer Browser* service must be running.
- For VDI: Connection and login information for desired hypervisors

Installation

PowerTerm WebConnect DeskView is automatically installed with the *Full Installation* option of the PowerTerm WebConnect installer.

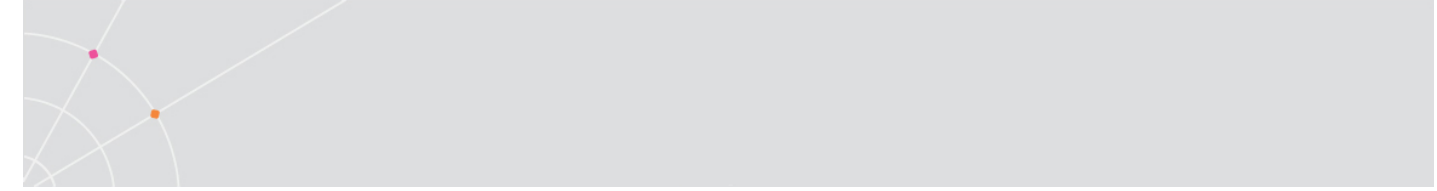
To install *DeskView* manually after PowerTerm WebConnect Server has already been installed, go to *<PowerTerm WebConnect Installation Folder>\WebConnect 5.X\AddOns\DeskView VDI* and run *DeskViewServerSetup.msi* and *DeskViewAdminSetup.msi*.

<p>NOTE The connection broker cannot be installed on an operating system acting as the hypervisor. For example, DeskView cannot be installed on the Windows 2008/2012 operating system running the Hyper-V role.</p>

Preparing Virtual Desktops

Gold Image

When starting off, create or prepare an existing desktop for use as the gold image template. This desktop will be used as the base for all future desktops (child desktops) and cannot be accessed by an end-user. Once a desktop is



set as the gold template it cannot be modified as this would risk corruption in all child desktops that are generated from it. The Gold image should be configured with all the necessary applications and settings that go into creating a standard workstation desktop in the organization. Here is a checklist of actions to consider when preparing the Gold Image:

- Install, configure, and update the operating system
- Install any desktop agents used by third-party software (i.e., Ericom Access Server, Ericom Tools, etc).
- Install any applications that go into the standard workstation image (i.e., anti-virus, software deployment tools, PowerTerm WebConnect RemoteView client, etc.)
- Configure firewalls to allow ports that will be used by the agents and installed applications.
 - DeskView's *Sysprep* feature uses port 21
 - Access Server 3.x (AccessNow/Blaze) port is 8080 by default
 - Blaze 2.x port is 3399
 - Ericom Tools uses 4045.
- Ensure that only one (virtual) network adapter is used in the virtual desktops. Having multiple adapters (i.e., a VPN adapter) may confuse virtual desktop agents that need to reference a local IP address.

Ericom AccessNow

The Ericom Access Server is required to enable HTML5 RDP access. The Access Server installer is found under the AddOns directory. Install this on each virtual desktop that is planning to host HTML5 sessions.

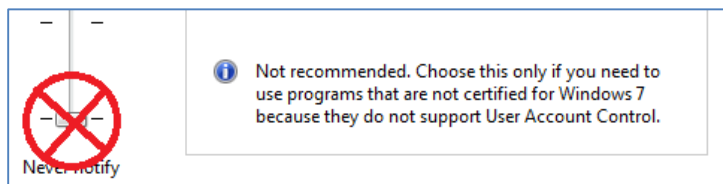
Ericom Blaze

The Ericom Access Server is required to enable Blaze RDP Acceleration. The Access Server installer is found under the AddOns directory. Install this on each virtual desktop that is planning to host Blaze sessions.

Ericom Tools for Windows

Ericom Tools (VmAgent) is an agent that is installed on each virtual or physical machine. It communicates with the DeskView server and relays important information about the machine's status. When using Free seating (user name authentication), Ericom Tools will pass the authenticated credentials to the target virtual desktop for provide single-sign on.

NOTE On Windows 7 desktops, in order for the SSO to operate properly, the desktop's UAC (User Account Control) cannot be set to *Never Notify*. Use any of the other three settings.



Once Ericom Tools is configured and running, use the Connection Broker Administration Console to verify that the Ericom Tools status is *Connected*. Once *Connected* the virtual machine will be available for user access.

NOTE Virtual machines must be added to a pool in the Connection Broker before it can be accessed by end-users.

Requirements

Operating Systems Supported: Windows XP and higher

Ericom Tools Installer Package Files: The latest Ericom Tools for Windows packages can be downloaded from the *AddOns* folder: <drive>\Program Files (x86)\Ericom Software\WebConnect 5.X\AddOns\DeskView VDI

- **32 bit** operating systems: EricomTools.MSI
- **64 bit** operating systems: EricomTools_64.MSI

NOTE Install the appropriate version of Ericom Tools based on your operating system. The x64 version of Ericom Tools must be used on x64 operating systems

Installation Instructions

Run the Ericom Tools MSI on the virtual desktop. Enter the address of the PowerTerm WebConnect DeskView server. Ericom Tools for Windows can also be deployed centrally from the Administration Console if the following conditions exist:

- The IP address of the virtual desktop is detected by DeskView
- The Domain administrator account configured under DeskView has access to install applications on the virtual desktop

Centralized Deployment

Ericom Tools can be deployed to any virtual desktop using the Connection Broker Administration Console. Right-click the desired virtual desktop and select *Install Ericom Tools*. Ericom Tools can only be deployed centrally if the IP address of the virtual desktop is recognized by the broker and the domain

administrator (configured under *Options | Network* tab) has rights to install applications on the local desktop.

HINT If the virtual desktop is not part of a Domain, the domain administrator may not have access to install applications.

Broker Discovery

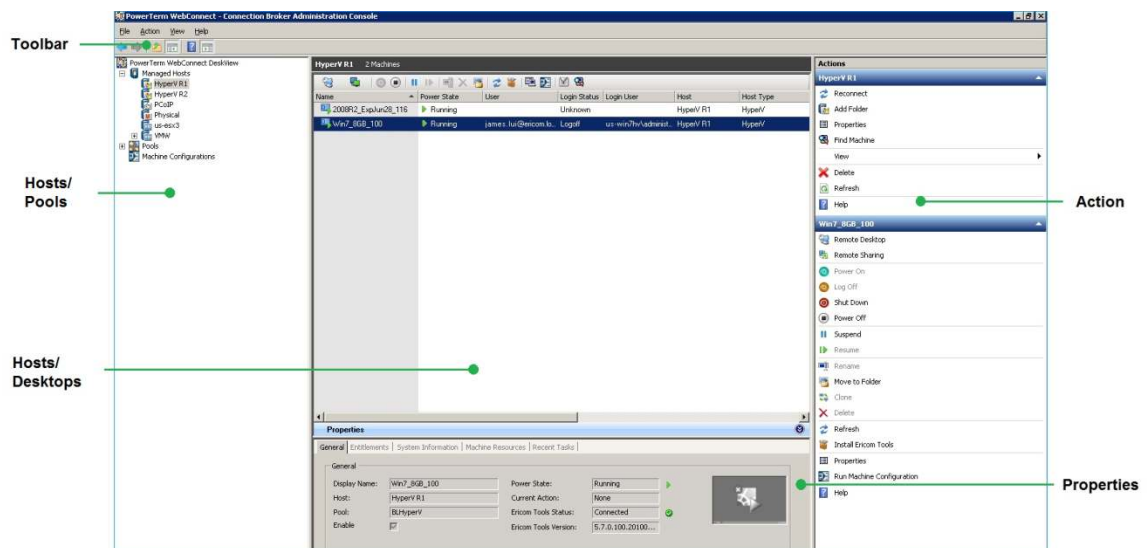
When Ericom Tools is first started, it initiates a discovery action for DeskView. The desktop running Ericom Tools must be using DHCP to use this feature. Ericom Tools performs the following discovery steps to determine the address of the Ericom broker:

- IP address if the *RegistryFirst* key is enabled (1) in the Registry
- DNS value: *ericom-broker*
- DNS-SRV value: *_ericom-broker*
- DNS value: *ws-broker* (only when PCoIP environment is verified)
- DNS-SRV value: *_pcoip-broker* (only when PCoIP environment is verified)
- IP address if the *RegistryFirst* key is disabled (0) in the Registry

Connection Broker Administration Tool

The DeskView Connect Broker Administration Console is an MMC snap-in module used to manage the connection broker settings.

Connection Broker Admin Console Panes



NOTE All objects under *Managed Hosts* and *Pools* will be listed alphabetically.

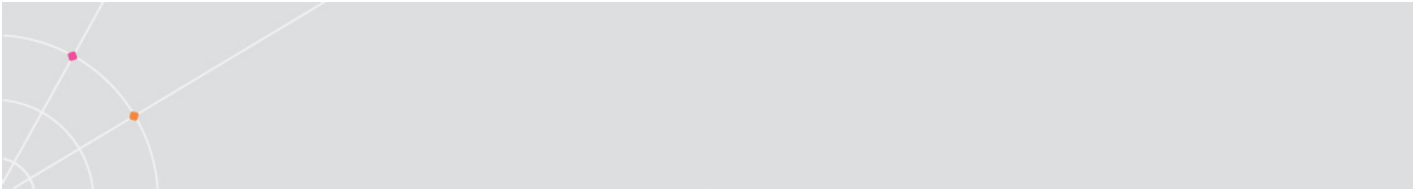
Pane	Description
Toolbar	Window pane functions
Hosts/Pools	Tree view of available hosts and pools
Hosts/Desktops	Detailed view of configured hosts and virtual desktops
Action	List of available actions for selected object
Properties	Displays <i>Properties</i> associated to the selected object

Hosts/Desktops Pane

Name	Power State	Ericom Tools	User	IP Address	Login Status	Login User
------	-------------	--------------	------	------------	--------------	------------

Right click on the Status bar to select settings to display

Column	Description
Name	The desktop's name
Unique Identifier	A unique ID assigned to the desktop
Power State	The status of the desktop's power state <i>Running</i> , desktop is active <i>Stopped</i> , desktop is currently in a stopped state <i>Paused</i> , desktop is currently in a suspended state <i>Missing</i> , desktop is not found on the host.
Ericom Tools	Displays status of Ericom Tools agent. <i>Running</i> , Tools are active <i>Disconnected</i> , Tools were previously connected, but is currently disconnected. <i>Unknown</i> , Tools never connected.
User	Active user of the desktop
IP Address	The desktop's IP address
DNS Name	The desktop's DNS address
Operating System	The desktop's operating system type <i>Unknown</i> , the information is not found
Login Status	Displays the desktop's user status. <i>Logout</i> , the user is logged out.



	<p><i>Connect/Disconnect</i>, the user is logged in and connected/disconnected.</p> <p>Only available when Ericom Tools is installed.</p>
Login User	<p>Last logged in user</p> <p>Only available when Ericom Tools are installed.</p>
Host	Displays the name given to the host.
Host Type	Displays the virtualization host type.
State	<p>Displays status of the desktop on the virtualization host</p> <p><i>Connected</i>, the desktop is found</p> <p><i>Disconnected</i>, the desktop is not found (may be deleted)</p>
MAC Address	MAC address of the desktop
Owners	Displays current owners of the desktop
Current Action	Displays any current actions that are applied on the desktop by DeskView
More...	Show dialog to configure the columns

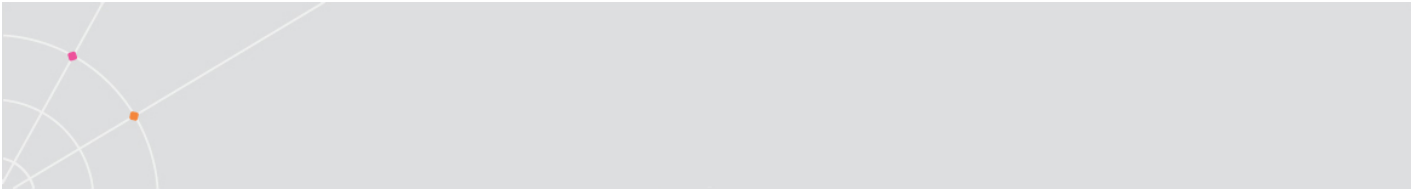
Properties Pane

Field	Description
General	Displays the desktop's details
Entitlements	Displays the users/MACs/computers that have be assigned to this desktop.
System Information	Displays the system details
Machine Resources	Displays the memory and CPU resources
Recent Tasks	Displays tasks applied to the selected object by DeskView

DeskView Server Options

To configure settings associated with DeskView Server, right click on *PowerTerm WebConnect DeskView* and select *Options*.

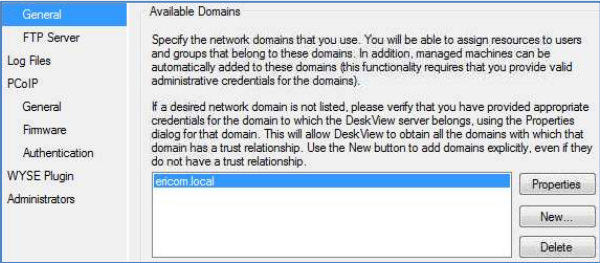
Tab	Description
General	Failover and Refresh Interval Settings.



Network	Configure domain administrators. Specify the network search range. Enable FTP server.
Log Files	Configure server logging criteria.
PCoIP	Configure PCoIP configuration for PCoIP enabled hosts.
WYSE Plugin	Enable and configure WYSE Plugin settings.
Administrators	Configure Administrators for DeskView

Configuring Directory Services in DeskView

Directory Services must be configured in DeskView to assign user and group objects to DeskView-managed desktops and pools. This is also required for PCoIP user/group assignments. Add desired directory services (domains) using the PTWC DeskView *Options | Network | General* dialog.



NOTE All VDI assignments are managed using the PTWC Connection Broker Administration Console, not the PTWC Administration Console

Ericom PowerTerm WebConnect DeskView uses Microsoft Negotiate to peek the security support provider.

[http://msdn.microsoft.com/en-us/library/ms721625\(v=VS.85\).aspx#_security_security_support_provider_gly](http://msdn.microsoft.com/en-us/library/ms721625(v=VS.85).aspx#_security_security_support_provider_gly)

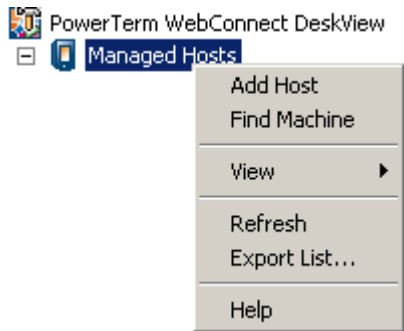
When PowerTerm WebConnect is running on the same domain that the LDAP server is running on, Microsoft Kerberos is used. In Kerberos (version 5) the password is not sent over network the network at all. See

[http://msdn.microsoft.com/en-us/library/aa378157\(v=VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa378157(v=VS.85).aspx) – this is the best security protocol on a Windows OS.

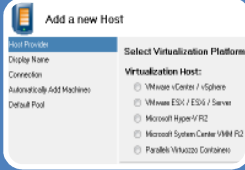
If the VDI server is not running on a system that belongs to the domain, NTLM or simple binding is used.

Managed Hosts

To add a VDI host for management by DeskView, right click on *Managed Hosts* and select *Add Host*.

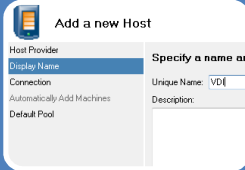


This will start a wizard to configure a new VDI host.



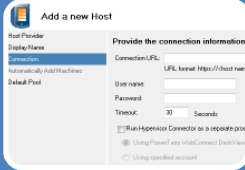
VDI Host Selection

- Select the type of host to be added



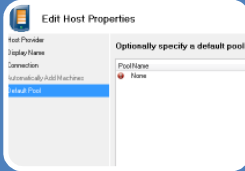
Host Description

- Enter a name for the host (see supported platforms)
- Enter a description for the host (optional)



Host Configuration

- Enter the connection parameters for the host
- Certain hosts require credentials to connect to them



Default Pool

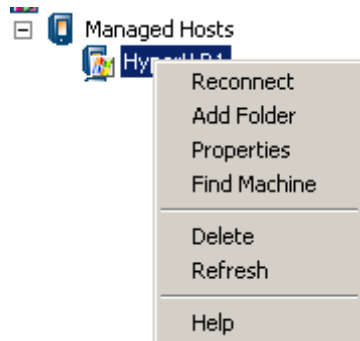
- Set a default pool if desired
- A Default Pool contains all machines of its Host

Supported Platforms	Configuration parameters
VMware ESX/ESXi	Web service address (<a href="https://<server>/sdk">https://<server>/sdk) Username/Password
VMware vCenter	Web service address (<a href="https://<server>/sdk">https://<server>/sdk)

	Username/Password
Parallels	<a href="https://<IP>:4646">https://<IP>:4646 Domain Username/Password Domain <i>Host-routed configuration is not supported</i>
Microsoft Hyper-V R2	DNS/IP of the Hyper-V machine Domain account that can access the host
Microsoft SCVMM	Server name or IP
XenServer	Server name or IP Root username/password
Oracle VM	Server's agent URL and Port (<a href="https://<IP>:8899">https://<IP>:8899) Oracle VM Oracle Agent username/password
Xen based hypervisors	Driver Transports Server Address Username/Password Port Path Extra Parameters (if any)
Enomaly	Web service address (<a href="http://<IP>:8080/">http://<IP>:8080/) Username/Password

Host Menu

Right-clicking on a Host will display a menu.



NOTE The Host menu may vary based on the type of host selected.

Menu item	Description
Properties	Opens the Host Properties
Reconnect	Reconnects to selected host
Add Folder	Creates a subfolder for the host - makes it easier to arrange virtual desktops with similar traits
Delete	Deletes the selected host
Refresh	Refreshes the selected host

Machine Properties

Virtual Machine/Desktop specific settings can be set from its *Properties* page. To access the Properties page, right click on the desired machine/desktop and select *Properties*.

General tab

Displays status information of the selected machine/desktop. Use this page to perform the following functions: change the assigned Pool of the machine, *Start, Stop, Suspend, Resume, edit Memo, and Enable*.

Entitlements

Displays ownership information of the selected machine/desktop. Use this page to perform the following functions: Remove current user assignment, *Add Users, Add Computer, Add PCoIP client, Add MAC Address* objects.

The *Alternative Machine* setting assigns an alternate virtual machine/desktop to be the failover desktop. If the primary machine/desktop is unavailable, users will be automatically redirected to the *Alternative Machine*. The machine/desktop specified as the *Alternative Machine* must be contained in a Pool, although the user requiring access does not need to be explicitly assigned to the Alternative Machine's pool. The feature is useful for PCoIP users who need a backup desktop in case of mechanical failure of their primary PCoIP host desktop.

When the primary host is down upon user connection, DeskView will try to start it with a wake-on-lan (magic) packet. If the machine is not active after 30 seconds, the *Alternative Machine* will be launched as the failover desktop.

System Information and Recent Tasks

Displays detailed information on the machines characteristics and past events.

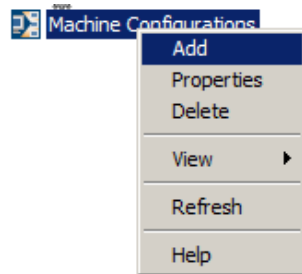
Machine Configuration

A *Machine Configuration* defines the parameters that will be used in the Sysprep process when a virtual desktop is cloned. This enables cloned desktops to be created with necessary characteristics and settings and start on the network without causing conflicts with existing desktops. Multiple *Machine Configurations* may be created to serve different purposes.

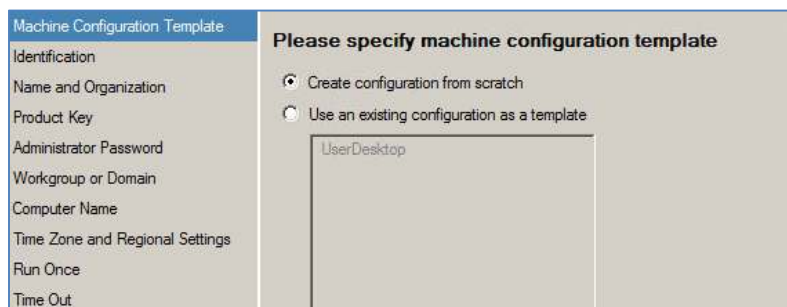
NOTE Ensure that Machine Configurations are only applied on desktops that are properly licensed and activated. Applying a Machine Configuration on an expired operating system will cause the Sysprep operation to fail.

Step 1: Starting the Machine Configuration Creation Process

Right click on Machine Configuration and select Add.



To create a new configuration, select *Create configuration from scratch*. A new configuration can also be created using the settings from an existing configuration.



Step 2: Set the identification parameters

Enter the Configuration Name and select the Windows operating system that will be used. Three operating systems are available: Windows XP, Windows 7, and Parallels Virtuozzo Container.

Machine Configuration Template	Please specify configuration name and description
Identification	
Name and Organization	The configuration name will be recorded as the Sysprep Identification String in the registry of the configured machines.
Product Key	Configuration Name: <input type="text" value="UserDesktop"/>
Administrator Password	Select the windows product that will be installed using this configuration.
Workgroup or Domain	Windows Product: <input type="text" value="Windows 7"/>
Computer Name	Description (optional)
Time Zone and Regional Settings	<input type="text" value="Parallels Virtuozzo Container"/>
Run Once	
Time Out	

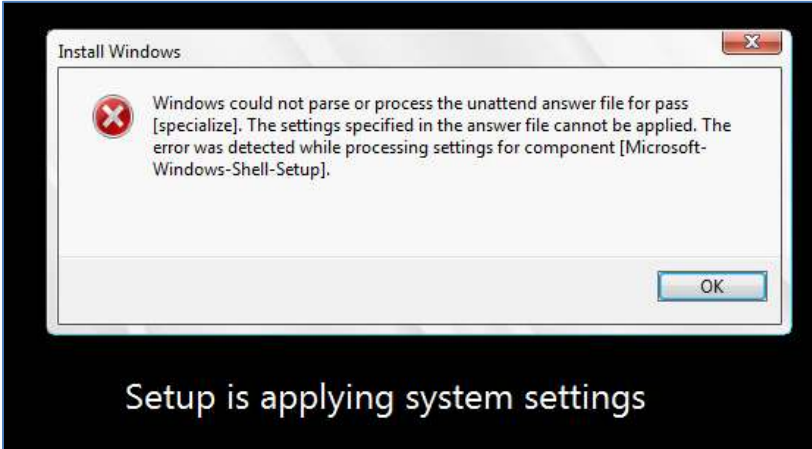
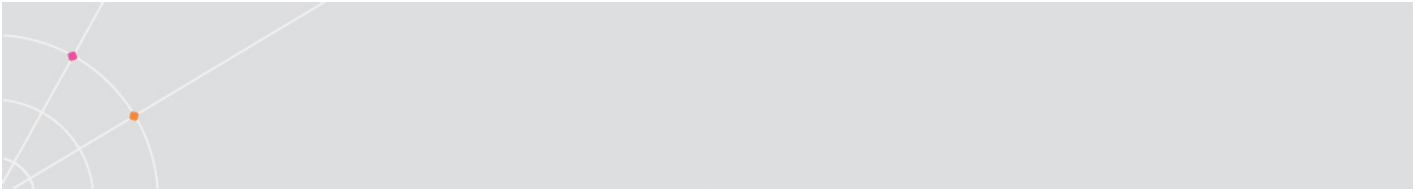
Step 3: Set the default name and organization

Machine Configuration Template	Please specify the registered owner's name and organization
Identification	
Name and Organization	Type the default name and organization you want to use.
Product Key	Owner: <input type="text" value="User"/>
Administrator Password	Organization: <input type="text" value="Your Company"/>
Workgroup or Domain	
Computer Name	
Time Zone and Regional Settings	
Run Once	
Time Out	

Step 4: Enter the Windows product key to be used for the clones

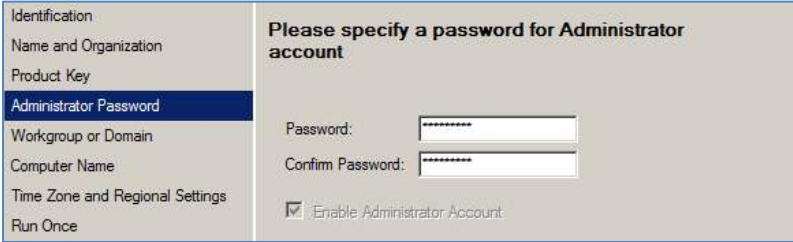
Machine Configuration Template	Please specify Product Key
Identification	
Name and Organization	Type the Product Key for the destination computers. You need a separate license for each copy of Microsoft Windows that you install.
Product Key	The Product Key you specify must match the Product Key provided to you by Microsoft Licensing, Inc. If an invalid Product Key is specified the configuration process will fail.
Administrator Password	<input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/> - <input type="text"/>
Workgroup or Domain	
Computer Name	
Time Zone and Regional Settings	
Run Once	
Time Out	

If the product key is invalid, this error may appear at the newly created VM's console:



Step 5: Enter the password for the Administrator account

Enter the current */ocal/* Administrator password used by the template desktop. This is used to login to the desktop to apply the Sysprep operation.



HINT The Administrator's password entered here should match that of the gold template VM.

Step 6: Join the desktop to a workgroup or domain



Step 7: Set the desktops computer name

Two options are available. Either use the hypervisor's name as part of the computer name or enter a custom string. The custom string can only be nine characters. The suffix of the computer name will consist of a dash and five digits. The Computer Name has a maximum of 15 characters.

Machine Configuration Template	<p>Please specify computer name</p> <p>This setting will be ignored and not used when applied to an auto-sizing pool. In that case, the auto-sizing pool name will always be used instead.</p> <p> <input type="radio"/> Use the hypervisor's machine name <input checked="" type="radio"/> Use the following computer name: </p> <p>desktop</p> <p>NOTE: In case multiple machines are created, the name will be prefixed with consecutive numbers, e.g. machine-00001 and machine-00002.</p>
Identification	
Name and Organization	
Product Key	
Administrator Password	
Workgroup or Domain	
Computer Name	
Time Zone and Regional Settings	
Run Once	
Time Out	

Step 8: Set the time zone for the desktop

Machine Configuration Template	<p>Please specify Time Zone and regional settings</p> <p>Select a time zone for the destination computer.</p> <p>Timezone: (UTC-05:00) Eastern Time (US & Canada)</p> <p>Select the Language for non-Unicode programs.</p> <p>Locale: English (United States)</p> <p>Select the language you would like menus and messages displayed in.</p> <p>Language: English (United States)</p> <p>Select the locale used for numbers, time, currency and dates.</p> <p>Locale: English (United States)</p> <p>Select the input locale.</p> <p>Locale: English (United States)</p>
Identification	
Name and Organization	
Product Key	
Administrator Password	
Workgroup or Domain	
Computer Name	
Time Zone and Regional Settings	
Run Once	
Time Out	

Step 9: Set the Run Once command

This is useful where additional commands need to be launched the first time Windows starts.

Machine Configuration Template	<p>Please specify Run Once command</p> <p>To automatically run a command the first time a user logs on, type the command in the following box, and then click Add.</p> <p>Command to add:</p> <p> <input type="text"/> Add </p> <p>Run these commands:</p> <p> <input type="text"/> Remove <input type="text"/> Move Up <input type="text"/> Move </p>
Identification	
Name and Organization	
Product Key	
Administrator Password	
Workgroup or Domain	
Computer Name	
Time Zone and Regional Settings	
Run Once	
Time Out	

Step 10: Set the Machine Configuration process timeout

The Machine Configuration process will stop after the specified amount of time has elapsed.

Machine Configuration Template

Identification

Name and Organization

Product Key

Administrator Password

Workgroup or Domain

Computer Name

Time Zone and Regional Settings

Run Once

Time Out

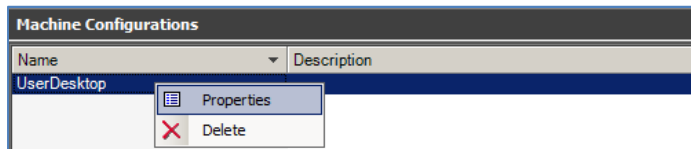
Please specify process time out

Time for the Machine Configuration to be done, if the process will not end at the specified time an error will occur

Time out (minutes): 30

Editing or Deleting a Machine Configuration

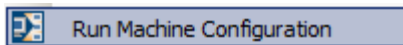
Right click on a *Machine Configuration* to edit its *Properties* or delete it.



NOTE A Machine must be a *Stopped* state before it can be deleted

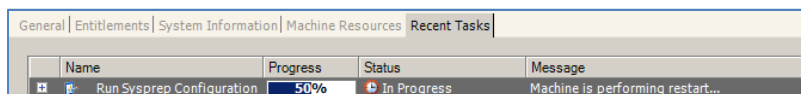
Applying a Machine Configuration to an existing Desktop

To apply a Machine Configuration to an existing Desktop, right click on the desired desktop and select *Machine Configuration*.



NOTE When applying a Machine Configuration, a Sysprep is performed to the desktop and certain characteristics are changed (i.e. Computer name). The local Administrator account password is also changed.

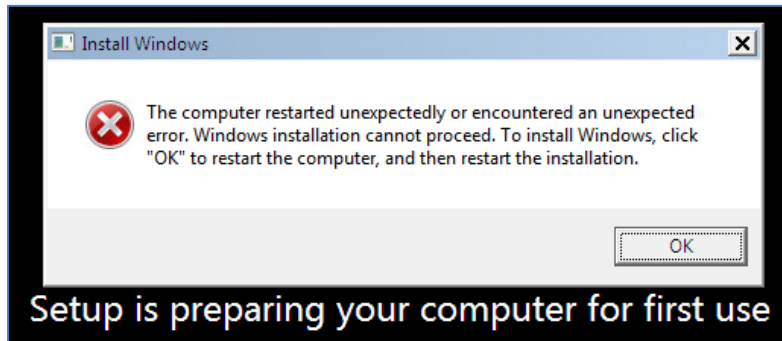
Select the desired Machine Configuration and continue. Monitor the progress under the Desktop's *Recent Tasks*.



During the Machine Configuration process, the desktop will reboot. The entire Sysprep process may take 5-10 minutes for each machine.

The newly created VM's preparation and Sysprep process can be using to the hypervisor's management tool and connecting to the console of the target desktop. The configuration process may stall if an error was encountered (i.e. invalid Product Key is entered by the Machine Configuration).

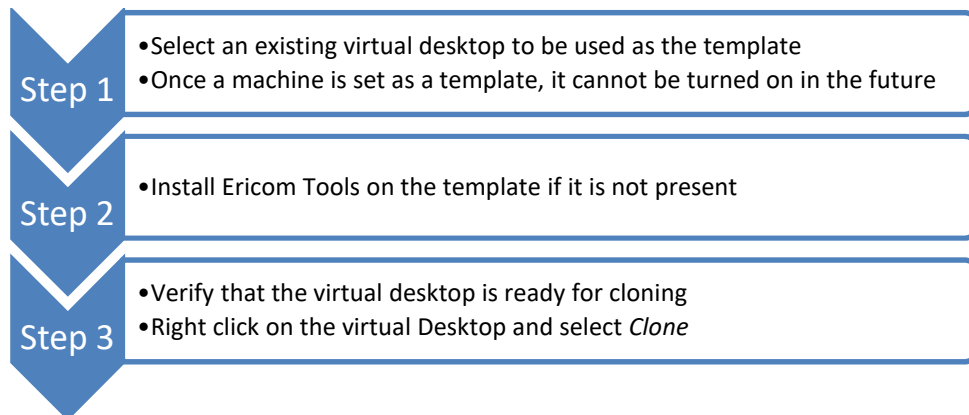
The VM may also reboot continuously if invalid data was received from Sysprep; the error below may appear. If this occurs, delete the VM and start over after verifying the *Machine Configuration* (Sysprep) data.



Virtual Desktop Cloning

PowerTerm WebConnect DeskView provides a simple interface to clone existing virtual machines. Standard cloning and linked cloning are supported.

NOTE Hardware based virtual desktops (i.e., PCoIP hosts) cannot be cloned



Preparation

- The gold template master generating linked clones *cannot* be altered once clones have been generated. Modifying the gold template will render all child clones invalid for use.
- When shutting down a VM in preparation for cloning, perform a *graceful* Windows Shut Down rather than Powering off the VM. The Windows error on boot up after an unexpected shut down will interrupt the *Sysprep* process.

NOTE The VLAN ID value will not be maintained when cloning virtual machines on Hyper-V.

Linked Cloning

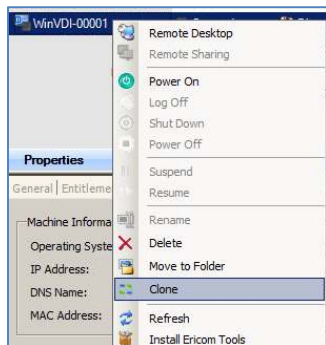
Linked cloning is supported with: VMware vCenter, VMware ESX, Microsoft SCVMM, Microsoft Hyper-V, and Parallels. All clones with Parallels and ESX are linked.

Cloning for Parallels does not execute sysprep on the container images. Ericom Tools (VmAgent) will receive a command to add the container to the domain. When selecting a sysprep configuration – DeskView will only take the domain information and the name of OS information from the sysprep configuration.

NOTE: When using linked clones with VMware vCenter it is not possible to use a vCenter template as the source image for cloning. Only standard cloning can use vCenter templates as the source image.

Step 1: Starting the Cloning process

Select the desktop that will be used as the template and make sure it is in the *Stopped* state. Right-click on the selected desktop and click on *Clone*.



Step 2: Set the parameters for the Clone

- Set the *Base Name*; this will be the prefix in the name for every cloned desktop.
- Set whether this clone operation will be to create a single clone or multiple clones.
- Set whether linked cloning will be used. This is on by default. Diff-Disks are used with Microsoft Hyper-V in this example.

General

Host

Datastores

OS Configuration

Specify name and number of clones

Please specify the base name for the clones:

WinVDI-clone

You can create one or more copies of a virtual machine. In case multiple machines are created, the base name will be prefixed with consecutive numbers, e.g. machine-00001 and machine-00002.

Please specify the number of clones you want to create:

Create a single clone

Create multiple clones

Number of clones to create: 1

Start numbering at: 1

Use Diff-Disks with Rapid Provision

HINT Running a large batch of multiple clones may be resource intensive on the virtualization platform so consider running these during off peak hours.

Step 3: Select the *datastore* where the clone will be saved to.

General

Host

Datastores

OS Configuration

Choose one or more datastores for the clone(s)

Datastore Name	Size(MB)	free Size(MB)	Type
C:	152484	4501	Local
E:	99	71	Local

Step 4: Select the Machine Configuration (optional)

General

Host

Datastores

OS Configuration

Please specify OS Configuration

Machine Configuration

Saved Setups:

UserDesktop

New...

Click *Finish* to begin the cloning process. Look under the *Recent Tasks* to monitor the progress of the clone creation.

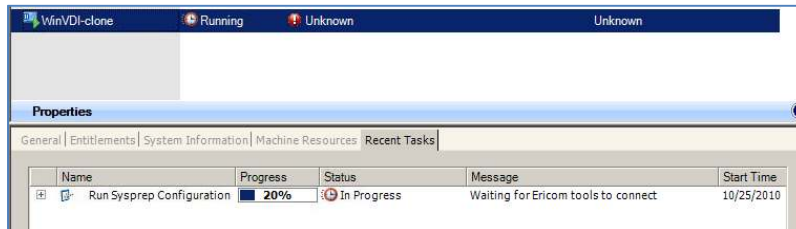
General | Entitlements | System Information | Machine Resources | **Recent Tasks**

Name	Progress	Status	Message	Start Time
Cloning	10%	Success		10/25/2010
Clone Creating		Success		10/25/2010
Stopping		Success		10/25/2010

Once the Clone creation is completed, the status will change to *Success*.

Name	Progress	Status	Message	Start Time
Cloning		Success		10/25/20
Clone Creating		Success		10/25/20
Clone LinkClone Disk		Success		10/25/20
Clone Reconfiguring		Success		10/25/20
Clone Reconfiguring		Success		10/25/20

The application of the Machine Configuration may take a few minutes to complete. The preparation duration will depend on the amount of resources available to the new desktop.



NOTE The preparation and Sysprep process can be monitored in more detail by using to the hypervisor’s management tool and connecting to the console of the target desktop. The configuration process may have halted if an error was encountered (i.e. invalid Product Key is entered by the Machine Configuration).

Remote Sharing

Any active machine running Ericom Tools is eligible for *Remote Sharing* support. *Remote Sharing* enables an administrator to connect and shadow a desktop being managed by the Connection Broker Administration Console. To start a Remote Sharing session, right click on the desired desktop and select *Remote Sharing*.



Only desktops that are *Powered On* and have Ericom Tools *Connected* are available for Remote Sharing.

Logging

All DeskView Administration console functions are logged in the file named *DeskViewAdmin.log*. The DeskViewAdmin.log file is created under the *Ericom* folder in the user profile.

On Windows 7, 8, 2008, 2012, and higher the path will be:

`<drive letter>:\Users\<user name>\AppData\Local\Ericom\DeskViewAdmin`

On Windows XP and 2003 the path will be:

<drive letter>:\Documents and Settings\\Local Settings\Application Data\Ericom\DeskViewAdmin

All DeskView Server service operations are logged in the file named *DeskViewServer.log*. The *DeskViewServer.log* is created under the *DeskViewServer* folder where PowerTerm WebConnect is installed.

PowerTerm WebConnect Administration Console and VDI

PowerTerm WebConnect Administration Console manages a few important functions for VDI sessions.

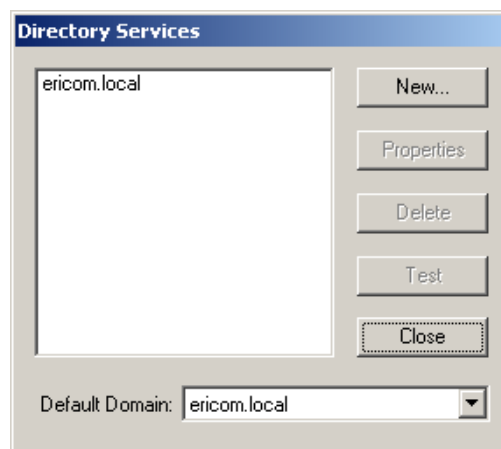
- NOTE When PowerTerm WebConnect Administration Console is launched for the first time, the *Connection* dialog is displayed with the user "Administrator". No password is required to login, but this should be changed immediately.
- NOTE By default, the Administration Console will deny connection attempts from any system other than the local machine. This is set by the *Access Limit Mode*.

Change publishing configuration for RDP sessions

Virtual desktops can be accessed via the Application Zone and Application Portal. To change the desktop characteristics (i.e., color depth) modify the *Properties* of the desktop pool under the *Connections* list. All published properties are configured here (i.e., sub-folders, icons, redirection settings, etc.)

Enable Directory Services

In order for PowerTerm WebConnect to work with Active Directory or LDAP based users and groups, use the Administration Console to link to the Directory Server. Go to *Server | Directory Services* and verify that desired domains are on the list. Click New to add additional domains.





Using Pools

Pools provide a method to arrange devices into logical groups for assignment to users. For example, virtual desktops hosting a sensitive HR application can be added to the HR Pool. The HR Pool is then assigned only to an "HR" group in the Active Directory. Only users part of the "HR" group will have access to the HR specific desktops when logging into PowerTerm WebConnect.

Creating a Pool

Step 1: Creating a Pool

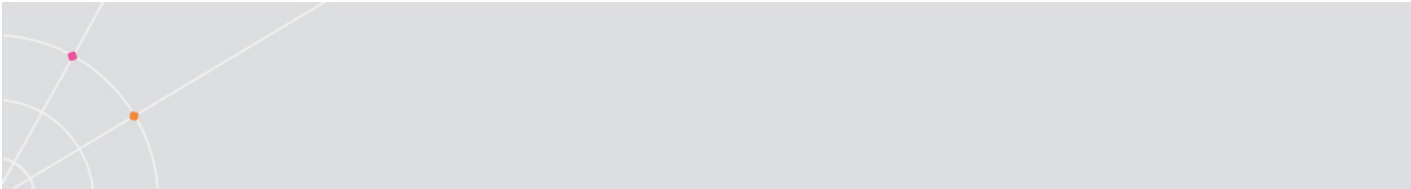
To create a pool, right-click *Pools* and select *Create Pool*. The *Create Pool* wizard will start. Enter a *Pool name* (this is displayed to end-users) and a description (optional).

STOP The name of Pool is restricted by length (max 9) and by valid characters (no spaces, no underscores...).

NOTE Auto-sizing pool names must not be longer than 15 character and must not contains some special characters. For example, if a pool is named SCVMMpool, new virtual machines will be named SCVMMPool_00001, SCVMMPool_00002. Since a Windows Computer name is limited to 15 characters, nine characters are allocated for the name and six are allocated to the counter value.

Step 2: Specify the Assignment Type and Duration

- *Static*, resources in this pool are manually mapped to users, computers, or PCoIP clients. Each device in the pool must be allocated to a user or device in order for it to be accessed.
- *Dynamic*, a free resource in the pool will be assigned to the user when the pool is launched. This enables a fixed group of virtual desktops to be shared among users. Enable *Auto-sizing Pools* if desired (see section on Auto-sizing Pools)
- *Persistent*, once the user receives an available resource, it will be mapped permanently to the user until the Administrator resets the assignment.
- *Non-Persistent*, the assigned resource is locked during use, but will be available to the next user once the current user logs off.
- Users can be allowed to connect to more than one virtual desktop within a pool.



Step 3: Configure Entitlements

Click *Add* to browse your directory service for desired users and groups that will have access to this pool. Click *Add PCoIP Client* to assign a specific PCoIP Client to have access to the pool.

Step 4: User Privileges

This setting will assign configured owners (from *Entitlements*) to the virtual machine's local *Power Users* or *Administrators* group. Select *Do not add* to bypass this setting.

Step 5: Availability

Hours marked in blue are times where virtual desktops in the pool may be accessed. To deny access, select the desired hour(s) and click the white box next to *Deny* *Deny*. Selected boxes will turn white.

To allow access, select the desired hour(s) and click the blue box next to *Grant* *Grant*. Selected boxes will turn blue.

Step 6: Not in use state

DeskView can stop or suspend machines that are not in use to make better use of server resources. This feature is not available for all host platforms (i.e., managed machines).

NOTE The time it takes to connect a user to a stopped or suspended machine will be longer as the user will have to wait for the virtual machine to power on. Enter a value greater than 0 for *Machines in Started state* to ensure that an active machine is always available.

Step 7: Logoff/Disconnect Event

Similar to the *Not in use state*, a *Logoff* event will stop or suspend a virtual machine when the user logs off. DeskView can also logoff the user from a virtual desktop if the user has been idle for a set period of time. To set the idle timeout check *The guest account will log off* box and set the *Idle Time*.

Perform the following action when user session is idle


The guest user account will log off

Idle Time (in minutes) 15

Check the *Suspend the machine on disconnect* checkbox to suspend the virtual machine when a user disconnects from the virtual desktop (RDP disconnect is different than a log off – the session remains active for a period of time).

Suspend the Machine on disconnect (*)

Step 8: Add Machines

Finally, assign which virtual machines will be a member of the pool. To add virtual machines, select (highlight) desired machines from the lower list and press the *Add*  button.



To remove machines from the pool, select (highlight) desired machines from the upper list and press the *Remove*  button.

Click *Finish* to complete the pool creation process.

Please specify machines belonging to the pool

Belonged Machines

Machine Name	Host	Path	Operation System
us-desktop2	HyperV R2	HyperV R2	Unknown

Available Machines

Hosts [All] Path [All] Name contains

Machine Name	Host	Path	Operation System	Current Pool
Tech Desktop 1	HyperV R2	HyperV R2	Microsoft Windo...	
us-desktop3	HyperV R2	HyperV R2	Unknown	

NOTE All machines of the same pool should have very similar characteristics, or be identical, to maintain a consistent user experience.

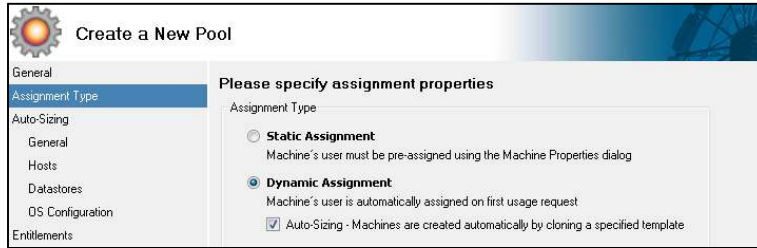
Auto Resizing Pools

Auto Resizing pools will ensure that enough machines are running at any given time. Virtual machines that are generated using an auto-sizing pool will be linked clones if the hypervisor supports it.

NOTE Hardware based virtual desktops (e.g., PCoIP hosts) cannot be members of an Auto Resizing Pool. Certain virtualization platforms (e.g. VMware ESX) may also not support auto-sizing pools.

Configuring an Auto Resizing Pool

During the Pool creation process, the *Auto Sizing* option can be enabled by selecting the checkbox.



Step 1

- Select the template to be used for new desktops
- Determine the pool specifications

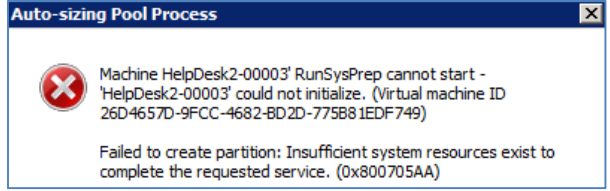
Step 2

- Specify the datastore on the host where new desktops will be stored

Step 3

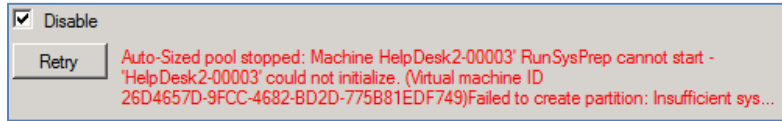
- Select the desktop configuration to be used
- Specify how machine machines to create in parallel

If there are insufficient resources on the virtualization host to clone additional desktops, an error similar to the following will be displayed:

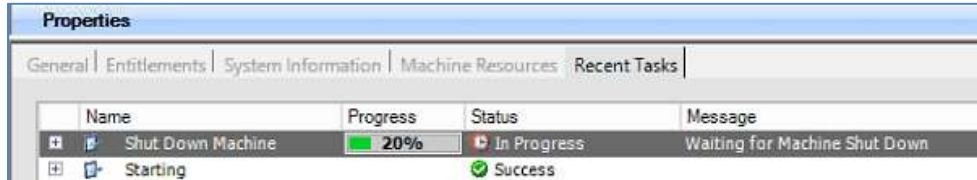


Additional resources may be freed up by stopping running virtual desktops or deleting files that are no longer needed on the virtualization host (i.e., unused desktops).

When an auto-resizing pool process fails, the pool will be disabled. Once enough resources are available on the virtualization host, go to the pool's *Properties* to enable it. Click on the *General* tab and uncheck *Disable* and click *Retry* to restart the auto-resizing process. Click *OK* to *Continue*. Monitor the desktop creation status under the *Host's | Machines* pane.



When configuring the Auto-sizing Pool, point it to the template VM while the VM is still running. The Auto-cloning process will automatically shut down the VM in preparation for cloning.



NOTE It is recommended to use a VM that is not domain-joined

Virtual Desktop Assignment Options

A virtual desktop may be assigned to one or more owners. Only owners in the Entitlements list can access the machine. There are two layers of security for virtual desktops: pool level and object level (higher precedence). If there are no entitled owners listed under the object, the desktop is accessible by the owners of the pool.

Fixed Seating: Assign a MAC address as Owner

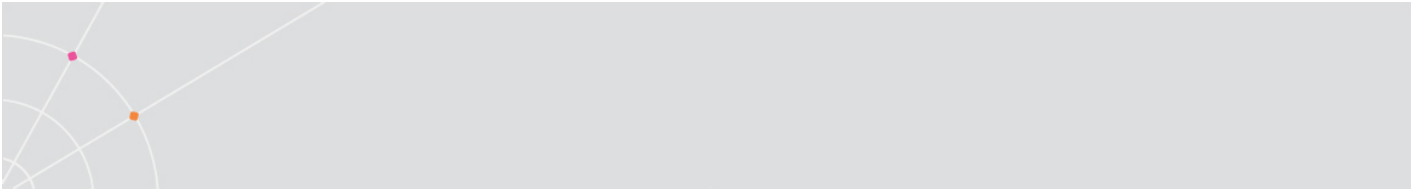
The MAC address of selected computers/devices may be assigned directly to a virtual desktop. This allows a “fixed seating” association where the virtual desktop may be accessed only from predetermined locations. More than one client device may be assigned to any virtual desktop.

- Right click the desktop and select Properties.
- Select the Entitlements tab.
- Click Add MAC Address and enter the MAC address of the client machine to assign.

Fixed Seating: Assign a DNS Name as Owner

The DNS Name of selected computers/devices may be assigned directly to a virtual desktop. This allows a “fixed seating” association where the virtual desktop may be accessed only from predetermined locations. More than one client device may be assigned to any virtual desktop.

- Right click the desktop and select Properties.
- Select the Entitlements tab.

- 
- Click Add DNS Name and enter the DNS name of the client machine to assign.

Free Seating: Assign a Directory Service object as Owner

Selected users and groups based on a directory service may be assigned directly to the virtual desktop. This allows a “free seating” association where the desktop may be accessed only by assigned users from *any* location. More than one user or group may be assigned to any virtual desktop.

- Right click the desktop and select Properties.
- Select the Entitlements tab.
- Click Add Users and enter the name of the directory service object to assign.

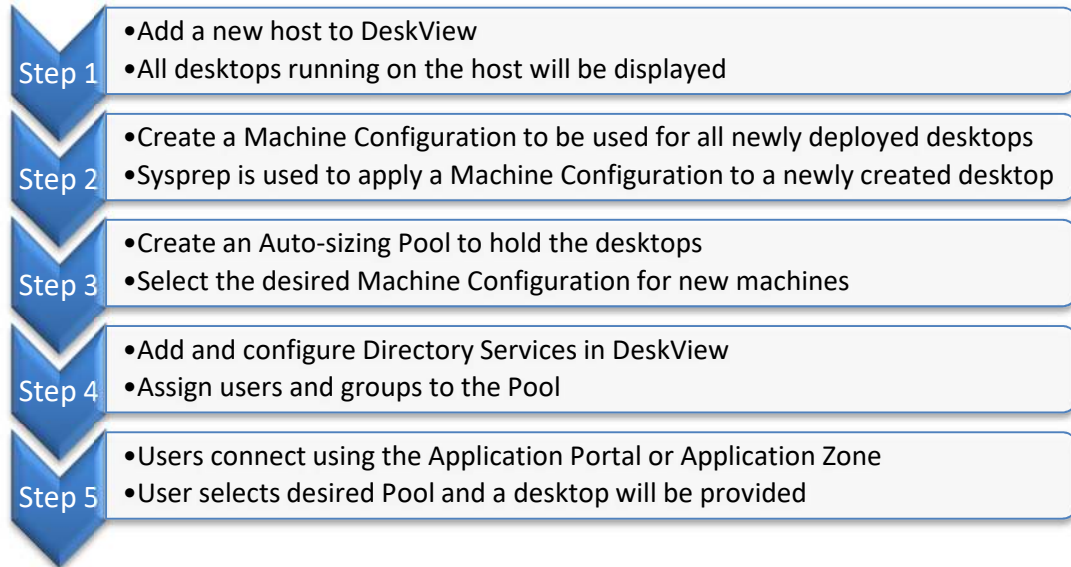
Creating a Simple VDI Implementation

DeskView is designed to help administrators implement a VDI environment easily without high costs or complexity. This section explains how to implement a VDI environment with basic components.

Requirements

- VDI Server(s) running a desktop hosting platform: VMware ESXi, Microsoft Hyper-V R2, or Parallels Virtuozzo
- Server to run PowerTerm WebConnect
- Virtual Desktops configured for deployment and ready for cloning. Ericom Tools must be installed on the desktop to be used as the template.

VDI in 5 Steps

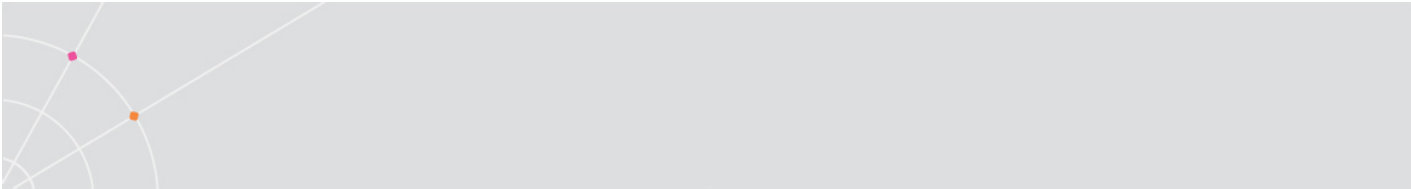


In this sample implementation, DeskView is the only management platform required to configure a fully functional VDI environment,

- No additional costly management tools are required
- Virtual desktops are centrally brokered. DeskView provides the following functions:
 - Automatically create new machines when needed
 - Assign desktops on a temporary or permanent basis
 - Suspend or power off machines when not in use
 - Restrict access to Pools to only certain hours of the day
- Additional hosts can be easily added in DeskView to increase scalability of virtual desktops.

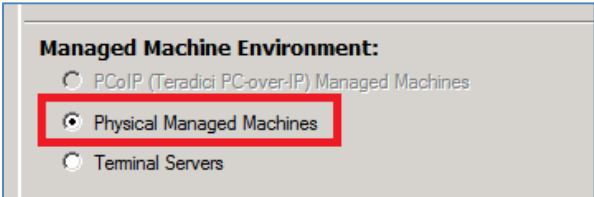
Creating a Remote PC Access Solution

Use DeskView to build a secure remote PC access solution. Physical PC's can be represented as virtual desktops in DeskView. As users connect to PowerTerm WebConnect, only allowed desktop pools will be displayed. As the user selects a desired pool, DeskView will connect to user to the destination PC for secured remote access.



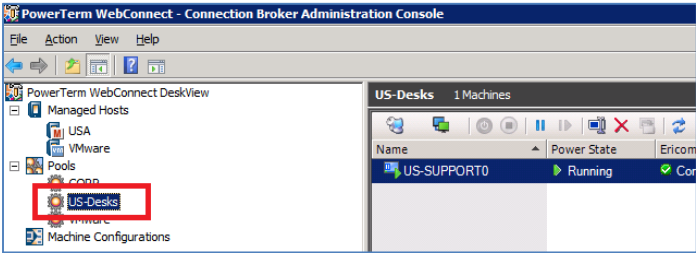
- Step 1**
 - Add a *Managed Physical* host to DeskView using the *Add Host* wizard
 - Add physical desktops and clients to the host
- Step 2**
 - Create Pools to hold the desktops.
- Step 3**
 - Add and configure Directory Services in DeskView
 - Assign devices, users, and/or groups to the Pool
- Step 4**
 - Install Ericom Tools
- Step 5**
 - Users can also connect using Application Portal or Application Zone

Step 1 – Add a Physical Machine Environment

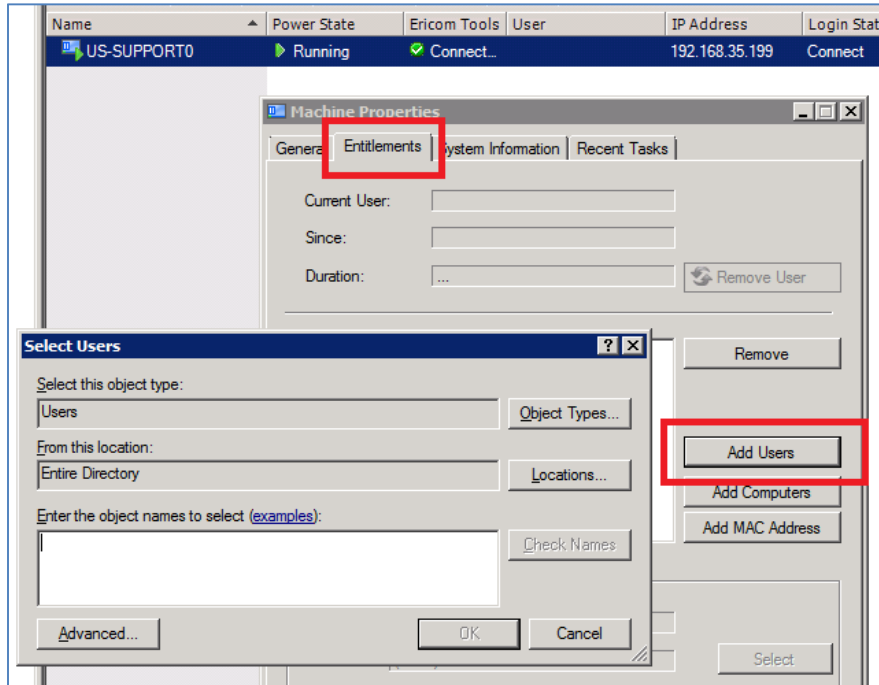


Step 2 – Create a Pool to hold the physical workstations

All physical desktops that will be assigned must be in a pool.

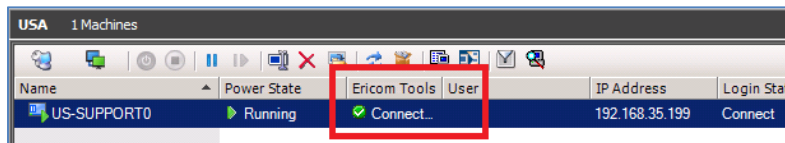


Step 3 – Assign the desired owner(s) to the desktop or pool



Step 4 – Install Ericom Tools

Install Ericom Tools for provide tighter integration between the broker server and the desktop.



Step 5 – Ready for access

Once the desktop is configured and available in the broker, it is ready for access from the Application Zone, Application Portal, or AccessToGo clients.

Creating an Enomaly Cloud

Use DeskView to build a secure cloud computing solution. Virtual desktops can be deployed in the cloud using Enomaly and DeskView. As users connect to PowerTerm WebConnect, only allowed desktop pools from the Enomaly cloud will be displayed.

When adding Enomaly to DeskView, do *not* use the Admin Enomaly user to add the managed host. Use the "customer" user (or member of the



"customers" group only). Add a managed host for every Enomaly user (customer) that will be used in DeskView.

CASE If there are five Enomaly users of the type "customers" on one Enomaly host, add a managed host in DeskView *for each* one of the five (each managed host must contain the username/password of its Enomaly user).

Once the host is added and configured, DeskView will have access to all the virtual desktops of the respective Enomaly "customer" account, and will be able to publish them to Active Directory users and groups.

NOTE When setting the entitlements of a pool or a virtual desktop using DeskView, the administrator should use the Active Directory users and groups; not Enomaly user accounts.

When creating a new virtual desktop on the Enomaly host, the administrator must ensure that it is assigned to only one Enomaly user account.

Enomaly ECP 3.5 and 3.5.1 are supported. If 3.5 is being used, contact Ericom for a required patch to support Auto-sizing Pools.

Connecting from WYSE ThinOS

DeskView supports connections from WYSE ThinOS devices (models S10, R10L, V10LE, etc). This enables ThinOS thin client to connect to VDI and Terminal Servers using PowerTerm WebConnect.

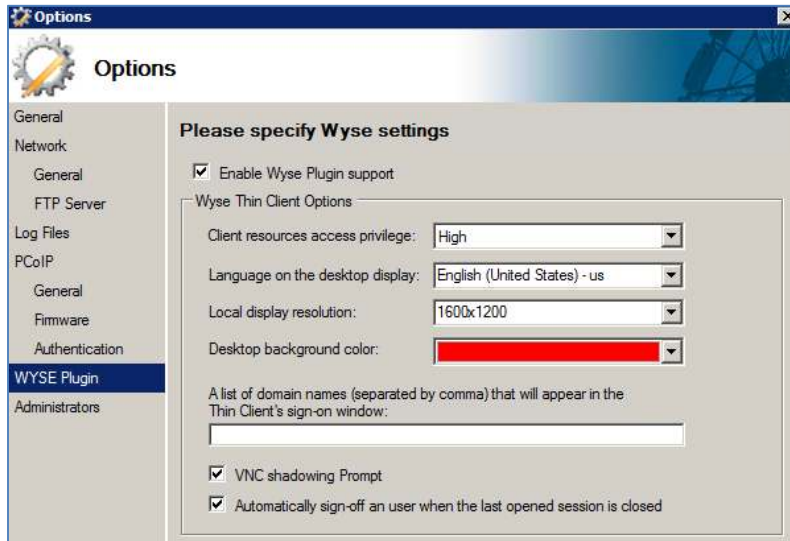
Enable WYSE Plugin Support

Open the *Connection Broker Administration Console* and right click on *DeskView*. Go to *Properties | Options | WYSE Plugin* configuration.

Check the *Enable WYSE Plugin* box

Set the parameters that will be passed to the WYSE ThinOS device:

- Language
- Display resolution on the ThinOS device
- Background color
- Domains that will be available on the ThinOS device



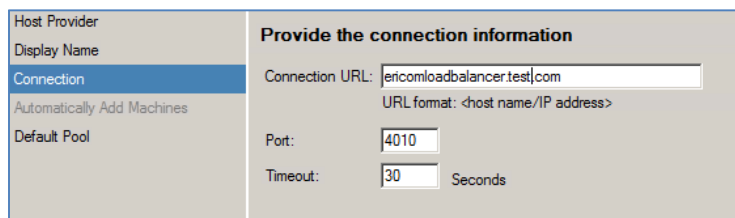
Configuring Full Desktop Terminal Server Sessions

Ericom DeskView and the Load Balancer can be used in conjunction to serve Terminal Server sessions to WYSE ThinOS devices. Seamless applications are not supported. To add a Terminal Server Connection, perform the following:

- Add a new host and select *Terminal Servers*



- At the *Display Name*, enter a name for the connection. This is displayed to the end-users.
- At the *Connection URL*, enter the address of the Ericom Load Balancer



- At the *Default Pool* dialog, create a new default pool for the host. This will also be added to the Server Administrator Console. Configure publishing related settings (i.e., color depth) using the Server Admin Console.

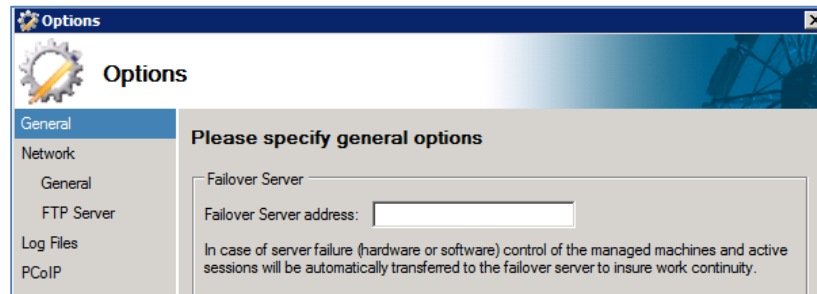
- Right click on the newly created pool and go to *Properties | Entitlements* to assign desired users and groups. Assigned users will now be able to access this connection.

DeskView Failover

Failover is a feature where if one PowerTerm WebConnect Server fails, another will take its place. This configuration ensures that there is high availability to the resources being managed by PowerTerm WebConnect DeskView. Two servers will be required: one will be assigned as the Primary and one as the Failover.

To begin, configure the Primary WebConnect Server Connection Broker settings:

- Login to the Connection Broker Admin Console
- Navigate to the Server's *Options*
- Enter the address for the **Failover Server**

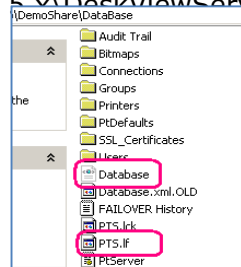


- Add a Managed Host. This will be used to verify that the failover mode is working

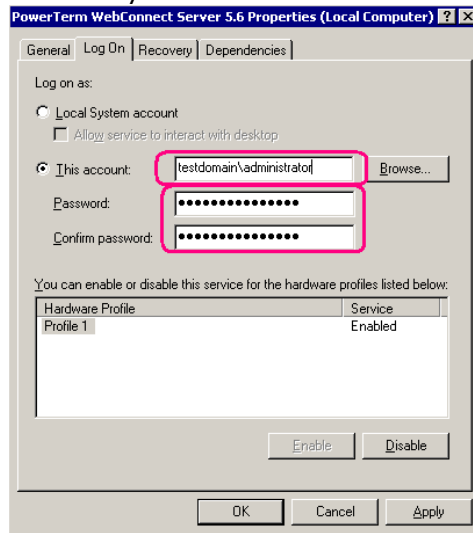


- Stop the PowerTerm WebConnect **Server** Service. The PowerTerm DeskView (VDI) service is *managed by the Server Service*, do not manage it independently.
- Configure the PowerTerm WebConnect server in a failover configuration.
- Create a network share that will be accessible from the Ericom server (it is recommended to place the share folder on highly available storage with redundant network connections).
- Copy the Primary server's *Database* and *Downloads* folder to the share
- Copy the **PTS.LF** file from the Primary server's *bin* directory to the shared *Database* directory (default: \Program Files\Ericom Software\WebConnect 5.x\bin)

- Copy the **Database.XML** file from the Primary server's *DeskViewServer* directory to the shared *Database* directory (default: \Program Files\Ericom Software\WebConnect 5.x\DeskViewServer)



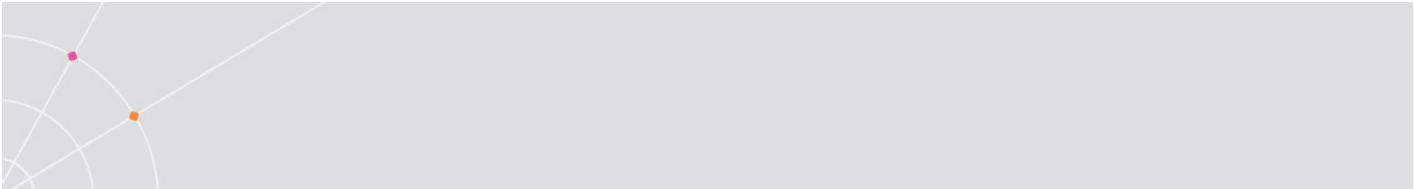
- The PowerTerm WebConnect services must be able to reach the share. This may require that the PowerTerm services run with elevated privileges.
- To configure this, go to each service's properties and enter the necessary credentials



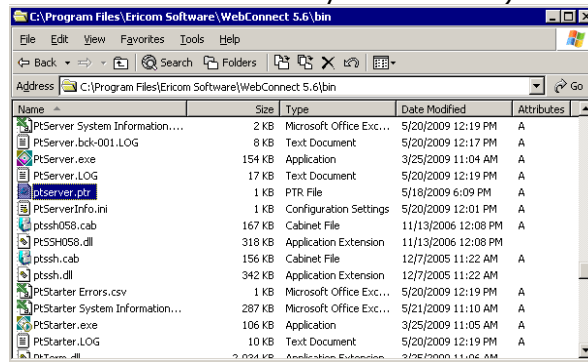
- Perform this for the following services:
 - PowerTerm WebConnect DeskView Server
 - PowerTerm WebConnect Server
 - PowerTerm WebConnect Server Starter

6) In the Primary's server's bin directory, create a text file named **PtServer.ptr**

- In this file, enter the path to the PtServer.ini file
\\<servername>\<share_path>\database\ptserver.ini
- Backup the existing Database.XML file on the Primary server and remove it from the DeskViewServer directory



- Restart the Primary Ericom PowerTerm WebConnect server
- Login to the Connection Broker Admin Tool
- If the previously configured host is visible, the broker is operating with the shared configuration file
- Failover configuration can also be verified in the DeskViewServer.log file, search for an entry that appears similar to:
5/21/2009 11:03:33 AM: Thread #:6 LoadDataBase():
Checking Database version: \\<server-name>/<share_path>/database/Database.xml
- On the **Failover** server's bin directory create the a **PtServer.ptr** file with the path to the shared **PtServer.ini** (the PTR file will be the same as the Primary server's file)



- Repeat Step #5 if necessary
- Restart the Failover Ericom PowerTerm WebConnect server
 - To verify that the Failover server is ready search for the following lines in the Failover server's **PtServer.log**:

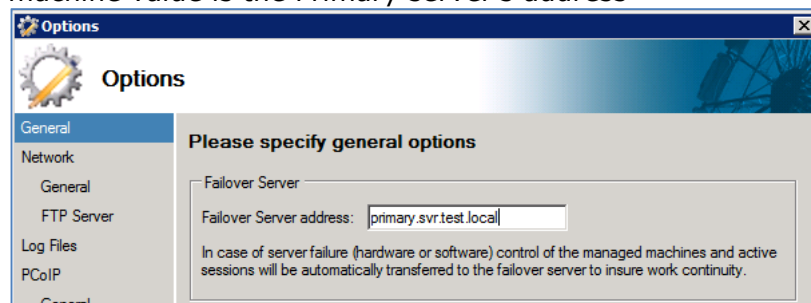
```
09/05/21 11:18:02.322 |          6e0 | FAILOVER: Failover synchronization
initiated.
09/05/21 11:18:12.664 |          6e0 | FAILOVER: The current active server is
US-VDIDEMO.1368, activated at 09/05/21 11:03:28
09/05/21 11:18:12.711 |          6e0 | FAILOVER: Waiting to get the control
on FAILOVER
```

- Administrators will be *unable* to login to the failover Connection Broker Admin console while the Failover server is in standby mode.
- When the Primary server becomes unavailable, the failover server will come online and update all listed desktop devices with its address
 - To test this, disconnect the network to the Primary server

- **Note:** Stopping the PowerTerm WebConnect Server service on the primary server will force the failover server to become the Primary Server
- The Failover transition takes approximately 2-4 minutes
 - During this time the broker services will not be available
- Once the Failover server is active, the administrator will be able to log in to the Connection Broker Admin Console
 - To verify that the Connection Broker is in failover mode, open DeskViewServer.log file and verify the database source. It will appear as:

```
5/21/2009 4:23:28 PM: Thread #:5      LoadDataBase( ): Checking
Database version: \\<server-name>/<share-
path>/database/Database.xml
```

- Under the Failover server's *Options*, verify that the Failover machine value is the Primary server's address



- When the Primary server is re-enabled, it will **regain** control of the managed desktops and Ericom Tools. The DeskView service will be stopped on the Failover server as it returns to Standby mode.

Using the Built-In FTP Server

The DeskView Server includes an FTP server. This is used to push updates to managed desktops, such as PCoIP firmware, Sysprep configuration, and Ericom Tools. For PCoIP firmware deployment, place the desired firmware files in the FTP root folder.

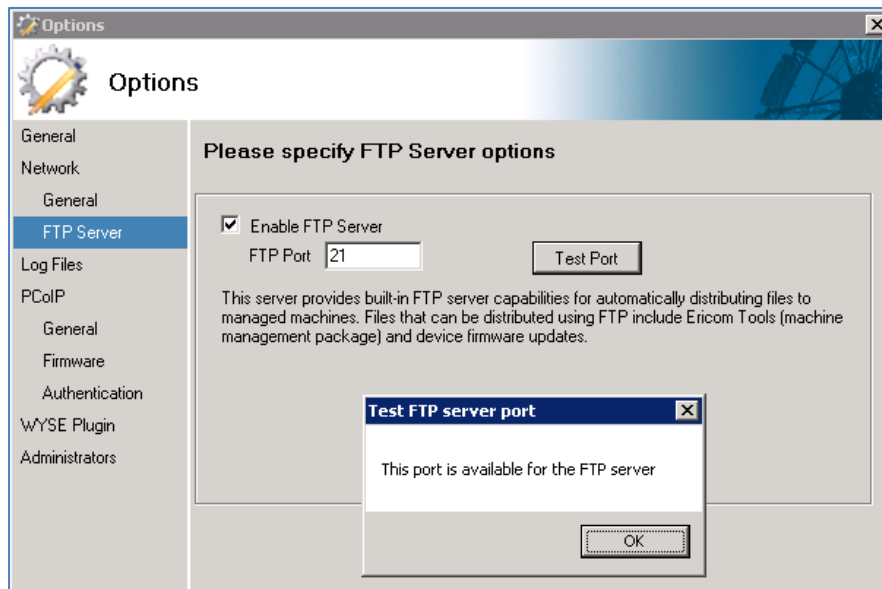
The FTP Server uses the following path as its root directory:

```
<drive letter>:\Program Files (x86)\Ericom Software\WebConnect
x.y\DeskViewServer\ftproot
```

By default, the FTP server uses port 21.

NOTE If PowerTerm WebConnect is installed on a server already running an FTP server on port 21, there will be a port conflict.

To disable the FTP server, or change the port value that it is using, go to the DeskView Admin console and open *Options* menu. Click on the *FTP server* to adjust the settings. To check if a certain port value is available, enter it and click on the *Test Port* button. If a dialog message appears confirming that the port is available, then this value may be used to host the FTP server.

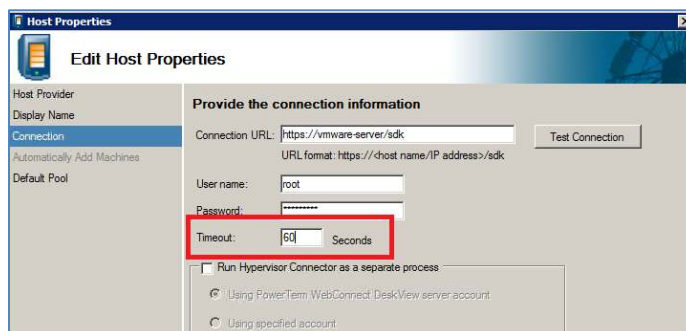


Troubleshooting

Desktops showing Power State as Missing

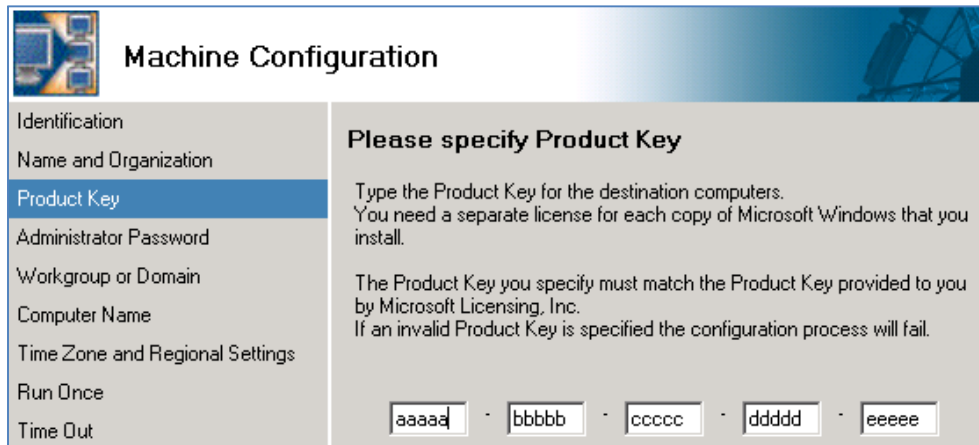
If all machines under the host start showing *Power State* as **Missing**, the connection to the host could be timing out. To prevent timeouts try extending the *Timeout* period.

Resolution: go to the Host's *Properties* and increase the *Timeout* setting from 30 seconds to **60** and reconnect DeskView to the host.



Machine Configuration Failing – VM keeps rebooting

If the virtual machine keeps restarting after applying a Machine Configuration, it is likely that the product key is invalid. Please verify that the Windows product key is valid.



Machine Configuration

Identification
Name and Organization
Product Key
Administrator Password
Workgroup or Domain
Computer Name
Time Zone and Regional Settings
Run Once
Time Out

Please specify Product Key

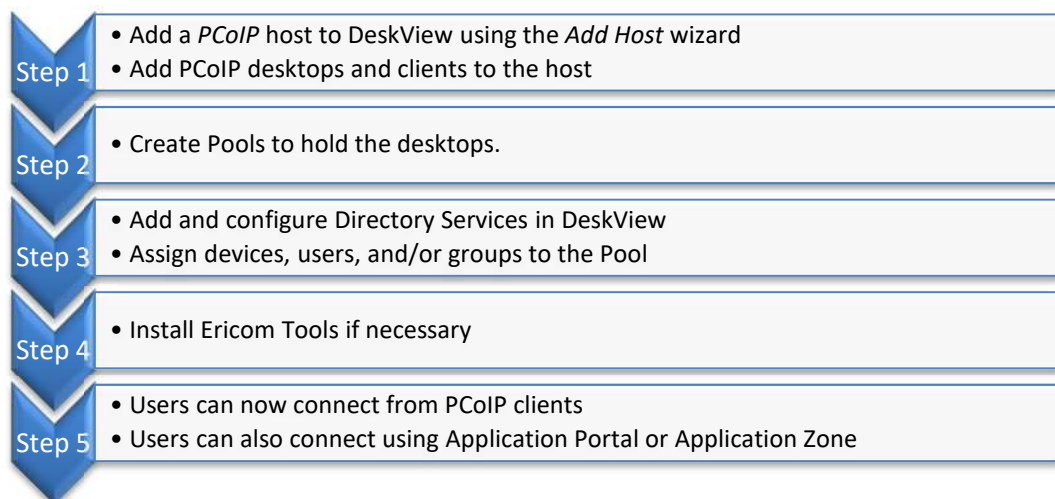
Type the Product Key for the destination computers.
You need a separate license for each copy of Microsoft Windows that you install.

The Product Key you specify must match the Product Key provided to you by Microsoft Licensing, Inc.
If an invalid Product Key is specified the configuration process will fail.

aaaaa - bbbbb - ccccc - ddddd - eeeee

15. CREATING A PC-OVER-IP BROKER

PowerTerm WebConnect DeskView is a connection broker to manage access between PCoIP Portals (clients) and hosts.



NOTE PCoIP devices can only be managed by one connection broker (also known as a CMS). If you have multiple PCoIP brokers running on the network, make sure that a PCoIP device does not appear in more than one broker.

Step 1: Adding PCoIP clients and hosts

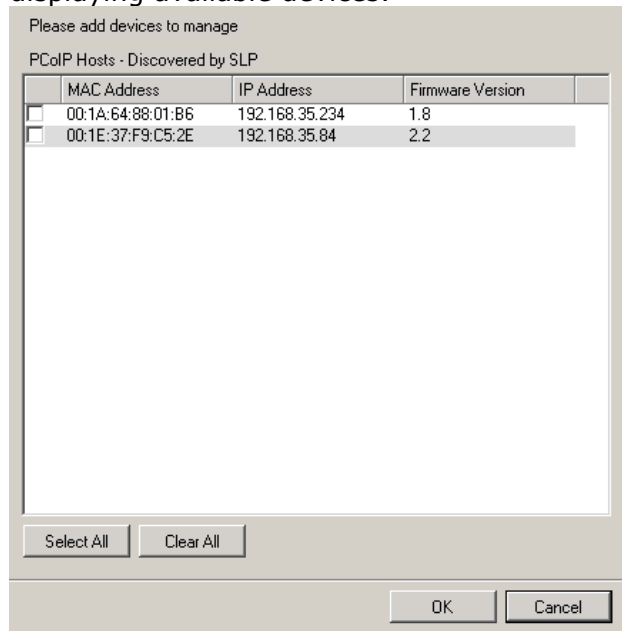
Right-click *Managed Hosts* and select *Add Host*, the *Add a New Host* wizard will appear. Specify *PCo-IP Managed Machines* as the *Host Provider* and click *Next*.

Enter a *Display Name* and a description (optional). Click *Next*. The Display Name is a reference label used in the Connection Broker Administration Console and will not be displayed to end-users.

Specify a *Default Pool* if desired (optional). A Default Pool allocates all devices of the host into one pool. Devices within a host linked to a Default Pool cannot be assigned to any other pools. This can be changed later under the host's *Properties*. Click *Finished* and the new *Host* will be added.

The PCoIP host will initially be empty. To populate devices in the host list, use the built-in SLP Discovery feature. Right-click the *PCoIP* host and select *Discovery | Find PCoIP Hosts/Clients*. The *PCoIP Devices* dialog appears

displaying available devices.



Select the hosts/clients to be added and click *OK*. The devices will appear under the *PCoIP Host/Client* list.

NOTE SLP-based discovery is not designed for multi-subnet environments. For multi-subnet support use *DNS-SRV* based Discovery. Information on this may be found in the Teradici user guide. When *DNS-SRV* based discovery is used, devices will automatically appear in the *PCoIP* host list. Manual configuration is not required in the Ericom Connection Broker.

Step 2: Using Pools to deploy desktops

Pools are used to arrange PCoIP devices into logical groups. To access resources, end-users simply connect from a PCoIP client or login to PowerTerm WebConnect from a workstation. The dynamic assignment feature of DeskView allows a group of users to share a common group of devices. For example, if there are 100 agents in a call center, but only 10 users are active at any time, assign the 100 users to a pool of 10 devices. This feature eliminates the need to manage mappings for every user.

Static assignment of PCoIP clients to hosts

PCoIP clients may be statically assigned to hosts. Static assignment maps PCoIP clients directly to PCoIP hosts. More than one client can be assigned to a host. Perform the following to create static assignments.

- Right-click the desired machine (host) and select *Properties*.
- Select the Entitlements tab.

- Click *Add PCoIP Client* to select a client to assign to the host.
- Select the desired client and press *Select*.
- Click *OK*. The Owner will be assigned.

When a user connects from an assigned PCoIP client, it will connect to the host as mapped in the Connection Broker.

NOTE The PCoIP host must be allocated in a static pool in order to accept static connections from PCoIP clients.

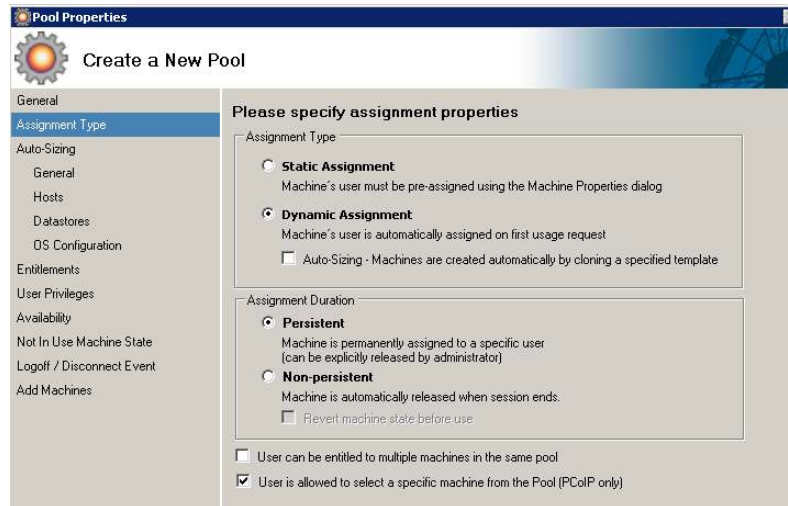
Username access without using Ericom Tools

For scenarios where Ericom Tools cannot be installed on the PCoIP host, username access (free seating) is still supported. Go to the DeskView Options | PCoIP | General. *Check PCoIP hosts do not contain Ericom Tools.*

NOTE When Ericom Tools is not running on the PCoIP host, the host will not be available for RDP access via PowerTerm WebConnect.

Selecting a PCoIP desktops in a Pool

A PCoIP pool can be configured such that the user can select a specific PCoIP host within the pool. To configure this, use the pool's *Assignment Type* property page and check the feature to enable machine selection (*User is allowed to select a specific machine*). When the user selects the Pool, a list of PCoIP hosts contained in the pool will be displayed for user selection.



Step 3: Assign hosts and pools to users and groups

Assign desktops and pools to users and devices. Determine if *Fixed* or *Free* seating should be used.

Fixed seating connections (PCoIP client is mapped directly to a PCoIP host) will mirror the PCoIP host exactly. System POST and BIOS information is accessible when using Fixed seating assignments. This method can also be useful for troubleshooting.

Free seating connections (users/groups are mapped to PCoIP hosts and pools) will only connect users to PCoIP hosts where the operating system is ready. In most cases, this method is more secure and reliable because the end user will not have access to POST/BIOS information and will only connect to a PCoIP desktop that is ready for use.

Step 4: Ericom Tools

Ericom Tools relay important information about the machine back to the PowerTerm WebConnect server. It is recommended to install Ericom Tools (but not required) in each virtual or physical machine that will be managed by PowerTerm WebConnect. The Ericom Tools installer (vmagent.msi) is located on the PowerTerm WebConnect server in *<PowerTerm WebConnect installation folder>\AddOns\DeskView VDI folder* (default installation folder is C:\Program Files\Ericom Software\WebConnect 5.x).

Step 5: Connecting to the PCoIP Host Desktop

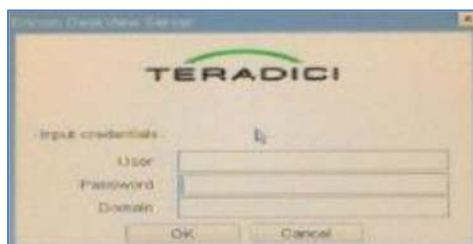
Once PowerTerm DeskView has been configured, users can connect using their PCoIP clients (also known as portals).

Static Mapped PCoIP Clients

If the PCoIP client is configured for Static mapping, only a Connect button will appear. When the user clicks *Connect*, the PCoIP client will be connected to the PCoIP host as assigned in DeskView.

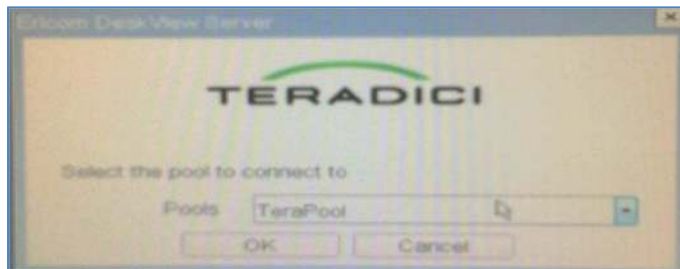
Dynamic Mapped PCoIP Clients

If the PCoIP client does not have a static mapping assigned, a username login dialog will appear:



A user must enter a username/password/domain to login. The username must be located within one of *Domains configured under PowerTerm WebConnect "Directory Services"*. When the user is authenticated, one of the following will happen:

- If the entered credentials are invalid, the login will be denied and the prompt will reappear.
- If the user only has access to one desktop, the PCoIP client will be connected automatically to the PCoIP host desktop.
- If the user has access to more than one pool, a list of pools will be displayed. Once the user selects the desired Pool, a connection will be made to a machine within the selected pool.



HINT If you see a “No Machines are available” error check the following:

- Verify that PCoIP Host operating system is not logged in by another user.
- Verify that Ericom Tools is installed on the PCoIP Host.
- Verify that *CurrentOwner* is empty, or is assigned correctly

Application Zone and Application Portal

PCoIP desktops may also be accessed via Application Zone or Application Portal. When a user logs into Application Zone or Application Portal and has access to a PCoIP device, an icon will be displayed. Double click a desired resource to launch it. Application Zone and Application Portal provides the user access to PCoIP hosts from non-PCoIP devices. The following protocols are supported: RDP, Blaze Accelerated RDP, and AccessNow HTML5 RDP.

NOTE When selecting a PCoIP pool from the Application Zone or Portal – RDP/Blaze/AccessNow will be used as the protocol. PCoIP is only available when both the client and host device supports PCoIP.

Administering PCoIP Devices

PowerTerm WebConnect DeskView provides management functions for PCoIP devices. To access the PCoIP management features, right-click on PowerTerm WebConnect DeskView and select *Options* and then click *PCoIP*. PCoIP devices communicate to PowerTerm WebConnect DeskView (also known as the PCoIP CMS) over port 50000.

General

SLP Discovery

Check *Enable SLP Auto-Discovery* to use SLP to find all available PCoIP devices on the network (subnet). SLP cannot traverse subnets.

To perform a manual SLP search, click *Find all PCoIP Hosts* or *PCoIP Clients*.

NOTE Only PCoIP devices that are not registered with DeskView will be listed in the search results.



The screenshot shows the 'SLP Discovery' configuration panel. It includes a checkbox for 'Enable SLP Auto-Discovery', a numeric input field for 'Auto discovery interval (in hours)' set to 0, and two buttons: 'Find all PCoIP Hosts' and 'Find all PCoIP Clients'.

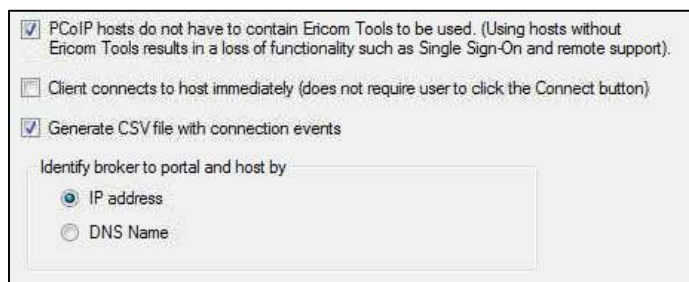
Security

PowerTerm WebConnect DeskView can force all PCoIP devices to use a predetermined password for firmware access. Enter a value for *Browser Password* to set the password for all devices. Pushing one firmware password secures all managed devices with a consistent password and saves time in setting the password manually at each device.

Additional Functions

Ericom Tools is not required for PCoIP connections, although certain functionality will be lost. To ignore the presence of Ericom Tools, *check PCoIP hosts do not have to contain Ericom Tools*.

The client can be configured to automatically connect to an assigned host and bypass the *Connect* button. This is useful for kiosk stations where the client device should always be displaying the desktop of the host.



The screenshot shows the PCoIP configuration panel with the following options:

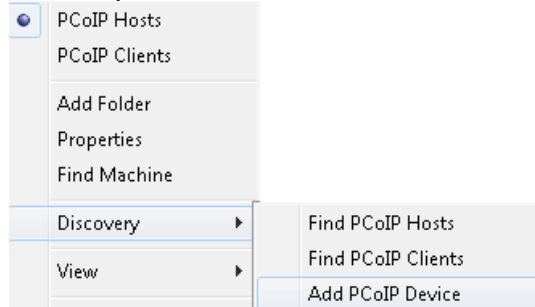
- PCoIP hosts do not have to contain Ericom Tools to be used. (Using hosts without Ericom Tools results in a loss of functionality such as Single Sign-On and remote support).
- Client connects to host immediately (does not require user to click the Connect button)
- Generate CSV file with connection events
- Identify broker to portal and host by:
 - IP address
 - DNS Name

Allow Connections to host only via broker will block any PCoIP portal from connecting to a PCoIP host without using the broker. This is for enhanced security by ensuring that all PCoIP connections are managed.

Amulet Hotkey Quad Monitor Support

Quad monitor configuration is supported with Amulet Hotkey PCoIP clients. To add a PCoIP client supporting Quad monitor:

- Add the desired PCoIP client to DeskView. Only the Primary PCoIP device will be displayed. Verify the MAC address by going to the Properties of the device.
- Manually add the IP address of the secondary PCoIP device.



- The second PCoIP device of the client will not be displayed in the DeskView Administration Console. It will automatically be mapped to existing entry of the primary PCoIP device. Once both PCoIP devices are added for the PCoIP client, Quad monitor support will be enabled.

Firmware

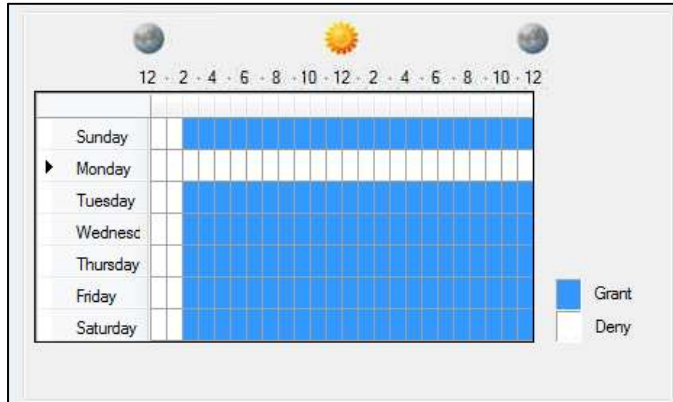
When the DeskView connection broker is used to deploy firmware, all PCoIP devices will use the same firmware version. Firmware is deployed using the FTP protocol. The FTP server containing the firmware file is defined under *FTP Settings*.

NOTE PowerTerm WebConnect includes a built-in FTP server. The default FTP folder is located at `<drive>:\Program Files\Ericom Software\WebConnect 5.X\DeskViewServer\ftproot`. To view the contents use a browser and navigate to ftp://<WebConnect_server_address>.

To use DeskView to deploy firmware, enter the *File name* of the firmware file (as hosted on the FTP server). Click *Test Download* to verify that DeskView can access the firmware file. Leave the *File name* empty to disable firmware deployment.

NOTE DeskView does not notify the users when the firmware is updated, there may be unexpected reboots when new firmware is applied.

DeskView can be configured to deploy firmware only on predefined times of the day. Configuring firmware deployment for off-hours will reduce or eliminate user disruption from reboots. Click *Specify update times* to configure this feature.



Authentication

The Authentication tab sets the client verification type.



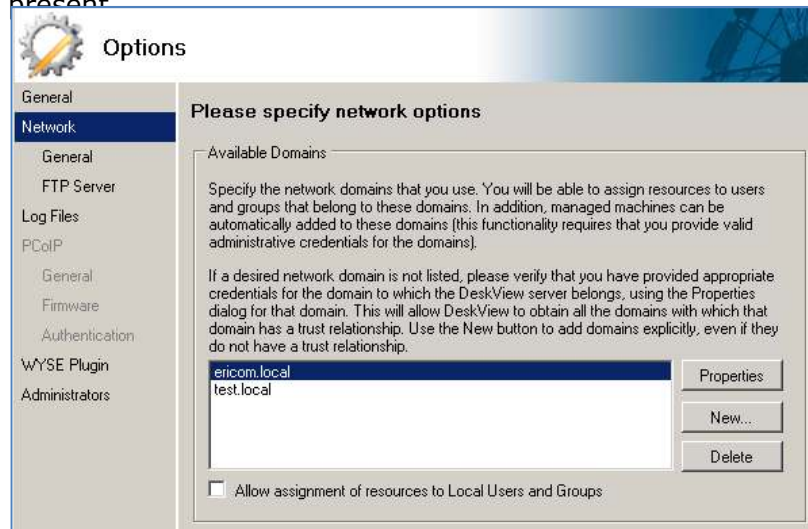
- *Regular* – use directory services based credentials
- *Radius* – use *Radius* server based credentials. See the section on Radius authentication for more details.

RADIUS for PCoIP Devices

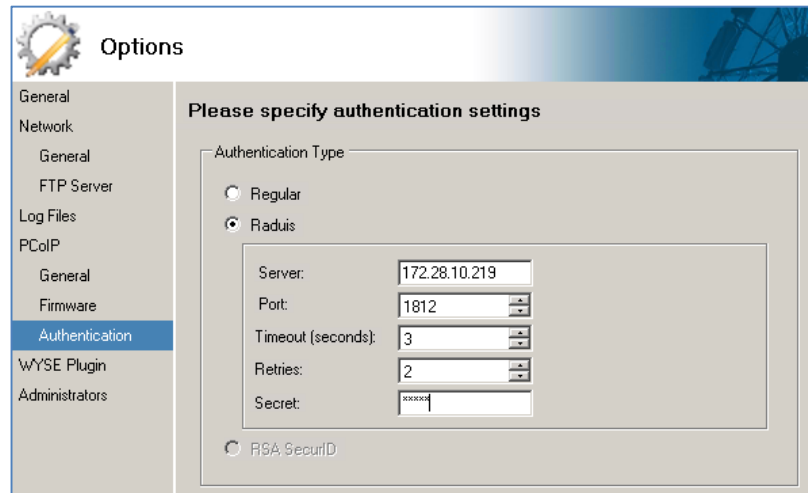
PowerTerm WebConnect DeskView supports RADIUS authentication from PCoIP clients. This section explains how to configure DeskView to use RADIUS for client authentication.

- Open and login to the PowerTerm WebConnect Connection Broker *Administration Tool*.
- Right click on PowerTerm WebConnect DeskView and select Options.

- Click *Network* and add the Radius Domain if it is not already present



- Click *PCoIP* and select the *Authentication* button
- Select *Radius* and enter the parameters for the desired RADIUS server



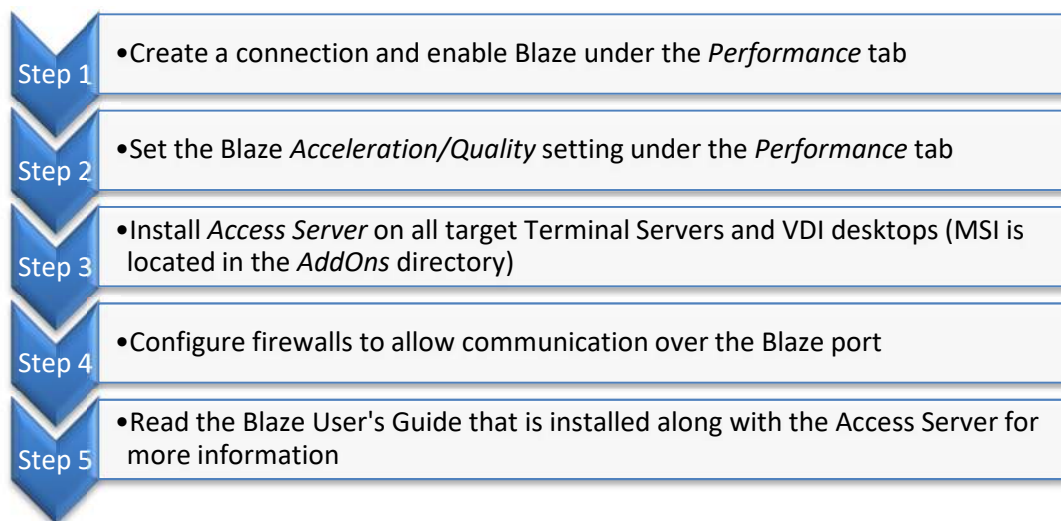
- Certain RADIUS servers require that the user enter the domain prefix or UPN - check the appropriate box if needed
- Click *OK* and use a configured PCoIP client to test the RADIUS login

16. ENHANCEMENTS FOR TS AND VDI

Ericom AccessNow and Blaze

Ericom AccessNow and Blaze provides end-users with an enhanced remote computing experience over slower networks: WAN, broadband, and air-cards. This is achieved by significantly accelerating and compressing Microsoft Remote Desktop Protocol (RDP). The results are higher frame rates, improved response times, and smoother screen updates. Ericom AccessNow and Blaze works with any x86 or x64 based host system that supports RDP, including Windows Terminal Servers, remote physical desktops and VDI based desktops.

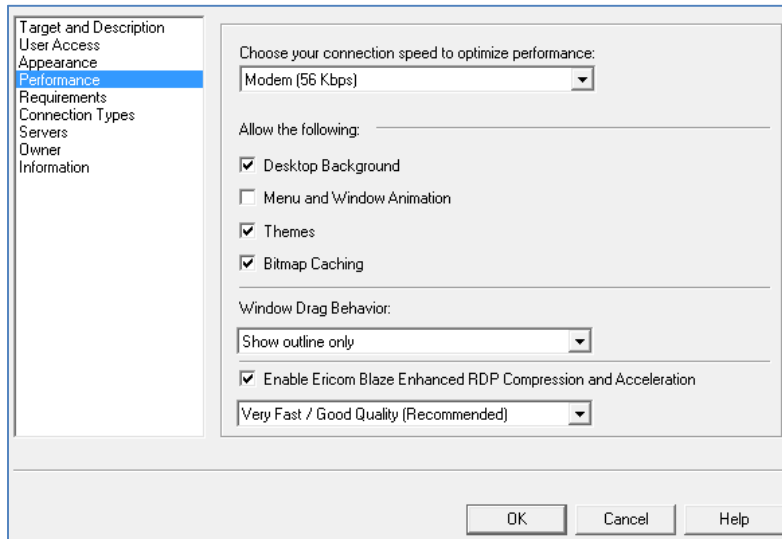
AccessNow/Blaze Configuration Summary



NOTE Actual performance improvement over RDP may vary across different types of devices and networks. The native Blaze client includes audio compression and, this technology will be available in a future version of AccessNow.

Ericom AccessNow/Blaze Configuration

Acceleration may be enabled for each published Windows application and desktop. During the publishing wizard, the administrator will be prompted to set the Blaze settings under the *Performance* dialog box. For an existing connection, this screen is accessed by right clicking on the Connection, selecting *Properties*, and going to the *Performance* view.



By default, Blaze is disabled. To enable Blaze, check the *Enable* checkbox and select the desired performance/quality setting. Blaze acceleration is included in AccessNow HTML5 connections as well.

Ericom Blaze Acceleration / Quality Settings

- *Moderate/Highest* – Perfect quality (lossless compression). Appropriate when exact image rendering is required.
- *Good/Very High* – Minimal image quality loss.
- *Fast/High* – Slightly less quality, slightly greater acceleration than Best.
- *Very Fast/Good* – Balanced quality and performance, ideal for most cases.
- *Fastest/Fair* – Lower quality but better performance. Appropriate when bandwidth is limited, especially when using graphic intensive applications.

Blaze Target Configuration

When manually defining an address for the server using the *Servers* configuration, verify that the Port number is set to *8080* (the Blaze port).

Required Access Server Installation

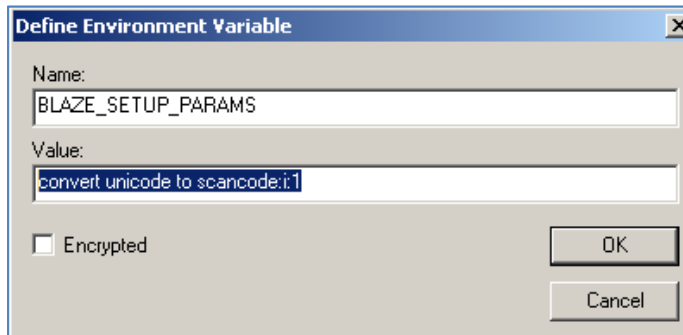
Once Blaze is enabled, the connection will connect using the default Blaze port of *8080*. The target server/desktop must have the Access Server installed and the firewall configured to allow incoming connections over the Blaze port. The Access Server installation is located in the *AddOns* folder. This is installed once on a Terminal Server, or on each virtual desktop.

NOTE When Access Server is installed on a system where TS Agent is running, uninstalling Access Server may disable the TS Agent (and its functions such as seamless applications). Reinstalling the TS Agent may be necessary.

AccessNow and Blaze Client Configuration

Additional AccessNow and Blaze related client settings may be configured in the PowerTerm WebConnect server as an environment variable. Add the variable `BLAZE_SETUP_PARAMS` and enter the desired parameters into the *Value* field. Refer to a `.blaze` file for possible values (download the Blaze client from the Ericom website to create a `.blaze` file).

In this example, the setting *convert unicode to scancode* is set to 1 to enable scan code support (required for certain applications and any Linux session).



To specify multiple values, separate each one with a semi-colon `;`.

NOTE Settings defined in `BLAZE_SETUP_PARAMS` will override any similar PowerTerm WebConnect setting. For example, if *audiomode:i:2* is set (disables audio), this will take precedence over the audio setting in the connection's *Properties*.

Single Sign-on from Workstation

PowerTerm WebConnect supports single sign-on (SSO) using the same user name and password credentials as those used when logging into the end user's desktop. The SSO feature streamlines the users' access process by reusing credentials that are already accepted and reduces the number of times they must sign on.

Client Configuration

The SSO feature is enabled by installing an MSI on each user's workstation. The MSI can be found under the `AddOns\SSO` folder:

- `PtSSOLogon32.msi` – use this for 32 bit operating systems

- PtSSOLogon64.msi – use this for x64 operating systems

After installing the SSO component, the user must logoff and back on for the SSO component to capture the local credentials.

NOTE This component is not compatible with *AccessPortal*, *AccessPad*, and *AccessToGo* clients

Web server Configuration

In order to use SSO, the client parameters must include `/USER=##`. This parameter will force the ptagent component to use the credentials provided by the SSO component.

```
var PT_server = location.hostname,  
var PT_agentParameters = "-wc-client " + PT_server + "/USER=## /SHORT  
var PT_clientDst = "";
```

NOTE Users without the SSO component installed can still sign on normally with the `/USER=##` parameter

Built-in Login Scripting

This product includes the PowerTerm TSagent. The PowerTerm TSagent supports the ability to launch a `.vbs` script during certain RDP session events. This adds an additional layer of functionality to run certain commands when an application is launched or when a session is connected/disconnected.

Post-Startup Login script for all sessions (`_login`)

Create a file named `_login.vbs` and place this in the `scripts` folder where the TSagent is installed. If this folder does not exist, create it. This script will execute after the TS/RDS session processes the `Startup` folder.

Pre-Startup Login script for all sessions (`__login`)

Create a file named `__login.vbs` and place this in the `scripts` folder where the TSagent is installed. If this folder does not exist, create it. This script will execute before the TS/RDS session processes the `Startup` folder.

Script for connecting into an existing session (`_connect`)

Create a file named `_connect.vbs` and place this in the `scripts` folder where the TSagent is installed. If this folder does not exist, create it. This script will execute upon connection into an existing TS/RDS session.



Script for disconnecting from sessions (`_disconnect`)

Create a file named `_disconnect.vbs` and place this in the `scripts` folder where the TSagent is installed. If this folder does not exist, create it. This script will execute after a TS/RDS session is disconnected.

Login Script for a connection

Create a file named `<connection-name>.vbs` and place this in the `scripts` folder where TSagent is installed. If this folder does not exist, create it.

For example, if a connection with the connection name *WordPad* exists. Each time this connection is launched, the file `wordpad.vbs` will be launched as well if it exists in the `scripts` folder.

Sample VB Script to create a new file

```
Set objFileToWrite =  
CreateObject("Scripting.FileSystemObject").OpenTextFile("newfile.txt",2,true)  
objFileToWrite.WriteLine("hello world")  
objFileToWrite.Close  
Set objFileToWrite = Nothing
```

17. UNIVERSAL PRINTING

Introduction

Remote printing with a Terminal Server environment can sometimes become problematic for the following reasons:

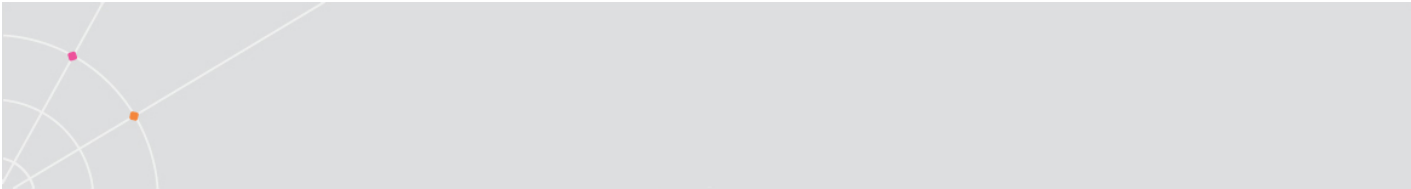
- Network traffic overhead of large print jobs transmitted from the Terminal Server's Print Manager to the local printer causes printing to be very slow.
- The need to install each user's printer drivers on every Terminal Servers is cumbersome. If a required printer driver is not installed on a Terminal Server, the user may not be able to print locally from that server.
- Each time a printer driver needs to be updated, the administrator must perform the update on each Terminal Server; the user has no control.

Universal Printing is a type of redirected printing where a single (universal) printer component is installed on each Terminal server and end user client device. On the Terminal Servers, a server component receives the user's print request and redirects it to the user's printer agent (connected to the local printer). This form of printing simplifies printer driver management, but may sacrifice print accuracy.

PowerTerm WebConnect is compatible with *five types of* universal printing solutions:

NOTE Linux Native client support will be available in an upcoming version.
Please use AccessNow with Linux devices

<i>Print solution</i>	<i>Platform(s) supported</i>	<i>Protocol(s) supported</i>
Blaze Universal Printer	Windows, Mac, Linux	Blaze (All platforms) RDP (Mac and Linux)
AccessNow Universal Printer	Any device with an HTML5 compatible browser that can print to a local printer	AccessNow
Net2Printer	Windows	Blaze, RDP
triCerat	Windows	Blaze, RDP



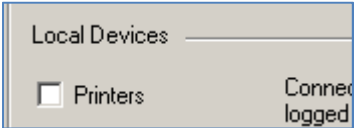
Microsoft Easy Print	Windows	RDP
----------------------	---------	-----

Supported universal print solutions will work with both *Direct* and *Gateway* modes. Most printer connection types are supported: USB, LPT, serial, and network (TCP/IP) connected printers.

NOTE Universal printers use a generic print driver to process the print jobs. Certain printer specific features may not be available (i.e. duplex printing).

Printer Availability

When the triCerat/Net2Printer add-on is enabled, it will always be available regardless of the *Local Printer* setting in the connection's *Properties*.



This table explains which printers will be available when triCerat or Net2Printer is enabled in conjunction with the Local Printer setting.

Windows (triCerat/Net2Printer enabled)	Printer Available
Blaze enabled, Printer setting disabled	triCerat/Net2Printer Printer
Blaze enabled, Printer setting enabled	triCerat/Net2Printer Printer, Blaze Universal Printer
RDP, Printer setting disabled	triCerat/Net2printer Printer
RDP, Printer setting enabled	triCerat/Net2printer Printer

Mac/Linux/Windows (triCerat/Net2Printer disabled)	Printer Available
Blaze enabled, Printer setting disabled	None
Blaze enabled, Printer setting enabled	Blaze Universal Printer
RDP, Printer setting disabled	None
RDP, Printer setting enabled	RDP Redirected Printer *

* On Mac/Linux, RDP sessions will use the built-in Blaze Universal Printer instead of the standard RDP redirected printer.

AccessNow and Blaze Printer on Windows 8 and 2012

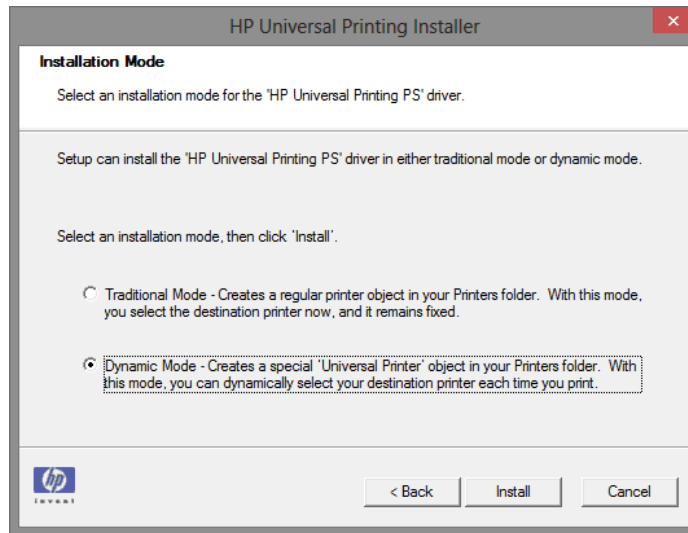
Windows 8 and 2012 do not include the necessary built-in drivers to support the AccessNow Printer. This functionality can be added by installing the HP Universal Postscript (PS) Printing Driver.

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>

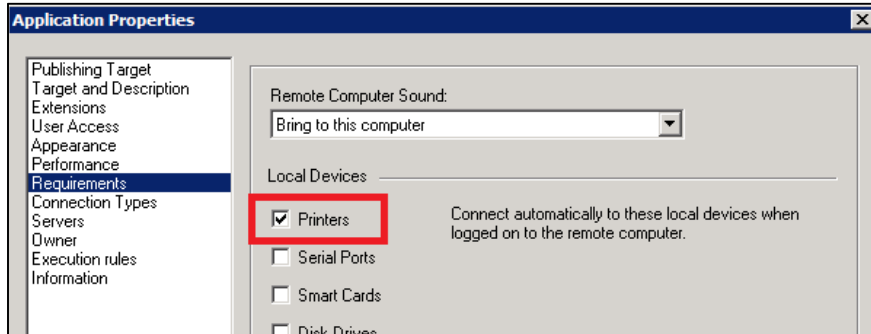
During the installation, when prompted for the *Installation Mode*, choose *Dynamic Mode*. Use default settings for all other selections.



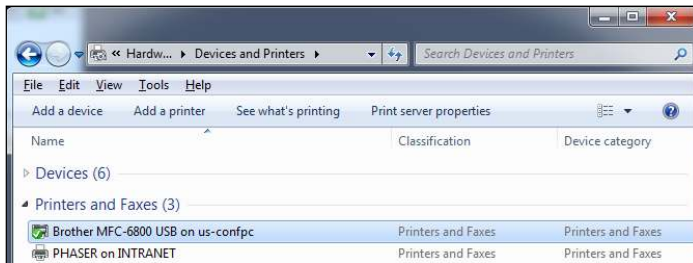
Using Ericom Blaze Printing on Windows

MORE Some content in this chapter is taken from the Ericom Blaze manual. Refer to the Ericom Blaze manual for additional details.

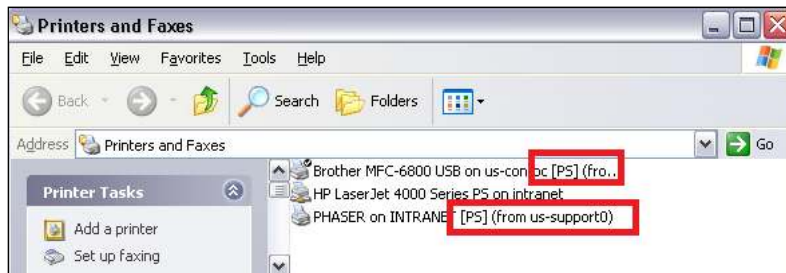
Ericom Blaze includes support for universal printing. The built in universal printer is based on Postscript and will redirect remotely executed print jobs to local printers. To enable universal printing, check the *Printers (universal)* setting:



In this example, the Windows 7 system running the Blaze has two local printers available:

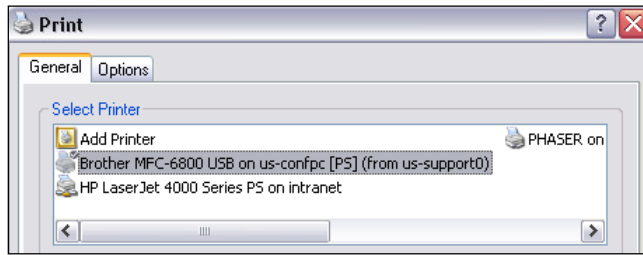


In the Blaze RDP session, the redirected printers will appear alongside any local printers configured on the remote desktop. Redirected printers will have the symbol "[PS]" along with the computer name in its label.



NOTE A generic HP Postscript driver is used to process the print jobs. Users will be able to print to most types of printers, however, certain printer specific functions may not be available (i.e. duplex printing, special trays, etc). To support advanced features, consider using a third-party print solution or standard RDP printing (by loading the printer driver(s) on the RDP host).

To print to a redirected printer, simply select the desired printer when the application's *Print* dialog appears.



NOTE If the redirected printers do not appear, verify that the following printer driver is installed: *HP Color LaserJet 2800 Series PS*. This is available on most operating systems, and can be manually installed if it is missing.

Using Ericom AccessNow Printing

MORE This chapter is taken from the Ericom AccessNow manual. Refer to the Ericom AccessNow manual for additional instructions.

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.

Requirements.

In order for the AccessNow Printer to be added to the remote sessions, the AccessNow 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 *AccessN Server Properties* and enter a user account that has the rights.

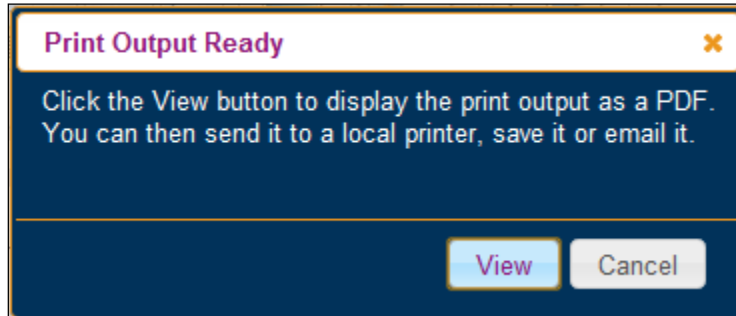
Usage

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 the desired printer when prompted at the Print dialog window.



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



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

Sample printout URL:

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

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

Universal Printing with Windows 8 or 2012 RDP Hosts

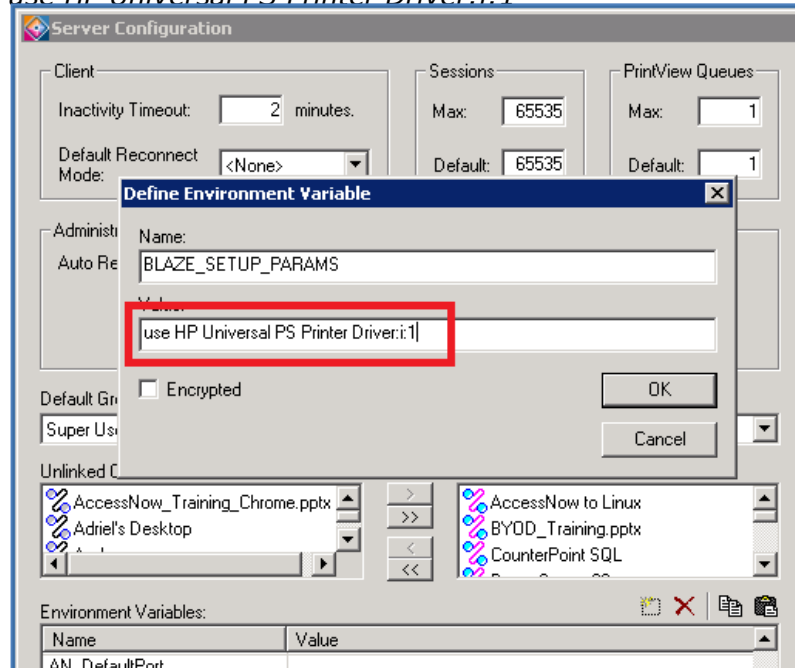
The HP Universal PS Printer driver is required in order to support universal printing with AccessNow, AccessPad, and Blaze on Windows 8, 2012, and 2012R2 operating systems. Download the appropriate driver from the HP website or Ericom's Update Center website.

After installing the HP Universal PS Driver, the Ericom printer will appear at the next user login (if printing is enabled for the session). Any instances of the HP Universal Printer may now be deleted from the Windows *Printers* menu as the driver is now present on the RDP host system.

Using AccessNow Printer in HP Universal PS Mode

AccessNow Printer on Windows 2008R2 and 2003 uses a specific printer model as the driver (LJ 2880 or 8500). If this driver does not return accurate print output, AccessNow Printer may also be configured to use the HP Universal Driver if it is installed (see the section prior to this one for instruction details). Once the HP Universal PS Driver is installed on the RDP host, perform the following to enable it in AccessNow with PowerTerm WebConnect:

- Add a new PTWC environment variable to *Blaze_Setup_Params*:
use HP Universal PS Printer Driver:i:1



- AccessNow sessions created with this setting enabled will use the HP Universal PS driver for the AccessNow Printer.

Using Net2Printer with PowerTerm WebConnect

Net2Printer installers are bundled with the PowerTerm WebConnect Server installation. The installers for the Net2Printer components are located in the *AddOns\Net2Printer* folder in the PowerTerm WebConnect application folder. These include the installers for both the Terminal Servers and clients. When Net2Printer is enabled, PowerTerm WebConnect will install the Net2Printer client automatically on each user's system when RemoteView is launched. The printers will be mapped by Net2Printer during the logon process to the Terminal Server.

Terminal Server Installation

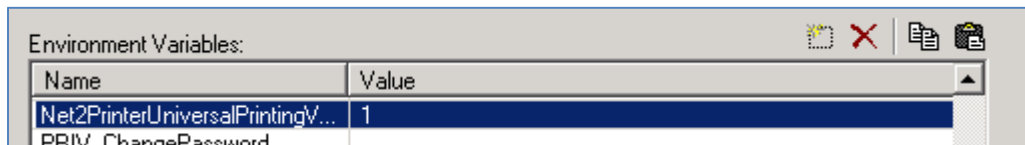
To use Net2Printer Universal Printing, install *NPSSetupRDPServer.exe* on each Terminal Server that will be managed by PowerTerm WebConnect. During the installation, the default selections can be used.



Enabling Net2Printer

To configure Environment Variables for Net2Printer Universal Printing:

- Launch PowerTerm WebConnect Administration Tool.
- Select *Server | Configuration*. The *Server Configuration* dialog opens.
- Set *Net2PrinterUniversalPrintingVersion* to 1.
- Set *PRIV_UniversalPrinting* to 1.
- Set *RDP_DisableUniversalPrinting* to 0.
- Click *OK*.



If Net2Printer is properly installed, the user will see a yellow Net2Printer systray icon when the Net2Printer client is properly connected to the Net2Printer server.

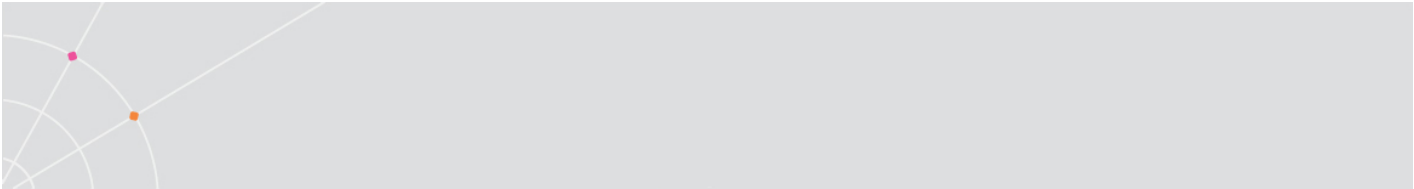




NOTE if the icon is white, the client was unable to connect to the server.

Once Net2Printer is active, additional configuration of the client can be performed by right clicking the yellow Net2Printer icon and selecting Configuration.

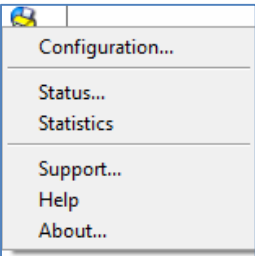
Usage

When launching any RemoteView session with Net2Printer enabled, the Net2Printer Systray icon will appear on the user's local system.



Status	Description
	Net2Printer is running, but not connected – not ready to print
	Net2Printer is running and connected – ready to print

When the icon is yellow (active), right click on it to open an action menu.

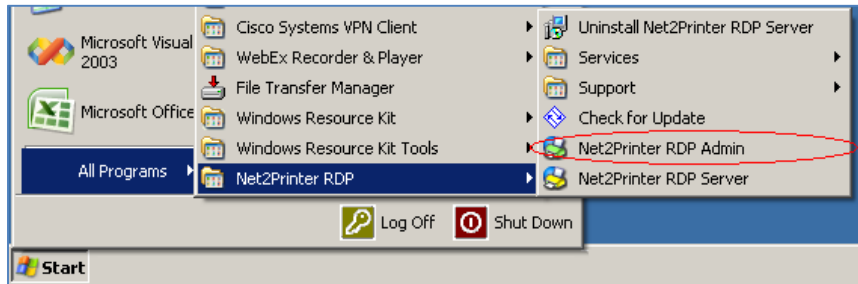


Menu Item	Description
Configuration	Select which local printer to redirect to the RemoteView session. Set the default printer to be redirected. Access <i>Advanced Options</i> page.
Status	Displays the status of the Net2Printer connection
Statistics	Displays how many jobs have been processed by Net2Printer
Support	Displays the log activity. Set the logging level to <i>Debug</i> to capture additional information for technical support. <i>Clear Log</i> = Clears the current log contents <i>Save Log</i> = Saves the log contents into a file
About	Displays the version number of Net2Printer being used

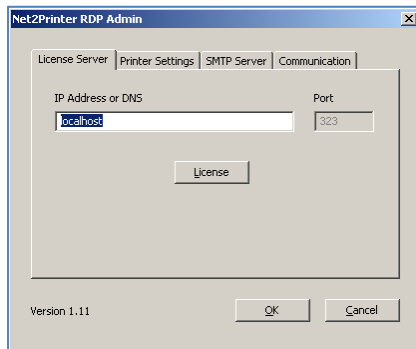
NOTE The Net2Printer icon will remain active even after all RemoteView sessions are closed. RemoteView sessions will remain open based on the setting *RDP_LogOffDelaySeconds*. Net2Printer will deactivate once the RDP session is closed.

Server Configuration

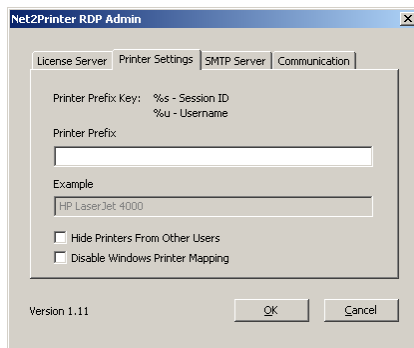
To configure the Net2Printer RDP Server component, open Net2Printer RDP Admin from the Start Menu.



Under the License Server tab enter the address of the Net2Printer RDP licensing server, or activate a license on the current server.



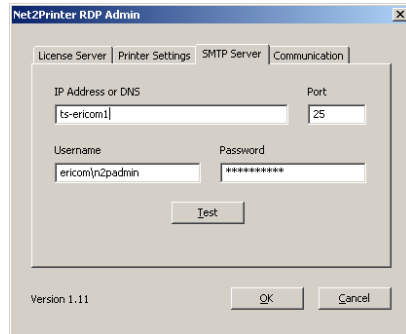
On the second tab configure the printer settings, such as the naming convention of the printers that will appear into RDP sessions. As the Printer Prefix is updated, the *Example* window will change to reflect how it would appear to the end user.



It is recommended to configure Net2Printer to hide any printers that it creates from other users on the same Terminal Server. This will prevent users from printing to someone else's printer. It is also recommended to disable the Terminal Server's internal Printer Redirection feature from this dialog box.

The SMTP Server tab enables users to email PDF printouts. By printing to the Net2Printer object named "Email", users can email the PDF output of the print

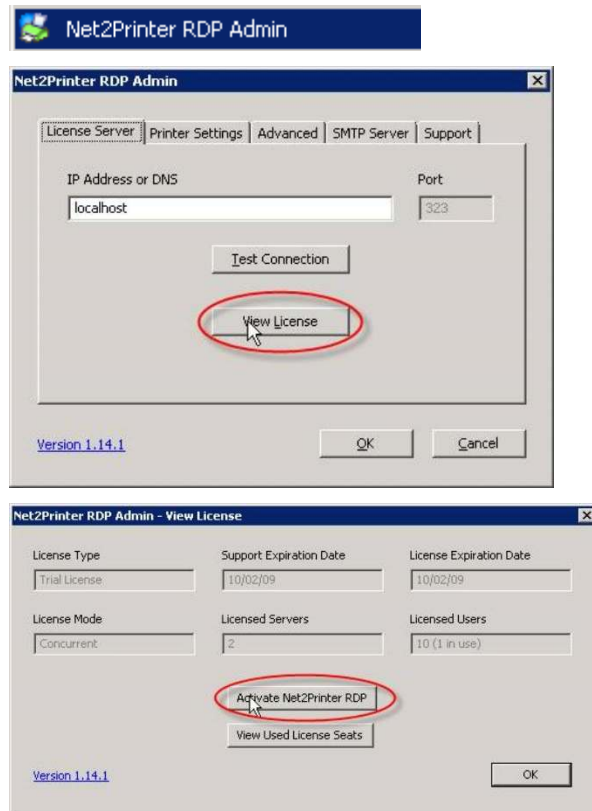
job. Enter the network's SMTP server IP/DNS name, port, and if required, a valid SMTP username and password.



Licensing and Activation

Net2Printer licenses are not included with PowerTerm WebConnect. In order to purchase Net2Printer licenses please contact Ericom Software.

To activate or reactivate a license, launch the *Net2Printer Admin* and go to the *License Server* tab. Click on: *View License* and then on the *Activate Net2Printer RDP* button.



On the *Activate* screen enter the *Net2Printer Signup Email Address* with:
net2printer@ericom.com

Enter the *Order Number* that has been provided. Click *Activate* to complete the online activation.

NOTE The procedures documented above requires an Internet connection. If the system is not connected to the Internet, click the *Manually Activate* button at the *Order Number* entry dialog box.

A rectangular button with a light blue border and the text "Manually Activate" centered inside.

Disabling Scanning in Net2Printer

Net2Printer includes a built-in scanning redirection technology. This may be disabled so that end-users will not have access to scanning redirection. To disable the Net2Printer scanning, remove the Net2Printer TWAIN file. Simply search the C: drive and remove all instances of NPScan.ds. This file may be located under one of these paths:

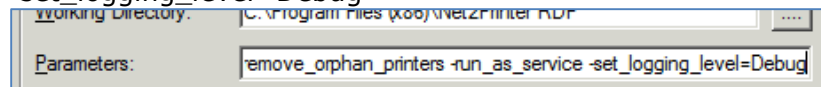
- C:\Program Files\Net2Printer RDP\TWAIN\
- C:\Users\\Windows\TWAIN

Troubleshooting

If there are technical issues with Net2Printer functionality, send Ericom the debug log(s).

On the affected Terminal Server running Net2Printer - using the user account that installed Net2Printer (i.e., local Administrator) do the following.

- Enable debugging on the printer service by going to Start | Programs | Net2Printer RDP | Services | *Configure Service*. Alternatively, launch *FireDaemonUI.exe* and click on the banner.
- Double click on the Net2Printer RDP Printer Service and change the Parameters value to:
-remove_orphan_printers -run_as_service
-set_logging_level=Debug



- Press *Update* or *OK* and then restart the service. Existing sessions will lose their printing functionality temporarily, so it is recommended to perform this when users are not printing (off-hours).

- Next, go to the batch file for the server located under the system32 directory of the server. Open the file NPserverRDP.cmd and add the following parameter to the end: -disable_process_monitoring -set_logging_level=Debug
 - The value entered will look similar to:
start /d"C:\Program Files (x86)\Net2Printer RDP\"
npserverrdp.exe -disable_process_monitoring -
set_logging_level=Debug

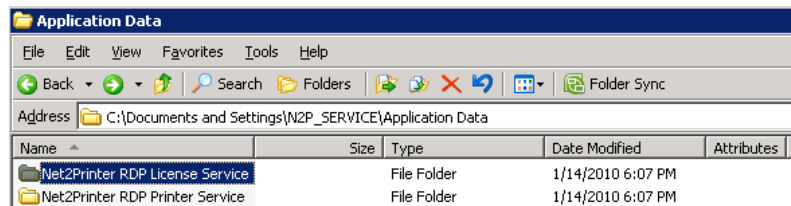
On Windows 2003 systems running the Net2Printer Server, debug log files related to the server services are found under the *N2P_SERVICE\Application Data* folder.

On Windows 2008/2012 systems running the Net2Printer Server, debug logs are found here:

C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\Net2Printer RDP Printer Service

Server logs are under the *Net2Printer RDP License Service* subfolder

Licensing logs are under the *Net2Printer RDP License Service* subfolder

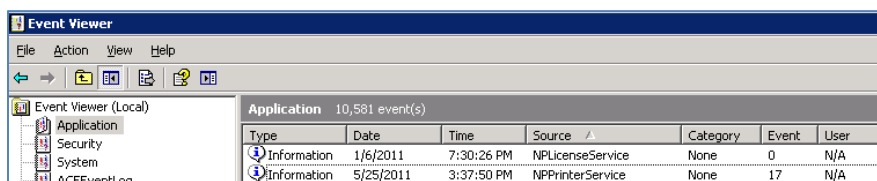


Each user will also have its own Net2Printer debug log file located under:

Windows 2003: <drive letter>:\Documents and Settings\<username>\Application Data\Net2Printer RDP Server

Windows 2008/2012: C:\Users\<username>\AppData\Roaming\Net2Printer RDP Server

In addition to sending Ericom the necessary log files, verify if there are any Event Viewer entries on the Terminal Server. Net2Printer related entries will have the source name of NPPrinterService or NPLicenseService.





Using triCerat ScrewDrivers with PowerTerm WebConnect

The triCerat ScrewDrivers installers are included with PowerTerm WebConnect. The installers for the ScrewDriver components will be located in the AddOns\triCerat folder in the PowerTerm WebConnect server folder. The server component needs to be installed on each Terminal Server. The client component is used for manual installations on client systems. When triCerat is enabled, its client components are automatically downloaded along with the PowerTerm WebConnect client components.

<p>NOTE triCerat ScrewDrivers may be installed and used independently of PowerTerm WebConnect as well.</p>

Terminal Server Installation

To enable universal printing on a Terminal Server, the appropriate *ScrewDriver* server component must be installed. For x64 servers, the x64 installer must be used (ScrewDriversServer_v4.5.02.44_x64.msi).

The ScrewDriver server installation includes a Control Panel Applet that can be used to configure its functionality. Each Terminal Server installation needs to be managed independently. Please refer to the triCerat ScrewDriver documentation and online help for further details.

Enabling ScrewDrivers

Configure the following Environment Variables to enable triCerat printing:

- Launch PowerTerm WebConnect Administration Tool.
- Select *Server | Configuration* - the *Server Configuration* appears.
- Set *PRIV_UniversalPrinting* to 1.
- Set *RDP_DisableUniversalPrinting* to 0.
- Set *TriceratUniversalPrintingVersion* to 1 and click *OK*.

If triCerat ScrewDrivers is properly installed, the user will see a red screwdriver systray icon when the RemoteView session is established.

Standalone Installation

If RemoteView is installed using the MSI installer, then the appropriate ScrewDriver Client MSI must also be used. If a ScrewDriver plugin has already been installed on the client device prior to the RemoteView installation, RemoteView will detect and use the existing plugin.

If RemoteView succeeds in loading the plugin, it will disable the RDP control "Redirect Printers" property in order to avoid using duplicate printers on the Terminal Server.

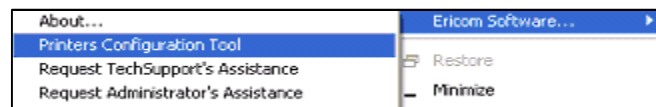
triCerat Printers Configuration Tool

If the triCerat client is installed using the MSI, the triCerat Client Configuration Tool will be available from the user's Windows Control Panel.

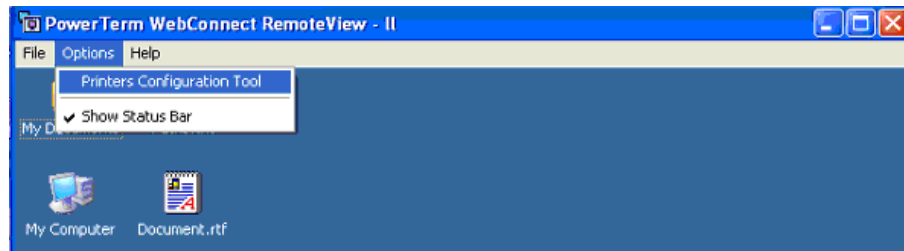
- Open the Windows Control Panel.
- Click triCerat Client Configuration.

If the triCerat client is installed using the PowerTerm WebConnect URL, the Configuration Tool is accessed using the published application's Start bar icon:

- Right-click on the Start bar icon and select *Ericom Software* from the menu list.
- Select Printers Configuration Tool.



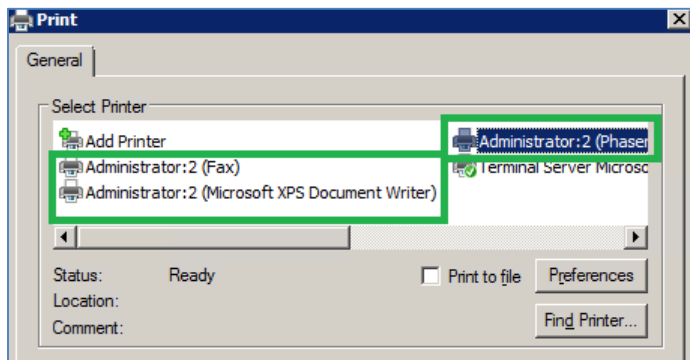
When working with a Full Desktop window, the Printers Configuration Tool is accessed by clicking Options | *Printers Configuration Tool*.



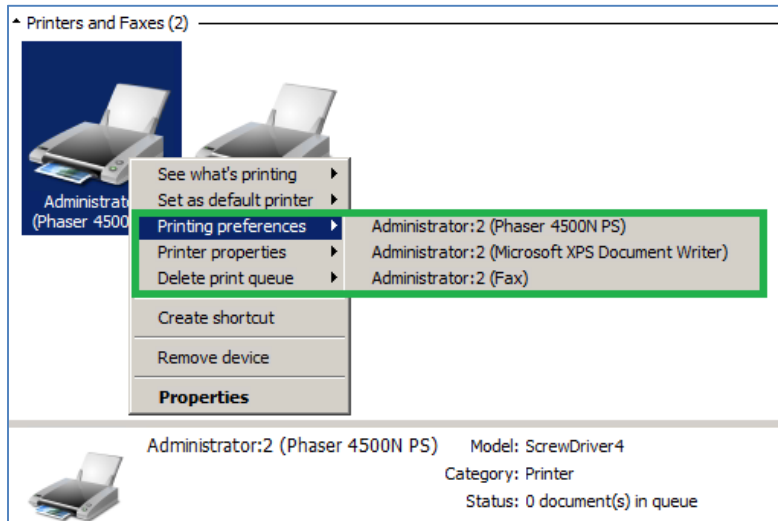
The Printers Configuration Tool is also accessible from the Application Zone.

Usage

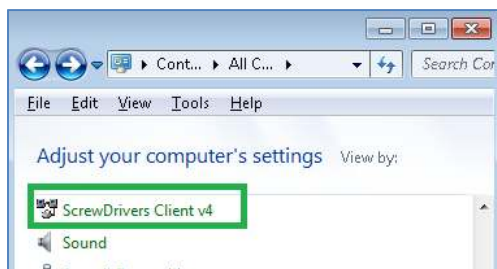
When launching a RemoteView session with triCerat enabled, the redirected printers will appear in the application's *Print* dialog:



Only the primary redirected printer will be viewable in the Print Manager. By right clicking on the primary triCerat printer in the Print Manger, settings for all redirected printers can be accessed.



Additional settings can be configured in the Screwdrivers Control Panel Utility on the client's device.



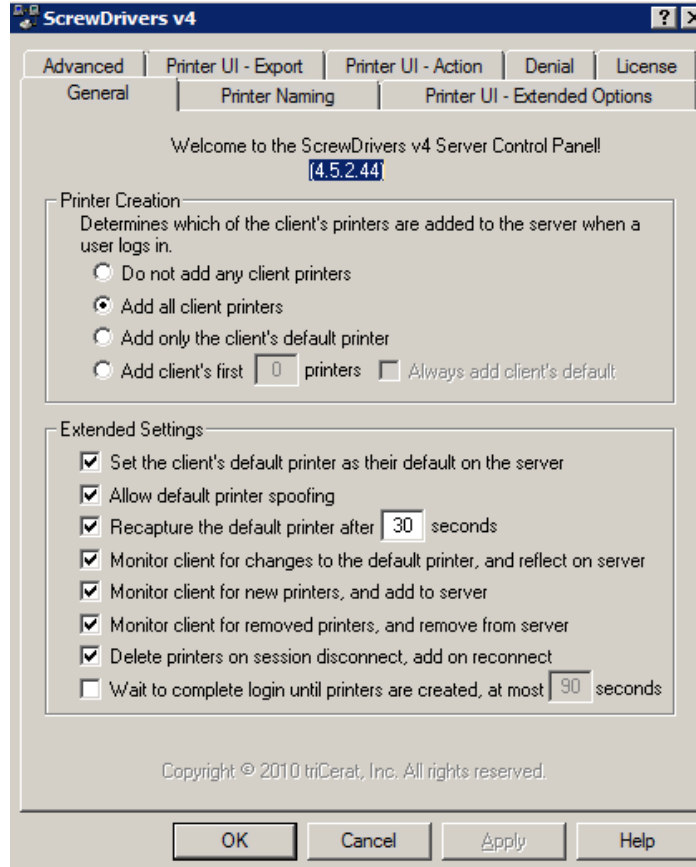
Server Configuration

To configure the triCerat Server component, use the ScrewDrivers Admin console from the Terminal Server's Control Panel.



These settings should be configured the same across all Terminal Servers to maintain consistent printing behavior.

To allow redirection of all local printers, select *Add all client printers* under the *General* tab. End-users can hide specific redirected printers by denying them by using the client-side Control Panel *ScrewDrivers* utility.



Configure any remaining settings as desired.

Licensing and Activation

triCerat licenses are not included with PowerTerm WebConnect. In order to purchase triCerat licenses please contact Ericom Software.

Using Microsoft Easy Print with PowerTerm WebConnect (RDP Only)

PowerTerm WebConnect supports Easy Print in most scenarios where Microsoft RDP (mstsc.exe) will support it. On the client end, MS Windows XP SP3 or higher is required. On the server end, MS Windows 2008/2012 or higher is required. Once the RDP session is established, the redirected local printers will appear in the remote session's printer list and ready to accept requests.

Ericom's RemoteView client (PTRDP.exe) uses a 32-bit Microsoft RDP control to support Easy Print. RemoteView currently does not support Easy Print from Windows x64 operating systems.

Selecting the Default Printer

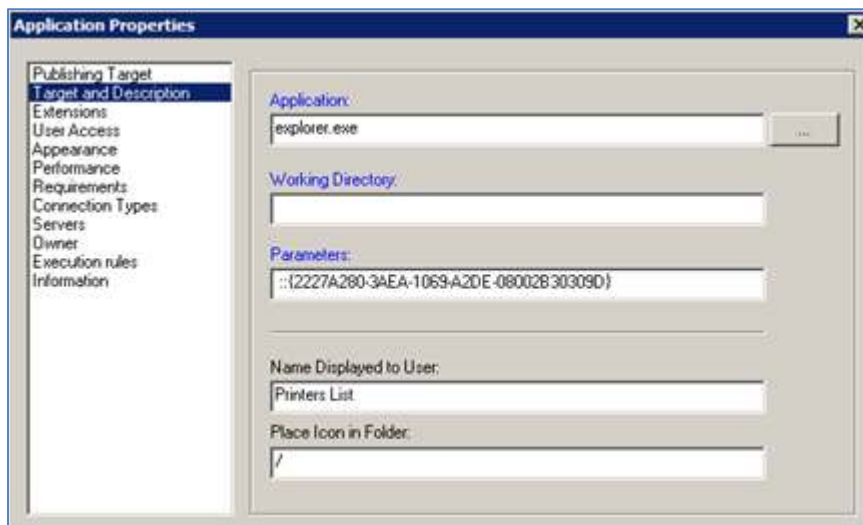
This section explains how to publish the Printer manager so users can select a default server printer (printer that is installed on the Terminal Server).

When using seamless applications, the Print Manager of the Terminal Server is not accessible to the user. To make the printer list accessible, publish the Printer user interface. This will allow users to select their own default printer.

Publish a new connection and enter these parameters:

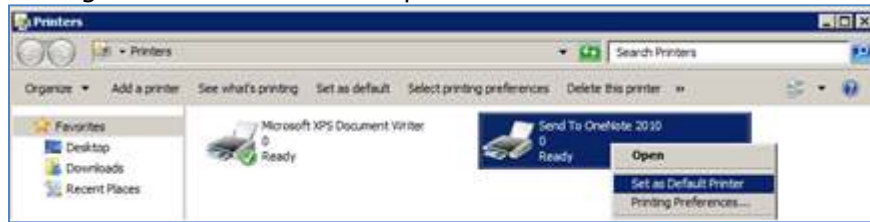
Application: Explorer.exe

Parameters: ::{2227A280-3AEA-1069-A2DE-08002B30309D}



When the user selects this connection, the printer list will appear. The user

can right click on the desired printer and select *Set as Default Printer*.



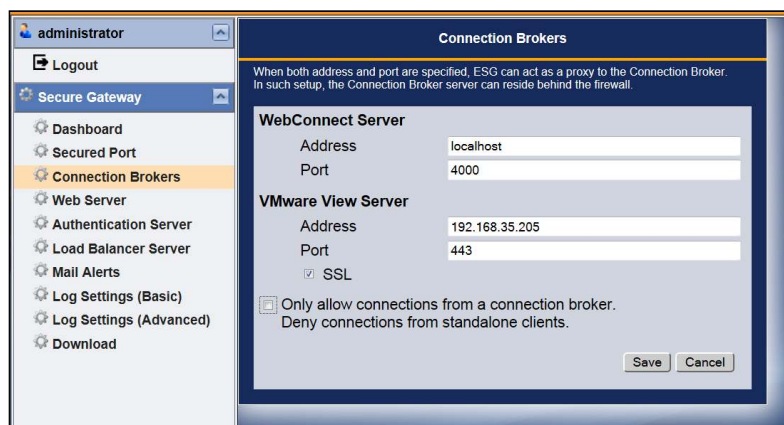
This was tested with a Windows 2008 R2 Server.

18. ERICOM SECURE GATEWAY (ESG)

MORE Portions of this chapter are taken from the Secure Gateway manual. Refer to the Secure Gateway manual for full installation instructions.

During the ESG installation, the Connection Brokers configuration page will appear.

Use this page to enter the address and port settings of the PowerTerm WebConnect that will be used with the ESG.



Select the *Deny connections from Standalone clients* setting to only allow connections through a connection broker. Connection attempts via the standalone Blaze and AccessNow clients will be denied, requiring all users to authenticate through a managed broker.

The PowerTerm WebConnect address must be configured with an address that is reachable from the ESG server. Use the *ping* and *telnet* utility to verify connectivity between the ESG and connection broker server.

Disabling HTTP/HTTPS content filtering

Port 443 on most firewalls are initially reserved for HTTP (and HTTPS) based communication. Most firewalls will have a rule in place to filter out any non-HTTP traffic. Depending on what the Secure Gateway will be routing, HTTP filtering may need to be disabled on the firewall. On firewalls where HTTP filtering cannot be disabled, choose a different port value other than 443 for the Secure Gateway.

The Ericom Secure Gateway can proxy various types of traffic. Some are HTTP based and some are not. The only configuration where HTTP filtering does not need to be disabled is if the Web Application Portal and AccessNow are used together.



This table denotes the protocol used by each connection method:

Communication type	Protocol used
Web Application Portal login	HTTP/HTTPS
AccessToGo login	HTTPS
Application Zone login	TCP
AccessNow RDP session	HTTPS (Secure Gateway required)
AccessToGo RDP or Blaze session	TCP
RemoteView RDP or Blaze session	TCP

On firewalls that have filtering enabled, but also support WebSockets, configure PowerTerm WebConnect traffic to use WebSockets by adding the client parameter **/websocket**.

PowerTerm WebConnect Configuration

PowerTerm WebConnect x.y client components support the Ericom Secure Gateway. The Secure Gateway is typically installed in the DMZ and acts as a single port relay proxy for all PowerTerm WebConnect related communication. This means that only one port needs to be opened on the external firewall. The Secure Gateway will securely tunnel all related communication through its port: PowerTerm WebConnect (4000), RDP (3389), Blaze 2.x (3399), AccessNow/Blaze 3.x (8080), HTTP (80), HTTPS (443), emulation (80), SSH (22), and more.

In order to configure PowerTerm WebConnect for use with the Secure Gateway, there are two steps to complete:

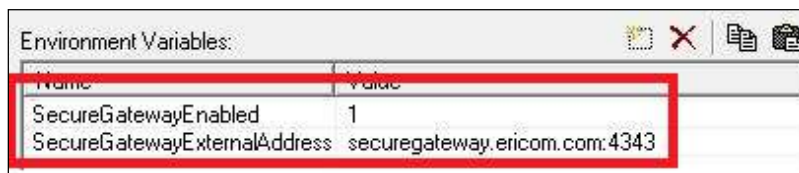
- Configure three environment variables in the PowerTerm WebConnect Administration console to enable the Secure Gateway.
- (Optional) Configure Secure Gateway "**sg**" specific Application Zone, Application Portal and AccessToGo clients that will be used externally to point to the Secure Gateway for the PowerTerm WebConnect address. The Secure Gateway is acting as a proxy to the broker server.
- (Optional) If the Secure Gateway will be used for both brokered and non-brokered access (i.e. Blaze Client) then the Authentication Server will be required in order to provide security for standalone clients.

Configure the Three Broker ESG Variables

Open the *PowerTerm WebConnect Administration Tool* and go to *Server | Configuration*. Scroll down the list of Environment Variables and go to the Secure Gateway related settings:

SecureGatewayEnabled	1 - Enabled 0 - Disabled (will an alternate service gateway built into the broker when Gateway mode is specified)
SecureGatewayExternalAddress	The address and port of the Secure Gateway server that will be reachable by the Ericom clients. This address and port must be reachable by end-users who will be connecting over the ESG.
SmartInternalIsGateway	AccessNow and AccessToGo do not support SmartInternal automatic detection. All settings that are set to SmartInternal will automatically use <i>Direct</i> by default with these clients. To force all SmartInternal connections to use Gateway, set this value to 1

In this example, all Ericom clients will connect to the Secure Gateway at the address: `securegateway.ericom.com` over port 4343.



NOTE If the Secure Gateway is using a trusted certificate, enter the DNS address of the Secure Gateway rather than the IP address here. A trusted certificate will need to recognize the domain name of the address.

If *SmartInternalIsGateway* is set to 1, all "Access" components (AccessNow, AccessPad, and AccessToGo) will use Gateway mode when the connection's Gateway setting is set to *SmartInternal*.

SmartInternalIsGateway | 1

NOTE "Access" components currently do not support the *SmartInternal* feature (this will be available in a future release).

Configure the Client files

When WebConnect is set as the Default ESG Web Server folder, the default page will be pointed to *sgstart.html*.



This may be changed in the .config file under `folder_name="WebConnect"`:

```
<add folder_name="WebConnect" default_page="sgstart.html"
allow_access="true" />
```

The "sg" versions of the *Application Zone* and *Web Portal page* files on the PowerTerm WebConnect broker may need to be configured to point to the Secure Gateway for the PowerTerm WebConnect Service.

STOP When using the same address (e.g. *sg.acme.com*) for internal and external users make sure that the external DNS for *sg.acme.com* will reference the external IP/address of the Secure Gateway (such as the address of the firewall that is forwarding port 443), and that the internal DNS will reference the internal IP/address of the Secure Gateway.

Optional /websocket parameter

When the Secure Gateway is using port 443, certain traffic may be filtered by the firewall. To prevent connectivity issues, configure the external facing firewall to allow **all** TCP traffic over the Secure Gateway port.

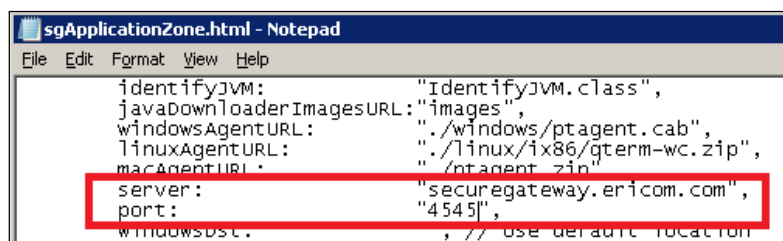
On firewalls where HTTP/HTTPS filtering cannot be disabled, configure PowerTerm WebConnect traffic to use WebSockets by adding the parameter */websocket*.

Application Zone Configuration

By default, the *sgapplicationzone.html* will use the address and port in the URL. In most cases, not customization is required in this page.

However, hardcoded values can be set for the "server:" and "port" variable.

In this example, the *sgapplicationzone.html* is pointed to the external Secure Gateway address on port 4545 (*securegateway.ericom.com:4545*) in order to access the PowerTerm WebConnect Service.



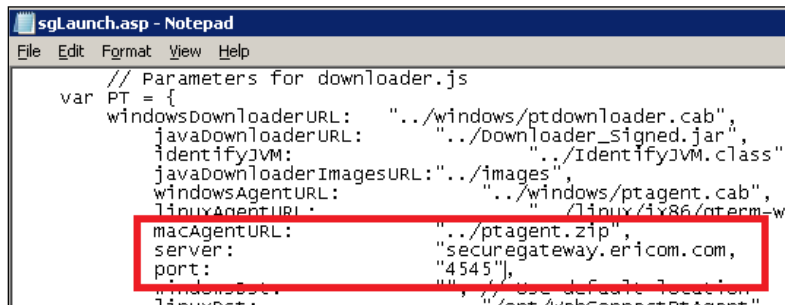
To enable WebSockets mode, add the parameter /websocket:

```
+ "/websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

Web Portal - sgLaunch.asp Configuration

By default, the *sgLaunch.asp* will use the address and port in the URL. In most cases, not customization is required in this page.

Similar to *sgapplicationzone.html*, hardcoded values can be set for the "server:" and "port" variable.



```
sgLaunch.asp - Notepad
File Edit Format View Help
// Parameters for downloader.js
var PT = {
  windowsDownloaderURL:    "../windows/ptdownloader.cab",
  javaDownloaderURL:      "../Downloader_Signed.jar",
  identifyJVM:            "../IdentifyJVM.class",
  javaDownloaderImagesURL:"../images",
  windowsAgentURL:       "../windows/ptagent.cab",
  linuxAgentURL:         "../linux/i386/pterm-wc",
  macAgentURL:           "../ptagent.zip",
  server:                 "securegateway.ericom.com",
  port:                   "4545",
  windowsPort:           "", // Use default location
  linuxPort:              "", // Use default location
}
```

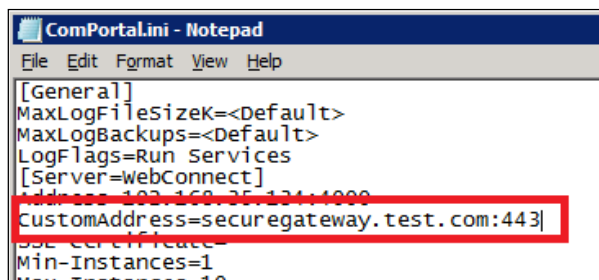
To enable WebSockets mode, add the parameter /websocket:

```
+ "/websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

Web Portal - ComPortal.INI Configuration

If the PowerTerm WebConnect Server and the IIS are running on separate machines, then configure *ComPortal.INI* to point to the Secure Gateway address and port. In this configuration there is no need to modify the *Launch.asp* or *sgLaunch.asp* file.

In the following example, the *ComPortal.INI* is configured to point to the Secure Gateway in order to reach the PowerTerm WebConnect service.



```
ComPortal.INI - Notepad
File Edit Format View Help
[General]
MaxLogFileSize=<Default>
MaxLogBackups=<Default>
LogFlags=Run Services
[Server=webConnect]
Address=193.168.25.134:1999
CustomAddress=securegateway.test.com:443
SSL certificate=
Min-Instances=1
Max-Instances=10
```

To enable WebSockets mode, add the parameter /websocket to the *Launch.asp* or *sgLaunch.asp* file:

```
+ "/websocket /SHORTCUT=BOTH /AUTOLOGIN=NO";
```

AccessToGo Client Configuration

Once PowerTerm WebConnect is configured for remote access with the Secure Gateway, it will support AccessToGo connections. Perform the following to connect to PowerTerm WebConnect using AccessToGo:

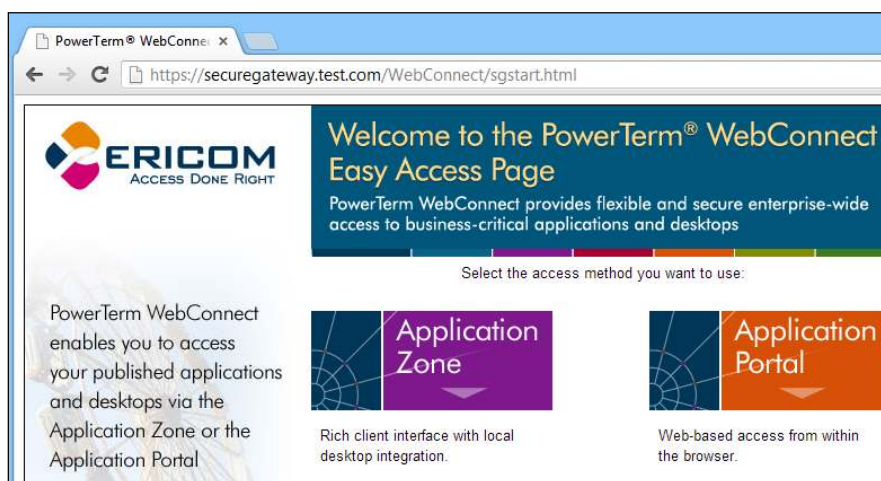
- Download the AccessToGo app
- Create a new PowerTerm WebConnect connection
- For the Server field, enter the server address and port (e.g. *securegateway.test.com:443*)
- Click OK and tap on the connection to launch it.

Connecting using the Secure Gateway

When using the Secure Gateway with PowerTerm WebConnect, direct the users to the URL of the Secure Gateway. The user simply has to enter <https://securegateway.test.com> (or http):



And the page will automatically redirect to <https://securegateway.test.com/WebConnect/sgstart.html>



Since the Secure Gateway is acting as a proxy to the Web server, all subfolders and filenames will be intact (i.e. /webconnect/sgstart.html).

If a port other than 443 is used as the Secure Gateway port, it must be explicitly specified in the URL (i.e. ":4343"):



NOTE All *SmartInternal* connections will automatically use *Gateway* mode when the user connects to PowerTerm WebConnect using the Secure Gateway. Direct connections will not be affected.

Manual Configuration of ESG

In addition to using the Configuration GUI, settings that were previously configured during the installation process may be changed by manually editing the *Config* file. This is a sample configuration where the Secure Gateway is configured to work with a PowerTerm WebConnect Server (PTWC) at address 192.168.35.134:

```
<WebConnectServer>
  <add key="Address" value="192.168.1.134"/>
  <add key="Port" value="4000"/>
</WebConnectServer>
<WebServer>
  <add key="Address" value="192.168.1.134"/>
  <add key="Port" value="80"/>
  <add key="SecuredConnection" value="false"/>
</WebServer>
```

Authentication Server

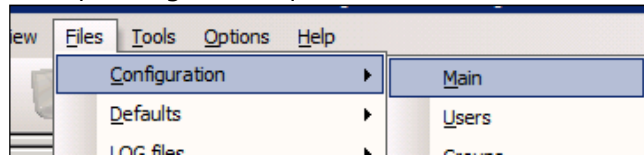
The Authentication Server is used in the following use cases:

- Support standalone clients in addition to WebConnect clients
- Provide support for RADIUS based two-factor solutions
- Provide the ability to recognize and change expired passwords with AccessPad and AccessPortal.

Configure the Authentication Server

The Authentication Server is required to secure standalone clients that will be used in the environment as well. In this scenario PowerTerm WebConnect and the Secure Gateway must work with the same Authentication Server. To configure PowerTerm WebConnect to use a specific Authentication Server, perform the following:

- Go to the PowerTerm WebConnect Administration Tool
- Files | Configuration | *Main*



- Go to the end of the file and search for the "Authentication Server" section. If you imported an earlier *ptserver.ini* file, the section may not be available and will have to be created
- Set the Address to be that where the Authentication Server is running at. In the example below, the Authentication Server is running on 192.168.0.2

```
[Authentication Server]
```

```
Address=192.168.0.2
```

```
Port=444
```

```
CertificateDnsIdentity=
```

```
MaxClockSkewMinutes=180
```

- In the Secure Gateway configuration file (EricomSecureGateway.exe.config) go to <externalServersSettings> | *AuthenticationServer* and set the value of *Address* to be the same value that is set in step 4.

```
<externalServersSettings>
```

```
<AuthenticationServer>
```

```
<add key="Address" value="192.168.0.2"/>
```

```
<add key="Port" value="444"/>
```

Configure RADIUS Two-Factor Authentication (2FA)

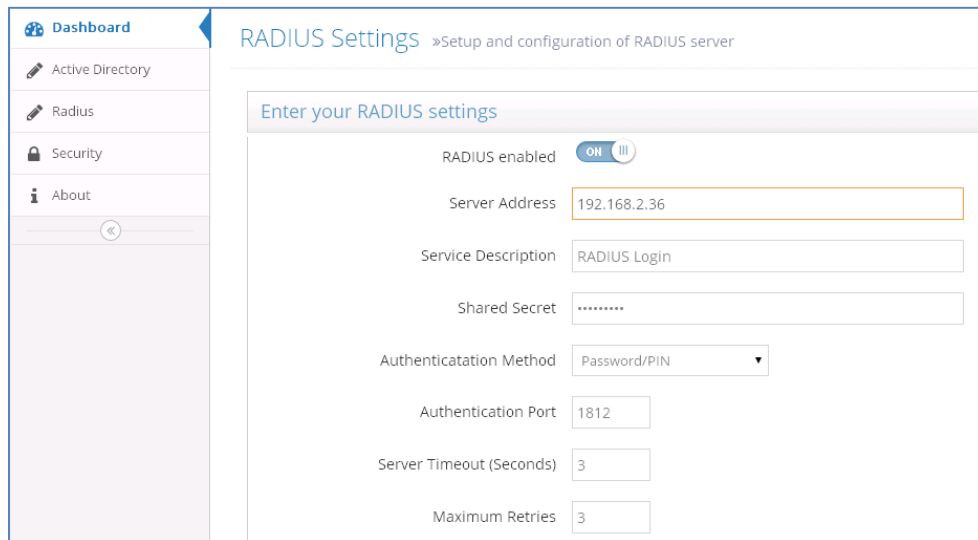
Requirements

- PowerTerm WebConnect 6.0 or higher
- Ericom Authentication Server 3.4 or higher

- Ericom AccessPad or AccessPortal
- Operational third-party RADIUS system

To configure RADIUS support in the Authentication Server, login to the Authentication Server's web admin console by navigating to the URL <https://<authentication-server-address>:7443/admin>

Select *Radius* and enter the parameters for the 2FA RADIUS server:



The *Authentication Method* configured in the Authentication Server must match the setting in 2FA system. If the incorrect method is configured, an error message will be displayed to the end user:

Reason: Ericom Authentication Server error (code 10030002):
Authentication error: ACCESS_REJECT

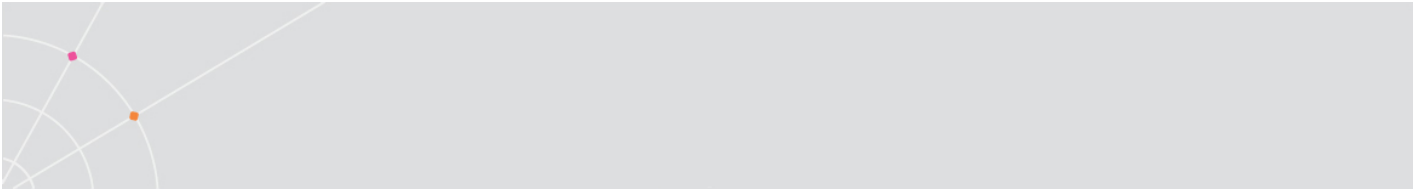
Try a different *Authentication Method* and test again.

HINT Use telnet to verify port connectivity between the Authentication Server and the 2FA server

Click *Save* to apply the settings on the Authentication Server

Changing the title of the Radius login prompt

The title of the RADIUS login prompt may be customized to describe the 2FA system that is being used. To set this label, configure the *Service Description* in the Authentication web console.



Update succeeded

Enter your RADIUS settings

RADIUS enabled

Server Address

Service Description

The next time a user authenticates with a supported WebConnect client, the new label will be displayed:

Two Factor Login

Passcode

Logging in using 2FA (Password/PIN setting)

2FA support is available with AccessPortal and AccessPad 3.3.1 and higher. Users will login using their Active Directory (LDAP) credentials at the initial login prompt:

ERICOM ACCESS DONE RIGHT

AccessPad

RADIUS Login

Please enter the host name or IP address of Ericom Server and your network credentials

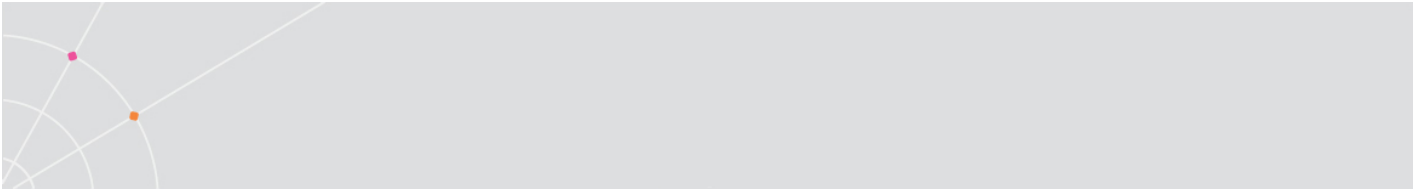
Server: webconnect.acme.com

User name: abc@acme.com

Password:

Login

And then the RADIUS passcode prompt will appear:



If both entries are valid, the user’s resource list will be displayed.

If either authentication fails, the error message below will be displayed and the user will have to attempt the login again.

Reason: Ericom Authentication Server error (code 10030002):
Authentication error: ACCESS_REJECT

Disabling Non-supported Clients

Authentication Server is designed to only work with AccessPad 3.4 (and higher), AccessPortal 3.4 (and higher), WebConnect Mobile Client 3.5 and higher, and AccessToGo 3.5 (and higher). Older WebConnect clients that do not support Authentication must be disabled to ensure robust security.

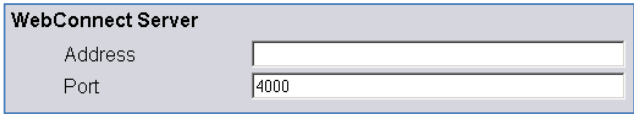
NOTE The instructions below require that all connections from AccessPad and AccessPortal are originating from the Secure Gateway

Disabling Application Portal

- Delete the *AppPortal* folder or move it to a location on the web server such that it is not accessible from the ESG.
- Edit the *PtServer.ini* file and ensure that the *Machines* setting is set to only *localhost* or *127.0.0.1*

Disabling Application Zone

- Login to the Secure Gateway Admin console and go to the Connection Broker dialog
- Remove the WebConnect Serer Address and click Save



Disabling AccessToGo (versions prior to 3.4)

- Open the file: *..\Program Files (x86)\Ericom Software\WebConnect 6.0\web\AppPortal\AccessToGo\web.config*
- Find `<add key="AcceptOldClients" value="True" />`
- Change the *value=* to *False* then save the file (*isreset.exe* not needed).



19. TERMINAL EMULATION WITH HOSTVIEW

Introduction

PowerTerm WebConnect HostView provides Terminal Emulation for legacy servers (i.e., IBM AS/400, UNIX, AIX, etc.) The following features of the terminal emulator can be modified centrally using the Administration Tool:

- Menus and menu options: Entire menus or specific menu commands can be hidden from specific users.
- Screen attributes such as display colors, number of rows and lines, cursor shape, and tab stops can be configured differently for each user and group type.
- Function buttons: There are two types of function buttons. Power Pad is a floating panel of buttons that the user can position manually on the screen. Soft Buttons are functions Buttons (Soft Keys) that are fixed to the bottom of the emulation screen.
- Keyboard mapping: Traditional terminal keys can be mapped to the physical system keyboard. Keyboard mapping also maps automated functions (also known as macros).

Configuring Legacy Connections

Legacy host connections are configured using the Administration Tool.

Creating a Legacy Host Connection

- Select Action | New | *Host Connection*. The *New Connection* dialog appears.

- Configure the legacy host's Connection properties:

- Click *OK* and the new connection will be created and added to the list of connections. Any user that has been assigned to the connection will also see it in their Application Zone automatically.

Copy a connection based on an existing one:

- Select a Connection to be copied and right-click it; then select *Copy*. The Copy Connection dialog will appear.
- Type in a new Connection Name.
- Click *OK*. The new connection will be created and the *Connection Properties* dialog will appear.
- Make necessary modifications. Verify that the *Display Name* is unique and then enable the connection.
- Click *OK*. The new connection appears with its own unique properties in the *Connection* pane.

NOTE A copied connection is initially disabled. It must be manually enabled for users access it. Go to the Connection's Properties | Information | Advanced button to *enable* the application.

Enable this Application



Testing a connection:

- Right-click on the connection in the *Connections* pane and select *Test*. The *Login* dialog appears.
- Provide a valid password and click *OK*. The desired host connection will be launched.

NOTE Testing the connection helps ensure that it is working properly before deployment to end-users.

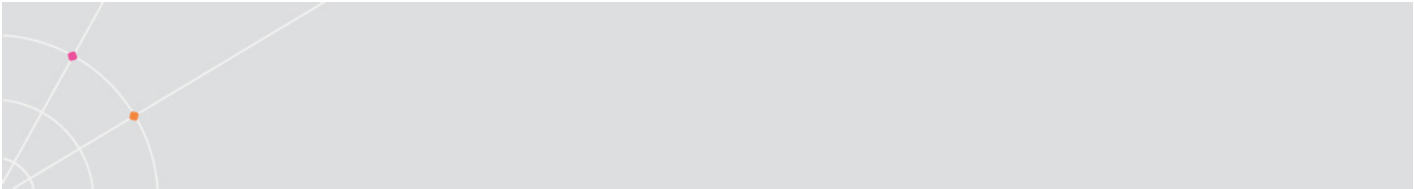
Modifying connection settings:

- Select the desired connection and right-click it; then select *Properties*. Or, select *Action | Properties*. The *Connection Properties* dialog is displayed.
- Make any modifications.
- Click *OK*. The new modifications will take effect.

Legacy Connection Properties

- **Connection Name:** Unique identifier used by PowerTerm WebConnect
- **Display Name:** Title of the connection displayed to the end-user. This value does not have to be unique, although it is recommended to avoid end-user confusion.
- **Settings button:** Displays the *Settings* dialog which configures the emulation window's appearance and behavior.
- **Key Mapping button:** Drag and drop keyboard mapping feature.
- **Power Pad button:** Programmable buttons to map commands and scripts.
- **Login Script:** Opens a text window to add scripts to be run after communication is established by the emulation client.
- **Memo button:** Opens a text file to track information for the connection.
- **Publishing button:** Determines where to place shortcut icons on the user's desktop.
- **Up and down arrows:** Clicking these arrows switches to the previous (up) or next (down) object.

NOTE The arrows are not displayed in the *Add Connection* dialog when you create a new connection.



NOTE If the next connection is a RemoteView connection, the Properties page will be displayed.

- OK and Cancel buttons: Save or discard your changes (respectively), and close the dialog box.

Deleting a connection

- Select a Connection to be deleted and right-click it; then select *Delete*. A confirmation message appears.
- Click *Yes* to delete the connection permanently.

Disabling a connection

- Select a Connection to be disabled and right-click it; then select *Properties*. The Connection Properties dialog appears.
- Clear the *Enabled* checkbox.
- Click *OK*. The connection is now disabled.

Enabling a disabled connection

- Select a Connection to be enabled and right-click it; then select *Properties*. The Connection Properties dialog appears.
- Select the *Enabled* checkbox.
- Click *OK*. The connection is enabled.

NOTE When a connection is deleted or disabled the user will no longer be able to access it. If the connection will be used at a later point, disable the connection rather than delete it. A disabled connection can be re-enabled.

NOTE If a parent connection is disabled, its child connection will also be implicitly disabled. (A child connection is a connection that has another connection as its owner.)

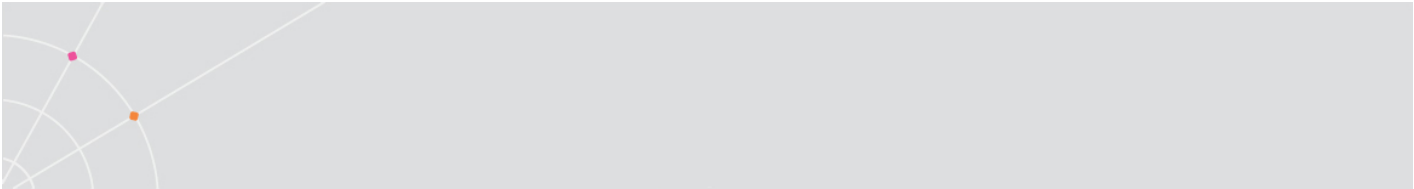
PowerTerm WebConnect HostView Settings

To configure settings at the user level:

- Double-click the desired User. The *Properties* dialog is displayed.
- Click the *Settings* button. The *Terminal Setup* dialog is displayed.
- Configure desired settings.

To configure settings at the group level:

- Double-click the desired Group. The *Properties* dialog is displayed.

- 
- Click the *Settings* button. The *Terminal Setup* dialog is displayed.
 - Configure desired settings.

To configure settings at the connection level:

- Double-click the desired Connection. The *Properties* dialog is displayed.
1. Click the *Settings* button. The *Terminal Setup* dialog is displayed.
 2. Configure desired settings.

To configure settings at the server level:

- Select Server | *Default Settings*. The Terminal Setup dialog is displayed.
- Configure desired settings.

Keyboard Mapping

It may be necessary to map host terminal keys to the PC keyboard to properly emulate the original terminal. Any keyboard key may be configured to emulate a key, macro, or script. The keyboard mapping definitions are stored in a file with the same name as the current terminal setup file, but with the extension *.ptk*. For example, the default keyboard mapping definitions are stored in a file named *ptdef.ptk*. The setup files are stored on the PowerTerm WebConnect server. End-users can load their own settings if they have the proper permissions (i.e., member of Super Users group).

To view key mapping configuration:

- Right click on the connection to be configured and select *Properties*. The Connection Properties dialog will appear.
- Click the *Key Mapping* button.
- Move the mouse over the different keys. The bottom line of the dialog shows the corresponding PC and terminal keys.

HINT Point to the "t" key of the VT keyboard and the corresponding PC key "T" will be displayed. Use this to track existing key mappings.
--

To map a PC key with a host key:

Using the Key Mapping window, drag a key from the upper *Terminal Keyboard* to the desired key on the lower *PC Keyboard*.

Click the <Control> key on the *terminal* keyboard to display additional key options.

HINT Click the <Shift> key and the alphabet keys on the terminal keyboard will be displayed in upper case. These keys can also be assigned or mapped.

To map combinations of Alt, Ctrl, and Shift keys

Using the Key Mapping window, click any combination of <Alt>, <Ctrl>, or <Shift> key on the *PC Keyboard*.

Drag the desired key from the *Terminal Keyboard* to the desired key combination on the *PC Keyboard*.

To copy a PC key to another PC key

Using the Key Mapping window, hold the <Ctrl> key while dragging the desired PC key to the PC key to be mapped. Both keys now have the same functionality.

To replace a PC key with another PC key

Using the Key Mapping window, drag the desired PC key onto the PC key that will be replaced (mapped).

To restore a PC key to the default value

Using the Key Mapping window, drag the desired PC key to the wastebasket icon. This restores the default function of the PC key.



To restore the default keyboard mapping of all mapped keys

Using the Key Mapping window, click the *Clear All* button.

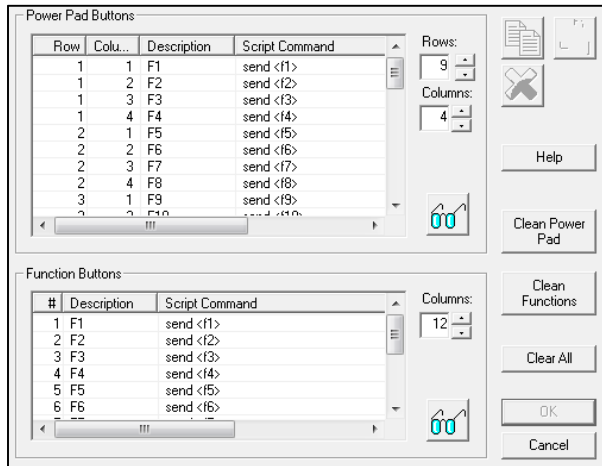
To assign a script command (macro) to a PC key

- Using the Key Mapping window, right-click a key on the PC keyboard to be assigned, and select Enter Script Commands. The PC Button dialog appears.
- Enter the script (PSL) command and click OK. The PC key has now been assigned a script command.

Power Pad

The Power Pad is a floating keypad with programmable buttons. The buttons are by default named F1, F2, F3, etc., with a few default functions, such as Clear, Enter, and Insert. The number of displayed buttons and their names can be modified.

The Power Pad can be defined at the server's level or at the connection level.



To open the Power Pad & Function Buttons at Server's Level

Select Server | *Default Power Pad*. Configure as needed.

To open the Power Pad & Function Buttons at Connection Level

- Select the HostView connection to be configured.
- Right-click the connection and select *Properties*. The Connection Properties dialog appears.
- Click the *Power Pad* button. The Power Pad & Function Buttons dialog will appear.

To program the Power Pad

- Double-click the row/column line for the button to be programmed. The *Power Pad Button* dialog appears.
- Enter its Description and Script Command.

HINT To hide the PSL command, add an asterisk to the beginning of the command.

3. Click OK.

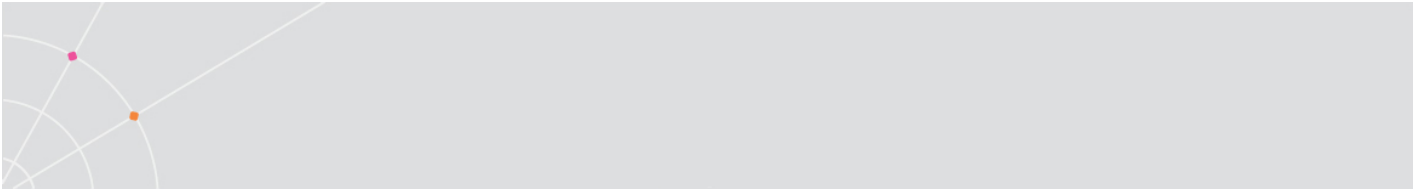
To reset the Power Pad

- Click the *Clean Power Pad* button.
- Click *Yes* at the confirmation prompt to restore the default values.

To adjust the number of buttons in the Power Pad

Enter the desired number of *Rows* and *Columns* to appear in the Power Pad.

NOTE There is a maximum of 10 rows and 10 columns in the Power Pad. The default is 9 rows and 4 columns.



Function Buttons

Along the bottom of the PowerTerm emulation window are Function buttons. By default, these are configured for F1, F2, F3, etc. These can be renamed and programmed to execute custom scripts. The Function buttons can be defined at the server's level or at the connection level.

To open the Power Pad & Function Buttons at Server's Level

Select Server | *Default Power Pad*. The Power Pad & Function Buttons will appear.

To open the Power Pad & Function Buttons at Connection Level

- Select the HostView connection to be configured.
- Right-click the connection and select *Properties*. The Connection Properties dialog appears.
- Click the *Power Pad* button. The Power Pad & Function Buttons dialog will appear.

To program the Function buttons

- Double-click the row/column line for the button to be programmed. The *Function Button* dialog appears.
- Enter its Description and Script Command.

HINT To hide the PSL command, add an asterisk to the beginning of the command.

4. Click *OK*.

To reset the Function buttons

- Click the *Clean Functions* button.
- Click *Yes* at the confirmation prompt to restore the default values.

To adjust the number of Function buttons

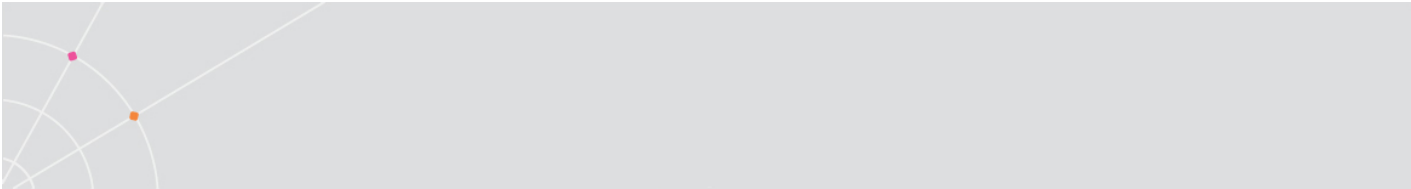
Enter the desired number of *Columns* to appear for the *Function Buttons*.

NOTE There is a maximum 24 columns in the Function Button bar. The default is 12 columns.

Custom Background Bitmap for HostView

Add a custom background image in HostView

- Select Files | *Put Background Bitmap*. The Select Background Bitmap File dialog will appear.



- Find and select the desired bitmap file.
- Select the desired file and click Open. The custom bitmap is now configured as the Server default.

To change the background image:

- Go to Server | *Configuration*
- Set the Background Bitmap File Name

Background Bitmap File Name:

20. QuickFTP

QuickVNC is centrally managed by the PowerTerm WebConnect server, so some settings are not configurable by the end-user. It can only be launched via the Application Zone. The Application Portal and AccessPad are not supported.

Installing QuickFTP

In order to use QuickFTP, the end user must install the component onto the local system. The installer may be obtained from the PowerTerm WebConnect server at this path:

```
C:\Program Files (x86)\Ericom Software\WebConnect 6.0\AddOns\QuickFTP
```

Launching QuickFTP

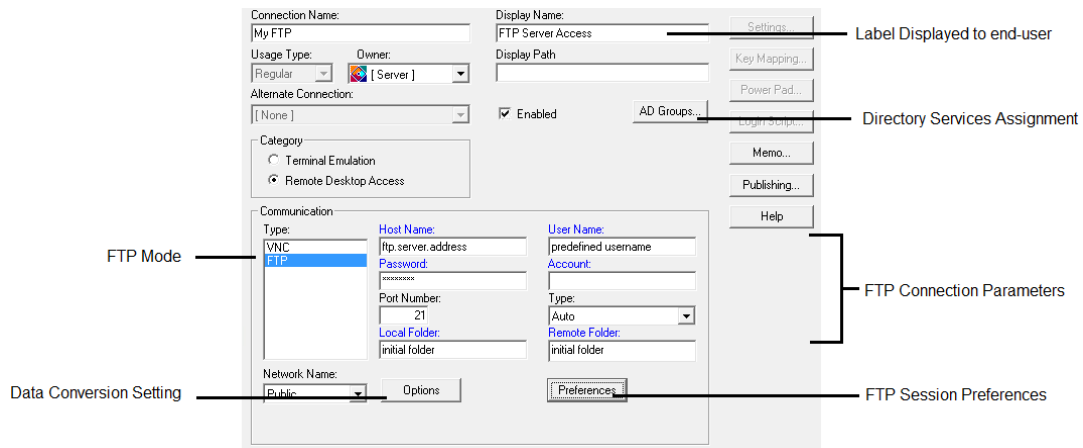
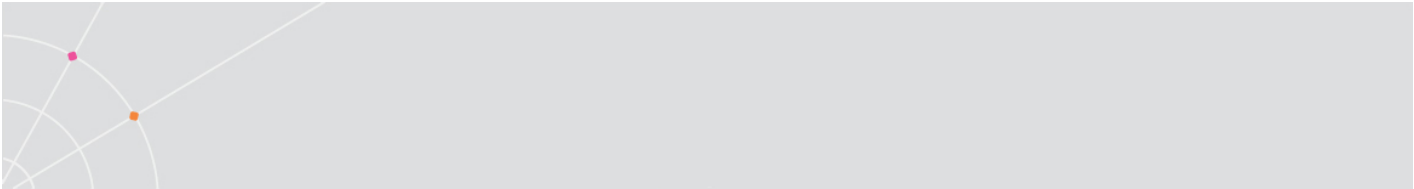
Published QuickFTP connections will appear in the user's Application Zone, AccessPad, or Application Portal once assigned. It may only be launched from the Application Zone.



QuickFTP connections are configured and published by the PowerTerm WebConnect Administration Console. The publishing steps are very similar to publishing a *HostView* connection.

To begin, in the Administration Console go to Action | New | *Host Connection*.

Select *Remote Desktop Access* and *FTP* as the Communication type. Configure the settings as desired and click OK to create the new FTP connection.



STOP All QuickVNC connections MUST have a username and password predefined. This cannot be entered manually by the end-user.

Using QuickFTP

When a QuickFTP connection is launched, the component will connect to the FTP site as configured centrally on the PowerTerm WebConnect server. Once the FTP connection is established, the FTP user interface will appear.

Start by selecting *Copy* or *Append* (Default is *Copy*).

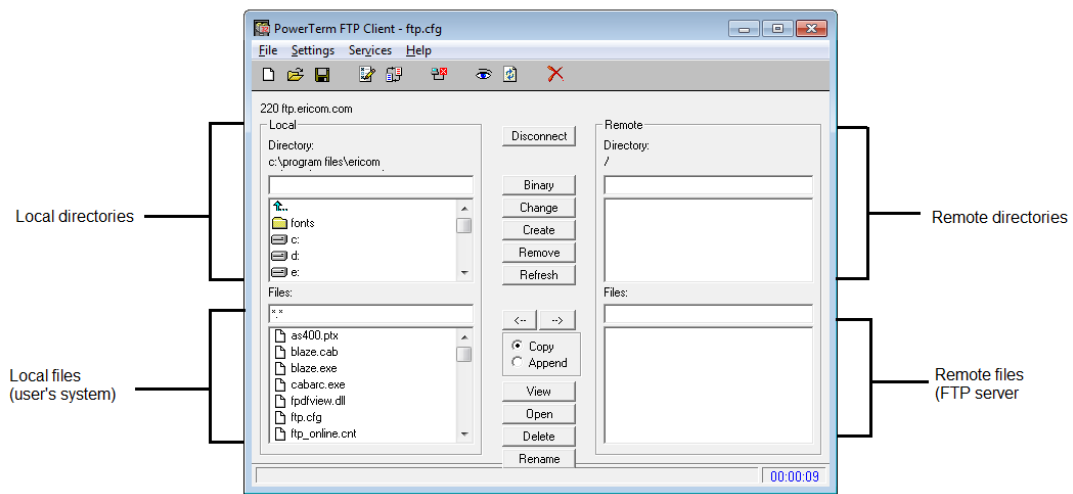
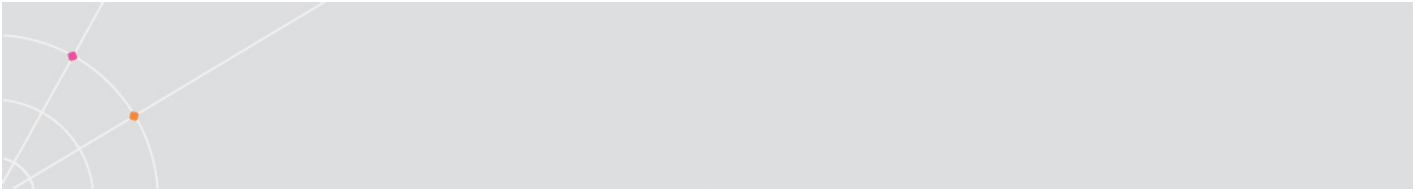
Next, set the transfer type to *Ascii* or *Binary* by clicking the *Transfer Type* button (Default is *Ascii*). This can also be set under Settings | *Transfer Type*.

Navigate to the desired source and destination folders for the file transfer.

To download files, select the desired files to be transferred from the file list under *Remote* and click the left arrow button.

To upload files, select the desired files to be transferred from the file list under *Local* and click the right arrow button.

HINT Depress the control (CTRL) key while clicking files with the mouse to select more than one file for transfer.



NOTE The directory and file panes do not support drag and drop. Select desired files by navigating to the appropriate directories.

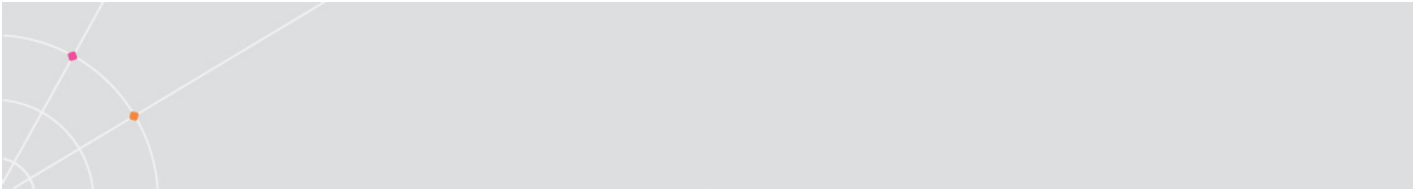
Click the *Disconnect* button to disconnect from the FTP site. From the File menu, select *Exit* to exit the application.

Menu Items

<i>File</i>	Create, open and save a configuration. Exit FTP client
<i>Settings</i>	Select preferences for file transfer data translation mode
<i>Services</i>	Display the FTP log; refresh the file list in both the local and remote directory; open the <i>Connect</i> dialog.

Toolbar

<i>New</i>	Create a new configuration file
<i>Open</i>	Open an existing configuration file
<i>Services</i>	Display the FTP log; refresh the file list in both the local and remote directory; open the <i>Connect</i> dialog.
<i>Save</i>	Saves a configuration file
<i>Preferences</i>	Displays current session preferences
<i>File Transfer Setup</i>	Select options for data conversion.



<i>Connect</i>	Enter connection parameters for file transfer
Log Window	Displays FTP session details
<i>Close</i>	Exit the FTP client



21. IMPROVING PERFORMANCE

This chapter provides best practice recommendations for optimizing PowerTerm WebConnect and Terminal Server performance.

Using a Dedicated Server

For optimal performance, install PowerTerm WebConnect on a dedicated server. Installing PowerTerm WebConnect on a server with heavy load will adversely affect performance of the server. PowerTerm WebConnect should not be installed on a server running any of the following:

- Microsoft Active Directory or any other directory service
- Microsoft Exchange or any other mail server
- Microsoft Terminal Server or Citrix Presentation Server
- Corporate Web server
- Any server under constant heavy load

<p>NOTE For prototypes and small to medium sized deployments, installing PowerTerm WebConnect on a Terminal Server is most practical.</p>
--

Running PowerTerm WebConnect separate from the Web Server

The PowerTerm WebConnect installer assumes that there is a web server on the same system. It is possible to host the *web* folder on a web server external to the PowerTerm WebConnect server.

Memory Resources

For optimal performance ensure that the PowerTerm WebConnect has sufficient resources. It is important to allocate sufficient memory for the PowerTerm WebConnect server, and to ensure that the server does not need to use the virtual memory swap file.

Use the server's Performance Monitor to monitor the system's performance and resource usage over time. Inspect memory related statistics such as *Memory\Pages/sec* and *Memory\Page Faults/sec*. High values indicate that more RAM is needed as memory is constantly swapped to and from the disk.



Alternate Connection Points

The default installation assigns the main connection point to the first known IP address of the computer and port 4000. These values are specified in the *Address* and *PortNo* entries of the [*ConnectionPoint*=name] section, in the server's Main Configuration (PtServer.ini).

Additional connection points can be added by simply copying an existing connection point and modifying the values. Connection points allow connections to the PowerTerm WebConnect server through additional ports.

EXAMPLE – in this connection point the server address is configured as 126.1.1.177 and the port of 443 will be used to accept connections to PowerTerm WebConnect. Only SSL connections will be accepted via this port.

- [ConnectionPoint=Secured]
- *Address*=126.1.1.177
- *PortNo*=443
- *SSL-Required*=True
- *LoginRequestTimeoutSeconds*=10
- *EchoTestFrequencySeconds*=60
- *EchoTestTimeoutSeconds*=30
- *KeepAlive*=False
- *UseConnectingMachineName*=True

<p>HINT When adding a new connection point, ensure that the server firewall allows traffic through the new port. Also verify that there is not another service on the server already using the port.</p>

After configuring Connection Points, restart the PowerTerm WebConnect Server service.

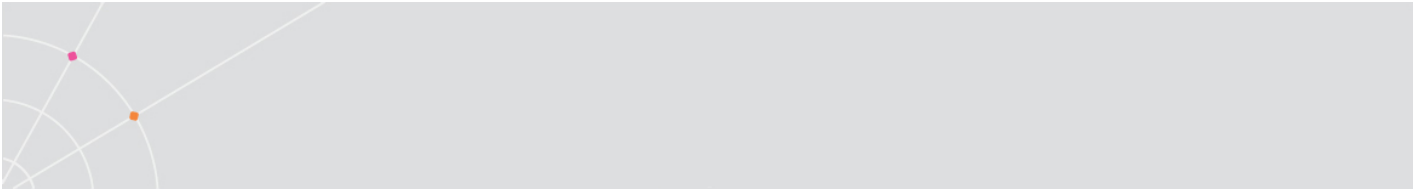
Best Practices for a Healthy Environment

Do not use vendor-supplied defaults for system passwords and other security parameters

Ericom recommends changing the password for the PowerTerm WebConnect Administration Console immediately after installation. The default password is <blank>.

Uninstall unused applications from Terminal Servers

Keep Terminal Servers optimized by not installing extraneous applications. Uninstall applications that are no longer used. Terminal Servers are accessed



by many users each day and should be optimized to run applications that are needed the most.

Virtualize servers to ease the backup and rollback process

Before making significant changes to any server (i.e. upgrading WebConnect) take a snapshot of the server. This will create an image of a “working” server and provide a simple method of rolling back the server.

Develop and maintain secure systems and applications

An Ericom PowerTerm WebConnect Terminal Server environment stores all data within the datacenter (minimizes impact of critical data loss due to equipment theft). Centralized data sources are easier to maintain and secure. Manage redirection features to meet security standards; such as disabling file upload and download to the Terminal Server.



22. IMPLEMENTING ACCESS SECURITY

An effective server access solution must ensure that critical computing systems are not compromised. This is especially important when access to these systems is extended beyond the local network to areas not managed by the IT department. PowerTerm WebConnect provides features to secure access to published applications and desktops.

Encrypting with SSL

PowerTerm WebConnect uses Secure Socket Layer (SSL) for establishing secure communication between the PowerTerm WebConnect server and the clients.

PowerTerm WebConnect supports three levels of communication security:

Unsecured (No SSL): Communication between the server and the client is not secured by PowerTerm WebConnect. For example, Telnet communication is transmitted as clear text, including user names and passwords.

Encryption without Authentication (Anonymous SSL): SSL is used for encryption only. The client will not verify the PowerTerm WebConnect server's identity. This is the default security level used by PowerTerm WebConnect.

Fully Secured (SSL with Server Certificate): SSL is used to both authenticate the server when communication is established, and to encrypt the communication data stream. In order to use this level of security, a certificate and primary key, must be placed on the server. The client will access a copy of the certificate from a source (file system, a Web server, or an FTP server) and will use it to verify the server's certificate. The certificate can also be downloaded from the PowerTerm WebConnect server and saved on the client's machine upon receiving confirmation from the end-user.

<p>NOTE The security level of the communication between the PowerTerm WebConnect server and clients, does not affect the security of <i>direct</i> connections between clients and hosts. Direct connections are independent of PowerTerm WebConnect security and handled by its protocol (i.e., RDP).</p>

Configuring No SSL Security Level


Client side configuration

Add the following parameter to the command line (i.e., ApplicationZone.html): `/NOSSL`

Server side configuration

Using the Administration Tool, go to File | Configuration | *Main* (PtServer.ini).

Set *SSL_Required*= to *False*. This will allow the server to accept unsecured client connections.

To verify that no SSL is used, go to the *About* dialog on the client side (i.e., Application Zone) and there will be no lock icon .

NOTE To disable compression set *UseCompression=False*

Configuring Anonymous SSL Security Level

Client side configuration

Add the following parameter to the command line (i.e., ApplicationZone.html): */SSL*

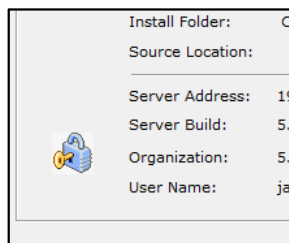
Server side configuration

Verify that the pair of security files (*PTS.crt* and *PTS.key*) are not in the same folder as *PtServer.exe*. If they are located in the same folder, the server will use them for authentication. If they are not in the folder, the server will use anonymous SSL.

Using the Administration Tool, go to File | Configuration | *Main* (PtServer.ini).

Set *SSL_Required*= to *True*. Now PowerTerm WebConnect will only accept SSL connections.

To verify that SSL is used, go to the *About* dialog on the client side (i.e., Application Zone) and verify the presence of the lock icon.



Configuring SSL with Certificate Security Level

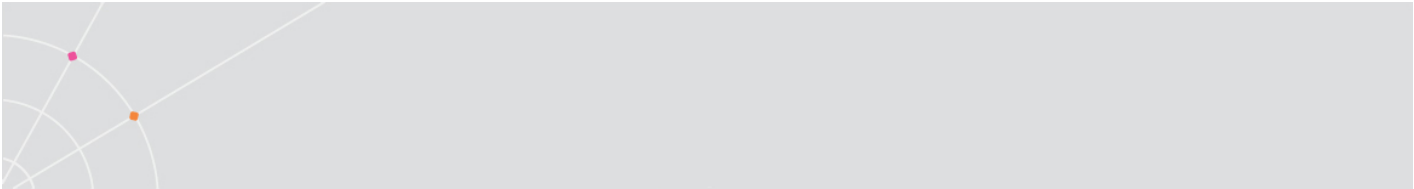
Client side configuration

Add the following parameter to the command line (i.e., ApplicationZone.html): */SSLCERTFILE* or */SSLCERTPATH*

/SSLCERTFILE is used to reference specific certificate files.

/SSLCERTPATH is used to reference a folder containing one or more certificate files.

The certificate filename or path is configured as follows:



/SSLCERTFILE=filename or /SSLCERTPATH=path

NOTE The certificate path is not searched recursively

Using multiple certificates

Both command line parameters can reference multiple files or paths:

/SSLCERTFILE="file1;file2;file3"

/SSLCERTPATH="path1;path2;path3"

Server side

Verify that the pair of security files (*PTS.crt* and *PTS.key*) are placed in the same folder as *PtServer.exe*. If they are not in the folder, the server will use anonymous SSL.

Using the Administration Tool, go to File | Configuration | *Main* (*PtServer.ini*).

Set *SSL_Required=* to *True*. Now PowerTerm WebConnect will only accept SSL connections.

NOTE The first time the certificate files are placed in the server's folder (and anytime they are replaced) the PowerTerm WebConnect Server service must be restarted.

If the server's certificate does not match the certificate file referenced by */SSLCERTFILE*, or is not located in a directory referenced by */SSLCERTPATH*, the connection is rejected.

To override this operation place an asterisk (*) in front of the certificate file name, or directory path. In this case, if the file does not exist or does not match the server's certificate, the server's certificate is presented to the user. If the user accepts the certificate, it is saved and the connection will be established. If a file name is provided without specifying a folder, the file will be saved to *Ericom-folder/certificates*.

NOTE Distributing a certificate in this manner is less secure than manually placing them on the client computer (there is no way to verify the source of the certificate.)

If the *SSLCERTFILE* file name is not specified, a search in the default folder will be conducted for the following:

ServerName=ServerIP-ServerPort.crt

Example: *steven= 127.0.3.37-4000.crt*

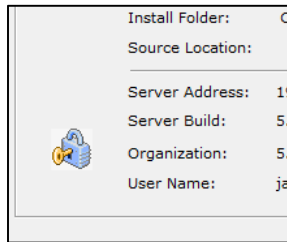
Ericom-folder is a private user folder. It is located under the user's profile (i.e., *C:/Documents and Settings /User-Account-Name/Application Data/Ericom*)

For certificate authentication, place the CA certificate in the web side root folder and specify its path in the following manner:

`https://webserver/WebConnectV.v/server.crt`

Example: `https://www.customer.com/WebConnect5.1/server.crt`

To verify that SSL is used, go to the *About* dialog on the client side (i.e., Application Zone) and verify the presence of the lock icon.



SSL with Server Certificate (Administrative Access)

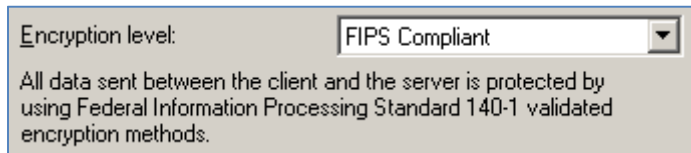
In the *Connect* dialog of the Administration Tool, the Administrator can connect to a server without a certificate. During a connection attempt, a dialog will appear stating the file name and path of the certificate that the Administration Console failed to find.

The administrator can choose one of the following options:

- Reject this certificate
- Accept this certificate
- Accept and Save this certificate to the specified server location

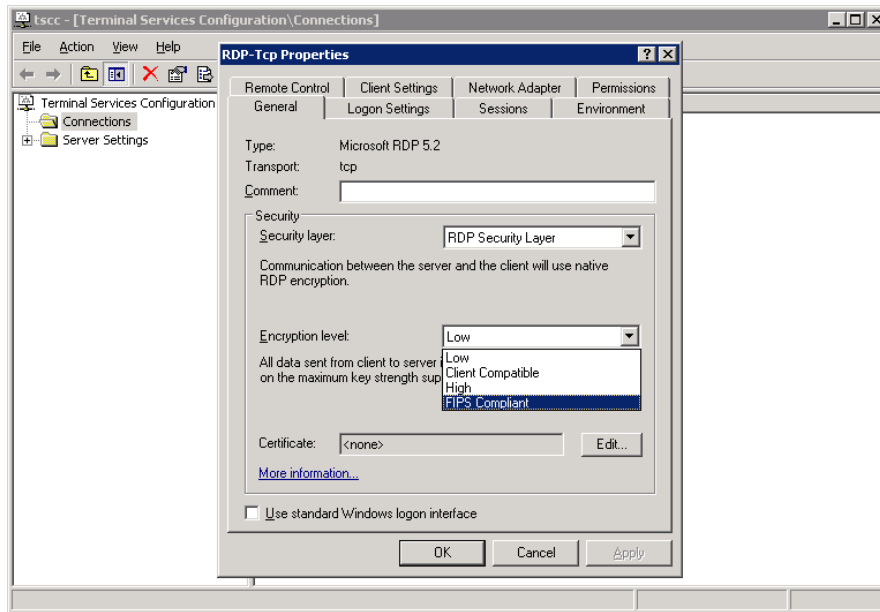
Enabling FIPS Compliancy in RDP

FIPS compliancy is supported by the RDP protocol. This is a vital feature when sensitive data (i.e., credit card information) is sent over public networks. FIPS is enabled using the Terminal Services (Remote Desktop) Host Configuration.



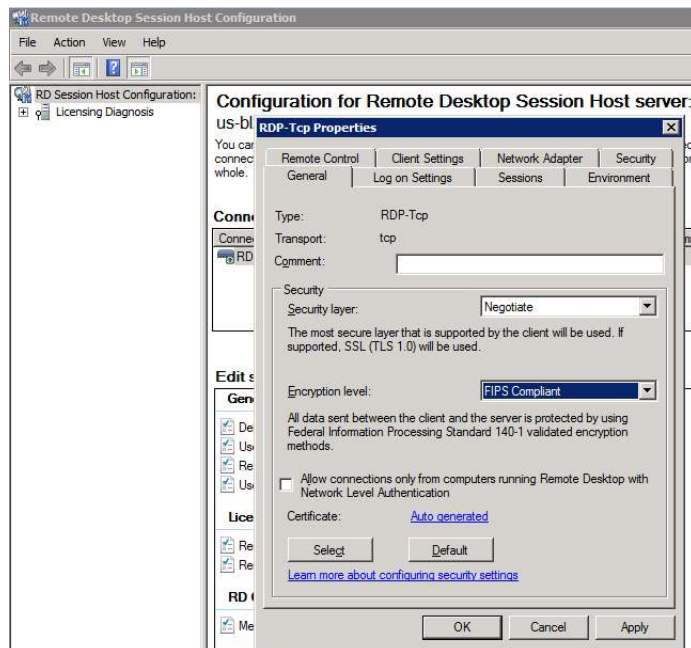
To enable FIPS Compliancy on Windows 2003 Terminal Servers:

- Open Terminal Services Configuration.
- Double click on RDP-Tcp and go to the General tab.
- Change the Encryption level to FIPS Compliant.



To enable FIPS Compliance on Windows 2008/R2/2012 Terminal Servers:

- Open Remote Desktop Session Host Configuration.
- Double click on RDP-Tcp and go to the General tab.
- Change the Encryption level to FIPS Compliant.



NOTE Blaze connections do not support FIPS.

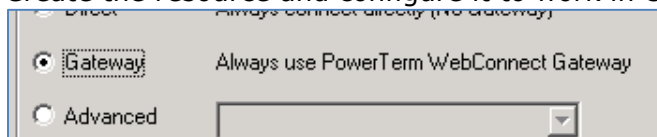
Secure Access Based on Subnet

PowerTerm WebConnect includes functionality to limit access to published resources based on the user's subnet.

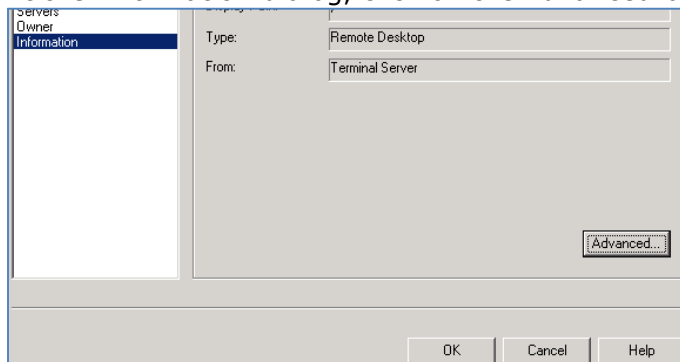
Use a dedicated ESG for the desired subnet of users

Create a dedicated ESG and give it an address that only the computers in the subnet can recognize (e.g. add the address to the local HOSTS file).

Create the resource and configure it to work in *Gateway* mode.



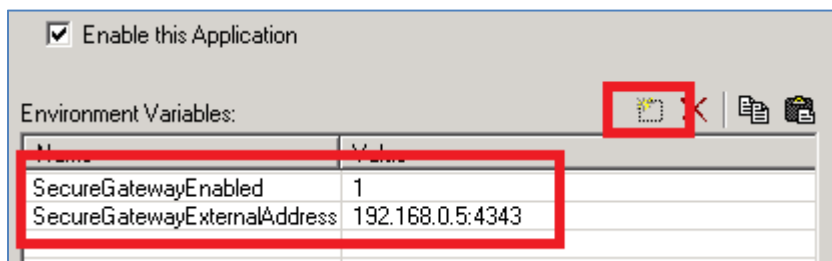
At the *Information* dialog, click on the *Advanced* button



Click on box icon to add new variables. Add the following two variables:

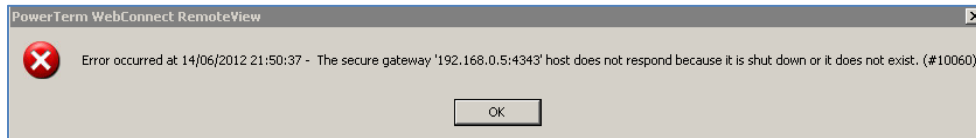
SecureGatewayEnabled = 1

SecureGatewayExternalAddress = 192.168.0.5:4343 (the target ESG address)



Click *OK* and then *OK* again to close out of the *Properties* (and save the new settings).

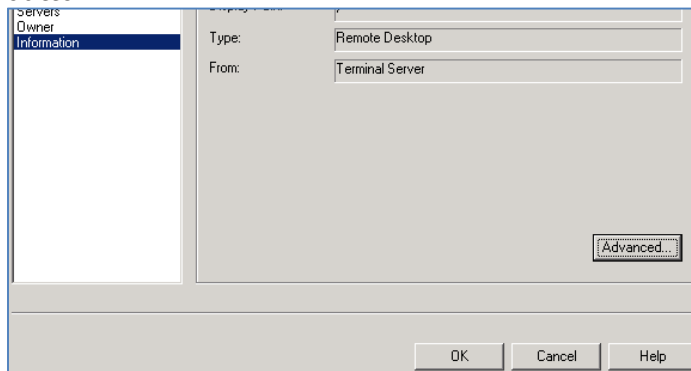
When a user tries to connect from a machine that does not recognize the target ESG, the following error will be returned.



Deny access outside of a specified subnet

Make sure that the Terminal server can be accessed **directly** from the desired users (e.g. a VPN tunnel is established).

Create the application and at the *Information* dialog, click on the *Advanced* button:



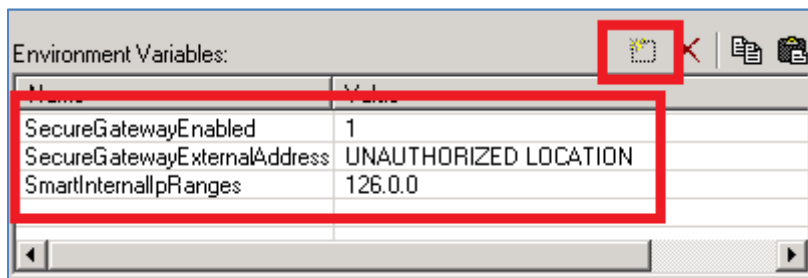
Click on box icon to add new variables. Add the following three variables:

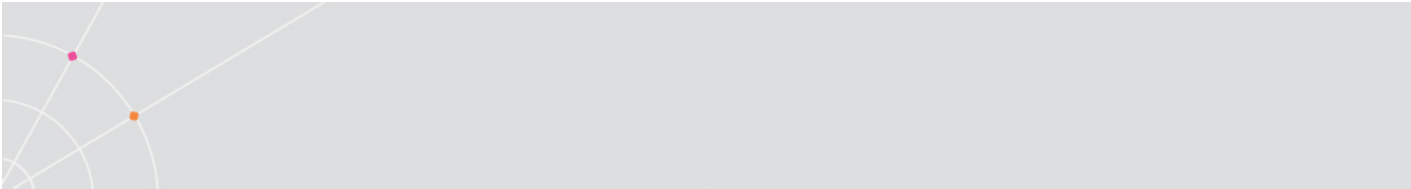
SecureGatewayEnabled = 1

SecureGatewayExternalAddress = UNAUTHORIZED LOCATION (or the message of your choice)

SmartInternalIPRanges = the subnet that will have direct access to the TS (126.0.0 will include all addresses 126.0.0.*)

NOTE This method is not strongly secured because if the user goes home and matches their subnet to the configured one, the user will be able to connect from an unauthorized location. Try to give the desired subnet something non-standard (such as 172.10.2)

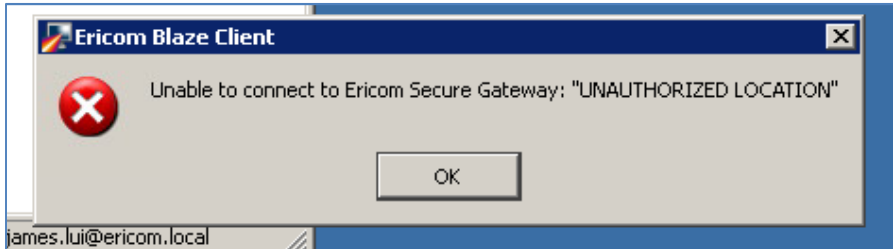




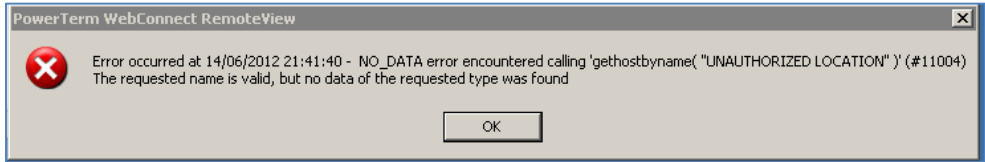
Click *OK* and then *OK* again to close out of the *Properties* (and save the new settings)

When the user tries to connect from an IP outside of the range, one of the following messages will appear:

Blaze session error:



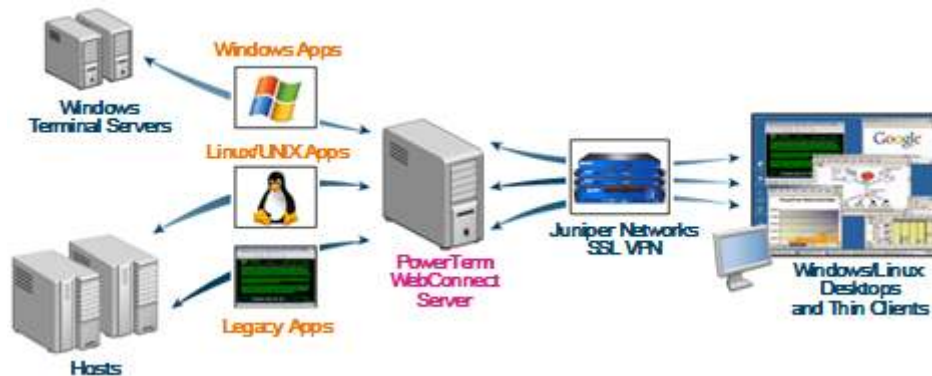
RDP session error:



23. JUNIPER[®] SSL VPN INTEGRATION

Juniper Network's SSL VPN solution, in conjunction with Ericom's PowerTerm WebConnect, provides secured remote access to mission critical applications, ensuring a cohesive and complete Server Based Computing environment.

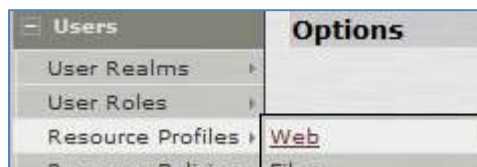
Juniper SSL VPN version 7.4 R1 or higher supports Websockets in the rewriter. This feature allows Ericom's AccessNow HTML5 to communicate natively using just the rewriter so no component downloads are required whatsoever. This configuration is recommended for most deployments as it will work with the most type of devices: tablets, PC's, Mac's, Chromebooks, etc.



General Portal Configuration

Add Profile in Juniper

To display the PowerTerm WebConnect Portal inside the Juniper web interface, create a new Juniper *Resource Policy*, and select *Web*.



Click *New Profile* and define the settings to the URL of the PowerTerm WebConnect Application Portal.

Base URL: <http://server.test.local/webconnect/AppPortal/index.asp>

Web Access Control: http://server.test.local/webconnect/AppPortal/*

Web Application Resource Profiles >
Production

Resource Roles Bookmarks

Type: * Custom
Name: * PowerTerm WebConnect Portal
Description:
Base URL: * /server.test.local/webconnect/AppPortal/index.asp
Autopolicies: Autopolicies are resource policies that correspond to this resource's fully qualified domain name in your base URLs.
Show ALL autopolicy types >>

Autopolicy: Web Access Control
Use this autopolicy to control access to web servers and URLs.

Delete ↑ ↓

Resource	Action
<input type="checkbox"/> http://server.test.local:80/webconnect/AppPortal/*	Allow Add

Examples:
http://*.domain.com
https://www.domain.com

PowerTerm WebConnect Configuration

Configure PowerTerm WebConnect to allow connections from the SSL VPN.

- Browse to the WebConnect *DataBase* folder. (Usually in "X:\Program Files\Ericom Software\WebConnect\DataBase", where "X" is the drive letter in which PowerTerm WebConnect is installed.)
- Open *PtServer.ini* and search for *Machines=localhost;127.0.0.1*.
- Add the server address to this line
(Example: *Machines=localhost;127.0.0.1;juniper.testdomain.com*)
- Search for the section beginning with: *[ConnectionPoint=Internet]*
- Add this line at the end of this section: *CheckIPMatch=False*
- Restart the PowerTerm WebConnect Server service.

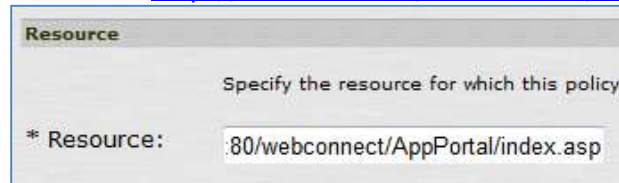
NOTE If this is not configured, users may receive an error stating *Credential Token Error*. Behavior may vary based on the version of Ericom and Juniper that are in use.

Form POST Single Sign-On with Portal

NOTE: Juniper Advanced License is required for *SSO Form POST* in the IVE platform.

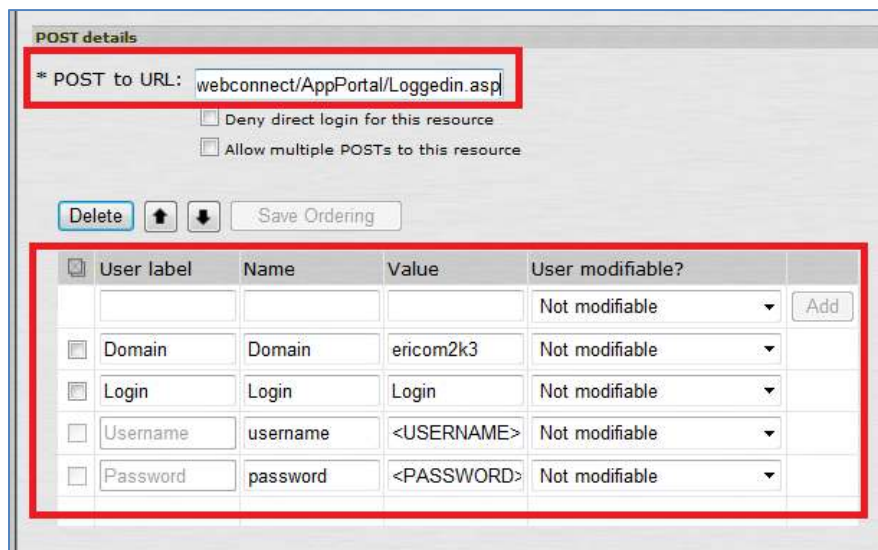
Configure the HTML Form POST to enable Single-Sign-on from the SSL VPN to the PowerTerm WebConnect portal.

- Click Users | Resource Policies | Web | *SSO Form POST* | New Policy
- Resource: <http://<server>:80/webconnect/AppPortal/Index.asp>



The screenshot shows a dialog box titled "Resource" with the instruction "Specify the resource for which this policy". A text field labeled "* Resource:" contains the value ".80/webconnect/AppPortal/index.asp".

- Roles: Select desired roles that will have access to this policy.
- POST to URL:
<http://<server>/webconnect/AppPortal/LoggedIn.asp>
- Login / Login / Not modifiable
- domain / widgets / Not modifiable
- username / <USERNAME> / Not modifiable
- password / <PASSWORD> / Not modifiable



The screenshot shows the "POST details" configuration window. The "* POST to URL:" field is highlighted with a red box and contains the value "webconnect/AppPortal/LoggedIn.asp". Below this are two unchecked checkboxes: "Deny direct login for this resource" and "Allow multiple POSTs to this resource". A "Delete" button, up/down arrow buttons, and a "Save Ordering" button are also visible. A table below is also highlighted with a red box.

User label	Name	Value	User modifiable?	
			Not modifiable	Add
<input checked="" type="checkbox"/>	Domain	Domain	ericom2k3	Not modifiable
<input checked="" type="checkbox"/>	Login	Login	Login	Not modifiable
<input type="checkbox"/>	Username	username	<USERNAME>	Not modifiable
<input type="checkbox"/>	Password	password	<PASSWORD>	Not modifiable

Set Ericom Portal Page as the Default

To set the PowerTerm WebConnect Portal page as the default Juniper page, go to the desired *User Role* and configure its *UI Options*. Set the *Custom page* to the Portal URL. If a POST SSO policy has been set for this URL, it will auto-login the user directly into the Portal.



The screenshot shows the 'UI Options' configuration page for a Juniper user role. The left sidebar contains a navigation menu with categories like Clustering, Log/Monitoring, Authentication, Administrators, Users, Maintenance, and System. The main content area is titled 'UI Options' and includes tabs for 'Session Options', 'UI Options', and 'Custom Messages'. At the top, there are 'Save Changes' and 'Restore Factory Defaults' buttons. The configuration is organized into sections: 'Header' (with 'Current appearance' set to the Juniper logo and 'Background color' set to #336699), 'Sub-headers' (with 'Current appearance' set to 'Label', 'Background color' set to #336699, and 'Text color' set to #FFFFFF), and 'Start page'. The 'Start page' section explains that it determines where a user starts after signing in. It offers three radio button options: 'Bookmarks page', 'Meetings page', and 'Custom page'. The 'Custom page' option is selected and highlighted with a red box. Below it, the 'Start page URL' is set to '34/webconnect/AppPortal/index.asp'.

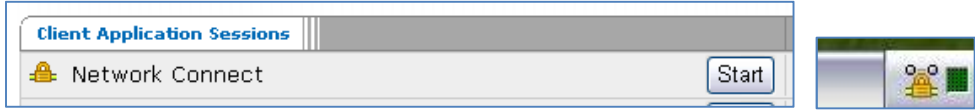
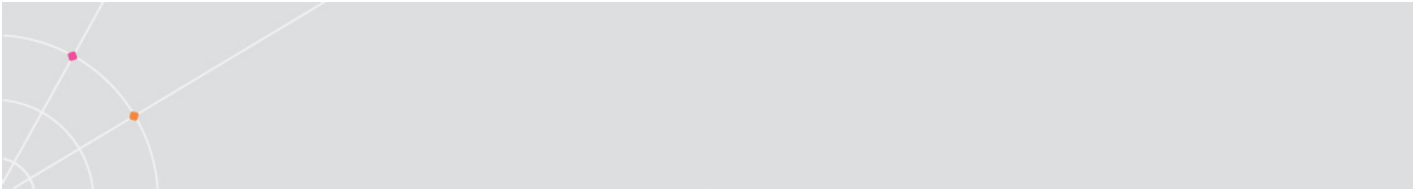
AccessNow HTML5 with Rewriter (Client-less)

Juniper SSL VPN devices running version 7.4 R1 or higher supports WebSockets natively. No additional configuration is required in the SSL VPN to use Ericom's AccessNow. Simply click on the desired connection from the Application Portal and the resource will appear as a new tab in the web browser. No client-side download or configuration is required. This combined solution will work on any device with a modern HTML5 compatible browser.

NOTE AccessNow is enabled by default in the Ericom Application Portal

Network Connect Usage (All Clients)

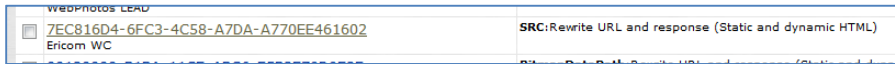
No additional configuration is needed when using PowerTerm WebConnect with Network Connect. Just make sure to launch Network Connect before launching any PowerTerm WebConnect published applications and desktops.



Set ActiveX Rewriting Parameter (Native Windows Downloader)

To configure ActiveX Parameter Rewriting (rewriting specific to Ericom's WebConnect):

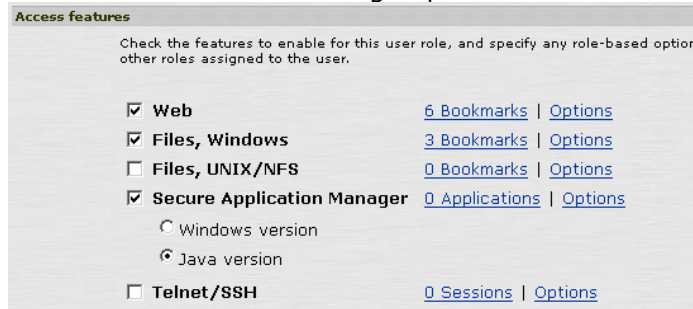
- From the Juniper IVE browse to Users | Resource Policies | Web | *ActiveX Parameters*
- Add: Class Id: **7EC816D4-6FC3-4C58-A7DA-A770EE461602**
- Parameters: **Src | Rewrite URL and response (Static and dynamic HTML)**



JSAM Configuration (Native Clients)

To configure JSAM to tunnel PowerTerm WebConnect's application traffic and ensure that the proper users have access:

- From the Juniper IVE, browse to: Users | User Roles | <role name> | General | *Overview*
- Scroll down to *Access features* section
- Select *Secure Access Manager | Java version*



- From the Juniper IVE, browse to: Users | User Roles | <role name> | SAM | *Options*
- Select *Java SAM*
- Configure JSAM Port Forwarding
 - a. From the Juniper IVE, browse to: Users → Resource Profiles → SAM → *Client Applications*

- b. Select *New Profile*
- c. Set Type to *JSAM*
- d. Set Application to *Custom*
- e. Set name to something descriptive, such as “PowerTerm WebConnect Servers”
- f. Add your PowerTerm WebConnect Server and Terminal Servers to the JSAM Port Forwarding section. The PowerTerm WebConnect Server port is 4000, and Terminal Server ports are 3389.
- g. Select “Save and Continue”

Client Application Resource Profiles >
New Client Application Resource Profile

Type: * JSAM
 Application: * Custom
 Name: * WebConnect Server
 Description:

JSAM Port Forwarding

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

Servers:

Delete				
<input type="checkbox"/>	Server Name *	Server Port *	Client Loopback IP	Client Port
<input type="checkbox"/>				<input type="button" value="Add"/>
<input type="checkbox"/>	ericomts1	4000		4000
<input type="checkbox"/>	ericomts1	3389		3389
<input type="checkbox"/>	ericomts2	3389		3389
<input type="checkbox"/>	us-mis1	3389		3389

- h. Select the *Roles* for this Resource Profile to be applied to and *Add* them to the *Select Roles* area. Click *Save*

Changes".

Client Application Resource Profiles >
WebConnect Servers

Resource Roles

Successfully created resource profile: 'WebConnect Servers'. Now select user resource profile.

Select the roles to which the resource profile applies. These roles will inherit the resource policy by the resource profile.

Available Roles:

- NC Users
- QA users

Selected Roles:

- Users Main
- Users

Add ->

Remove

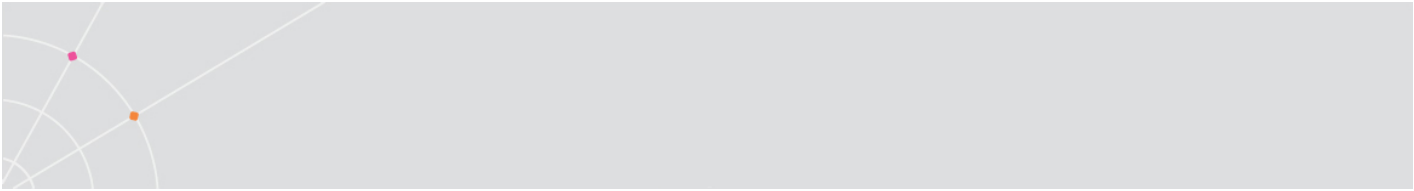
Save Changes

WSAM Configuration (Native Windows Client)

To configure WSAM to tunnel PowerTerm WebConnect's application traffic and ensure that the proper users have access:

From the Juniper IVE, browse to: Users | User Roles | <role name> | SAM | Applications

- Add Server: *server.widgets.com* (the WebConnect Server name)
- PowerTerm Port(s): 4000 (or the custom port number)
- From the IVE browse to Users | Resource Policies | SAM | Access Control | Resources: *server.widgets.com:4000* (<servername>:<port>)



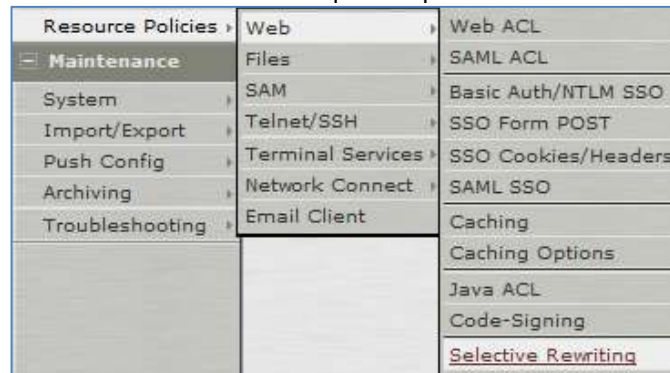
- Configure the “Allowed Servers”

- Set up Selective Rewriting policy, within the Juniper IVE, browse to Users | Resource Policies | Web | *Selective Rewriting*
- Add the server to the Initial Rewrite Policy
- Define the roles that the policy applies to.
- Select Rewrite content (auto-detect content type).
- Server gets added to Resources as: *http://server.widgets.com:*/**

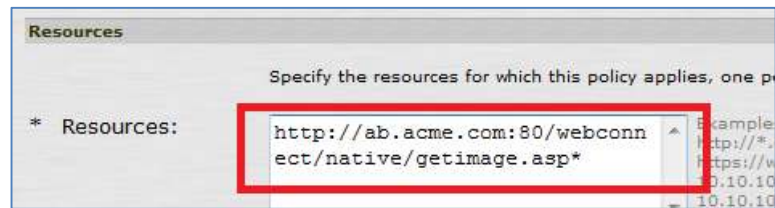
Application Portal Icons Fix

If portal icons do not appear properly in Juniper, configure a policy to not rewrite the *getimage.asp* page:

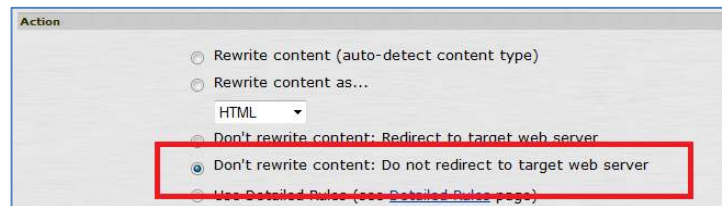
- Go to *Resource Policies | Web | Selective Rewriting*



- Enter the *getimage.asp* path for the Resource. Make sure to enter */** at the end:



- Add a new Policy with the Action: Don't rewrite to the target web server:



24. MONITORING AND AUDIT TRAILS

Monitoring Online Activity

The Administration Console provides information about user status and activities. This information is presented in two ways:

- By connection source: view status for computers, users, or groups.
- By sessions: view information about active client sessions.

Status Information for Computers, Users, and Groups

Three views report by connection source: the *Users* pane, filtered by Runtime Information; the *Groups* pane, filtered by Runtime Information; and the *Machines* window.

Identification Information Fields

The Users pane, Groups pane, and Machines window, each show runtime information for different characteristics of a connection source. The following table lists and explains all the runtime information fields, and indicates which are shown in each window (a ✓ indicates that the window shows the field).

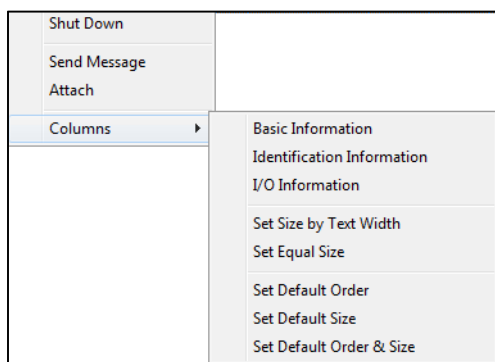
Fields displayed in the Users pane pertain to individual users; fields in the Groups pane pertain to all the users in a specific group; and fields in the Machines window pertain to all the users accessing the server from a specific computer.

Column	Description	User	Group	Machines
IP Address	IP address of the remote client.	-	-	✓
Sessions Count	Total number of sessions that are currently used by the group.	✓	✓	✓
First Entrance	The date and time of the login of the user.	✓	-	-
Last Entrance	The date and time of the last login of the user.	✓	✓	-
Logins History	The number of logins performed by the user.	✓	-	✓

Output Bytes	The total bytes of application traffic that were sent to the client.	√	-	-
Input Bytes	The total bytes of application traffic that were received from the client.	√	-	-
Output Messages	The total of application packets that were sent to the client.	√	-	-
Input Messages	The total of application packet that were received from the client.	√	-	-
Active Users Count	The total number of the group's users that are currently active.	-	√	-

Show Preset Columns Types

Right-click an *object* (not the column title) and select *Columns*



Select one of the following sets of information: *Basic, Identification, I/O Information*.

Viewing Active Sessions

In the *Client Sessions* view, a new entry is created each time a user connects to PowerTerm WebConnect and opens a new session (i.e., RemoteView, HostView, etc.)

The fields in session information table are divided into two groups: static fields that identify the session and I/O Information fields that show realtime information about the session (until it ends).

Viewing sessions for a user

Right-click on the desired user and click *Sessions*.

OR

Right-click on the user object and select *Properties*. The User Properties dialog will be displayed. Click the *Sessions* button.

View sessions opened by all users of a group

Right-click the desired group and click *Sessions*.

OR

Right-click on the group object and select *Properties*. The Group Properties dialog will be displayed. Click the *Sessions* button.

View sessions opened by all users

Select View | *Client Sessions* or click the icon.



Viewing administrative sessions

The Administrative Sessions window displays the online activity of users that have administrator status. Every entry in the table represents one administrator session, so if an administrator logs on twice, two lines are added.

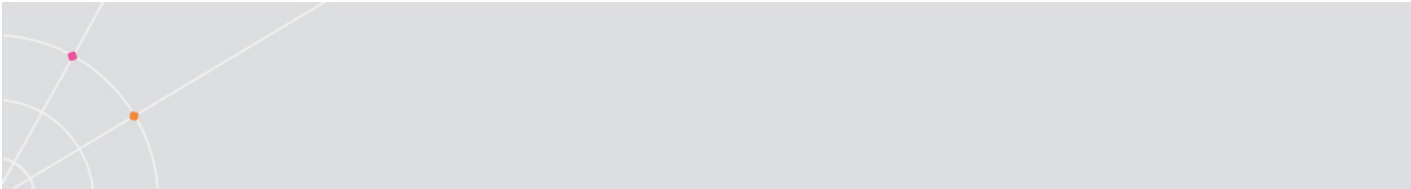
Select Views | *Administrative Sessions* or click the icon.



Viewing intruders list

The Intruders window shows suspected attempts at breaching PowerTerm WebConnect. Every entry in the table represents an instance where a user either:

- Attempted to connect using HTTP, or through an incorrect port.
- Entered a wrong password.
- Entered an unknown username.
- Entered a correct username and password, but connected from an IP or computer not specified in the user or group *Allowed List*.
- Attempted to connect from two different computers, although the *Allow Concurrent Machines* is disabled.



After several intruder attempts, users are blocked temporarily. The number of attempts and the time period of blocking are defined in the *Intruders* fields of the *Server Configuration* dialog.

In addition to showing suspected intrusion attempts, the *Intruders* window allows the administrator to remove restrictions on users. The administrator can also prevent users from being detected as an intruder in the future.

To open the *Intruders* view select *View | Intruders* or click the icon.



HINT To remove a user restriction right-click the desired user entry in the intruders table and select *Allow*. The allowed user will now be able to login to PowerTerm WebConnect using correct credentials.

Viewing Current Server Statistics

The *Deployment and Performance Statistics* dialog, displays current information (i.e., license count) for the PowerTerm WebConnect server. To open the *Deployment and Performance Statistics* dialog in the Administration Tool, select *Server | Deployment and Performance Statistics*.

Server Lifetime: 1 + 2:30:21	
Startup Begin: 06/08/10 15:21:23 End: 06/08/10 15:21:57 Elapsed: 0:00:34	Memory Working Set: 49,116 K Peak Working Set: 50,380 K Page Faults Count: 934,646
Logins First: 06/08/10 19:28:20 Last: 06/09/10 16:05:58	CPU Kernel: 0:00:08 0.009% User: 0:00:04 0.004%

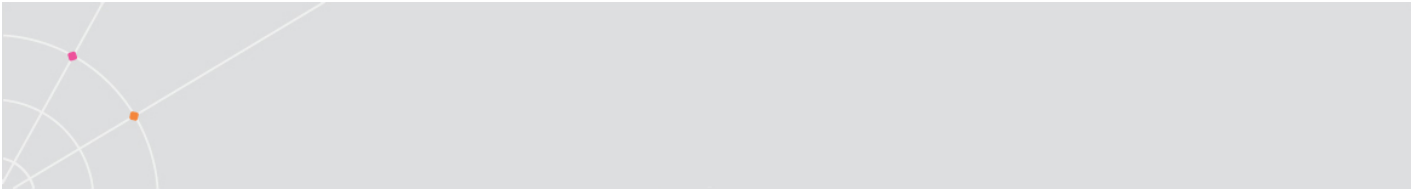
NOTE To refresh the information under *Deployment and Performance Statistics*, close and reopen the dialog window.

Event Viewer Access

Information related to server's operation will be tracked in the server's Event Viewer. The Administration Console provides a shortcut to the Windows Management Console Event Viewer. Select *Tools | Event Viewer*.

System Logs

Each start of the PowerTerm WebConnect server or starter service generates two new (standard) log files, *PtServer.LOG* and *PtStarter.LOG*. PowerTerm WebConnect maintains backup versions of these log files. They are named in the format: *exename.LOG.bck-00N*.



- *PtServer.LOG* represents the general log file of the PowerTerm WebConnect server.
- *PtStarter.LOG* represents the log file of the PowerTerm WebConnect starter.
- *Failover History* records the Failover state transition of PowerTerm WebConnect servers working in Failover mode
- *Error log*, is an Excel CSV document detailing errors from the PtServer log.
- *System Information* log, tracks periodic system checks, gathering information about the server-starter processes.
- *Communication Events* log, logs the LOGIN, LOGOUT, LOGIN-LOST, RECONNECT, etc. caused by client sessions (not administrative sessions).

The last log message contains the “~” character. If the maximum log file size is reached, then the last line contains the “^” character, indicating that any new log messages will be written at the start of the new log file.

Viewing the PowerTerm WebConnect Server log

Select Files | LOG files | Server | *Standard Log*.

Viewing the Failover log

Select Files | LOG files | *FAILOVER History.LOG*.

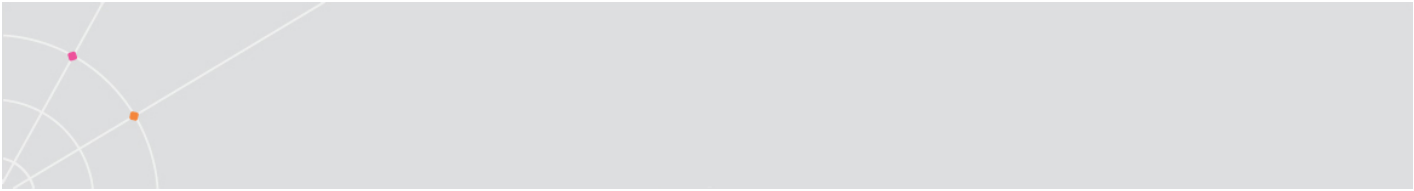
Viewing Audit Trails

The Audit Trail is a chronological record of the PowerTerm WebConnect user activities. This includes user login, application/desktop access, and other various actions. To view the audit trail using the Administration Tool: select Files | LOG files | *Audit Trail*. An editor supporting CSV is required to view the file (i.e., Microsoft Excel, Notepad, etc.)

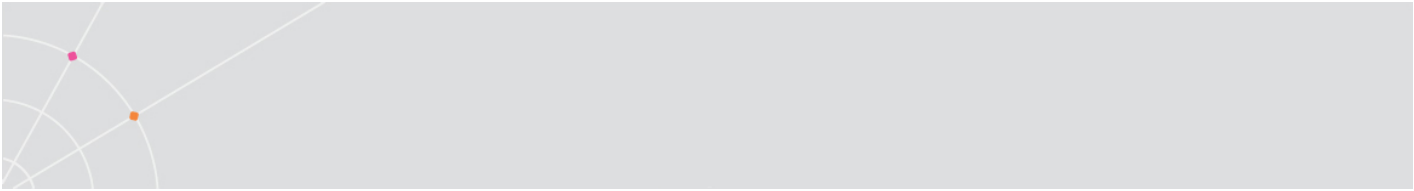
Audit Trail Options

The Main Configuration (PtServer.ini) has a setting to define Audit Trail options. *AuditTrail_Options* can be configured with the following parameters:

* /LAYOUT=	Establishes the layout mode <i>MINIMAL</i> (default) FULL
* One of /TITLE, /NOTITLE or /TITLE=...	Enables/disables/specifies the usage of the column titles row. /TITLE The default column titles will be used



	<p>(default).</p> <p>/NOTITLES Column titles will not be used.</p> <p>/TITLE=... The supplied list of column titles will be used. The very first character will be used as separator.</p>
* One of /READ_ONLY or /READ_WRITE	<p>Establishes the write permission mode of the file when it will be closed at midnight.</p> <p>Default: /READ_ONLY</p>
* /DIR=	<p>Specifies the folder of the audit trail output,. By default the Audit Trail (PtAT.dll) creates files in the folder <database>/Audit Trail.</p> <p>The value specified by /DIR= <option> may contain the logical folders <database> and <exe>.</p>
* /FILETITLE=	<p>Specifies the file title format of the audit trail output, other than the default. By default the PtAT.dll creates files name PtAT-<YEAR> <MONTH> <DAY>. The following placeholders are available:</p> <p><YEAR> Year with century, as decimal number.</p> <p><YEAR2> Year without century, as decimal number (00-99).</p> <p><MONTH> Month as decimal number (01-12).</p> <p><MONTHNAME> Abbreviated month name.</p> <p><MONTHNAMEFULL> Full month name.</p> <p><WEEKDAY> Abbreviated weekday name.</p> <p><WEEKDAYFULL> Full weekday name.<DAY> Day of month as decimal number (01-31).</p> <p><COMPUTER> PowerTerm WebConnect server's computer name.</p>
* /EXT=	<p>Specifies the file extension of the audit trail output, other than the default. By default the PtAT.dll creates files of CSV type.</p>
* One of /DAILY, /WEEKLY or /MONTHLY	<p>Establishes the file replacement (renewal) mode.</p>



/DAILY The file will be replaced at midnight (default).

/WEEKLY The file will be replaced on Mondays at midnight.

/MONTHLY The file will be replaced at midnight on the 1st of the month.

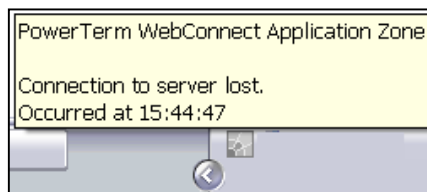
25. RECONNECT FEATURES

PowerTerm WebConnect includes four types of Reconnect features to ensure that end users have high availability to the PowerTerm WebConnect resources.

Type	Clients supported
Application Zone Reconnect	Application Zone
Session Reconnect	RDP RemoteView sessions
Blaze Reconnect	Blaze RemoteView sessions

Application Zone Reconnect

When an active Application Zone loses connectivity to its PowerTerm WebConnect server, it will automatically try to reconnect to the server. The Application Zone systray icon will start blinking when it attempts to reconnect.



Right-clicking on the systray Agent gives the user options to force a *Retry* or to *Quit* the Application Zone.



Once the network connection is re-established and the Application Zone properly reconnects to the PowerTerm WebConnect server, the Systray Agent will stop blinking and remain solid.

Two common cases where the Application Zone loses connectivity:

- The PowerTerm WebConnect server is shut down
- The client system loses network connectivity to the PowerTerm WebConnect server.

Session Reconnect

What is a Disconnected Session?

Disconnected Terminal Server sessions are user sessions on the Terminal Server that contain active applications, but not currently connected to by a client. Sessions may become disconnected for various reasons, such as:

- A network fault or any loss of communication.
- The Administrator disconnects the session.
- The user disconnects the session or closes the RDP client without logging out of the session.

Disconnected sessions have a finite lifespan as defined by a timeout period set on the Terminal Server (configured by the administrator). At the end of this timeout period, the session will automatically be reset. A user can reconnect to disconnected Terminal Server sessions as long as it is active.

NOTE PowerTerm WebConnect Session Reconnect does not require or use the Microsoft Session Directory service. As a result, Enterprise versions of Windows server are required.

Client Usage

Disconnected Sessions are reconnected by just launching a new application. When a user is logged in to the Application Zone and has a disconnected session assigned, the following icon may also appear in the Application Zone and the systray agent:



A balloon message will also appear displaying "*Power Term WebConnect Application Zone. You have disconnected sessions. Right click the icon in order to resolve them.*"

Right clicking on the disconnected icon will provide three options to the user:

Reconnect all	Reconnect to all disconnect sessions
Close all	Close all disconnected sessions
Hide notification	Hide the disconnect icon and do nothing

NOTE The user can only reconnect to disconnected sessions belonging to it.

Double-clicking the icon will reconnect the user to an active session. The icon will no longer be displayed if the user hides it or if there are no longer any disconnect sessions.

Logging off a user using the Administration Console

To close a disconnected session:

- Launch the Administration Tool.
- Click on the Terminal Server Sessions button. A list of all active Terminal Server sessions will be displayed, including the disconnected ones.
- Select the disconnected session(s) to be closed. Use the Ctrl key for multiple selections.
- Right-click on the selected session(s) and select Log Off Disconnected Sessions (or Log Off All Disconnected Sessions).



Logoff Disconnected Sessions

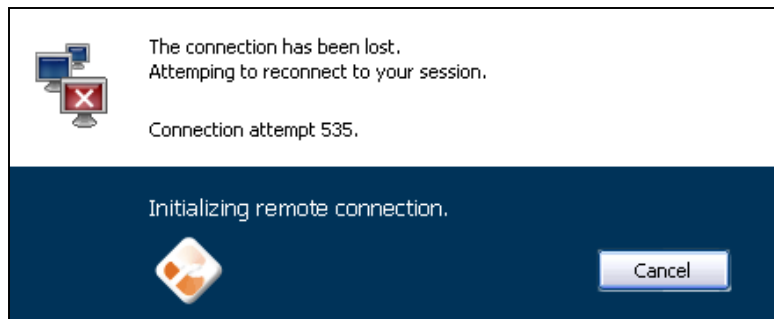
- Click on Yes to confirm.

NOTE Disconnected Session Reconnect is only available for sessions created through PowerTerm WebConnect and the Load Balancer.

NOTE Disconnected Session Reconnect Network Reconnect is only available from Windows clients. This feature is not available for users connecting from Mac or Linux systems.

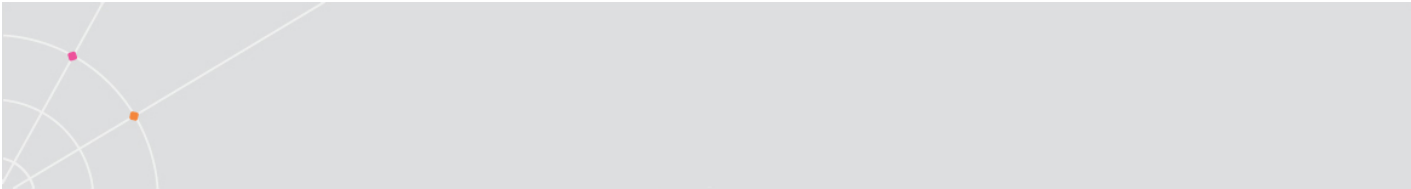
Blaze Reconnect

Ericom Blaze sessions use a different reconnect mechanism built into the client component. During a network interruption, the Blaze session will attempt to reconnect to the active session. During the reconnect process the user will be presented with a dialog box with the number of connection attempts. The user may stop the reconnection attempts by clicking the *Cancel* button.



Network Reconnect

Network Reconnect will automatically resume sessions that have been interrupted by a network disruption.



There are three available modes:

None	Will not reconnect an interrupted session.
OnDemand	Will reconnect only sessions connected through the PowerTerm WebConnect server's gateway.
Wireless	Will reconnect any session automatically. All wireless sessions use the PowerTerm WebConnect server's gateway.

The Network Reconnect configuration process consists of the following:

- Configure the PowerTerm WebConnect Server to use Network Reconnect (Network Reconnect is disabled by default).
- Specify which PowerTerm WebConnect objects have permissions to use Network Reconnect.
- Configure the client parameters to use Network Reconnect
- When the user launches a PowerTerm WebConnect component, the reconnect mode is activated for the session.

Enabling the Network Reconnect

Network Reconnect is disabled by default. Configuration to the server and client components are necessary to enable Network Reconnect.

Server Configuration for Reconnect Mode

To begin, set the Default Reconnect Mode. This will be the default value when Network Reconnect mode is not configured in objects that have higher precedence.

- Select Server | *Configuration*.
- Select the desired Default Reconnect Mode.

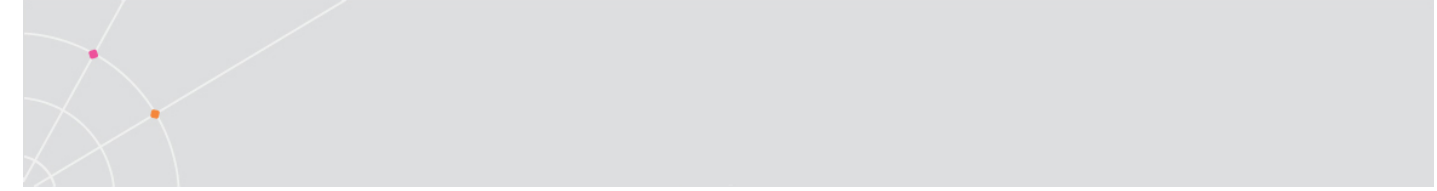
When the *Highest Reconnect Mode* is set as <Default>, the Server's value will be used.

To set the Reconnect mode for a group:

- Right-click on the desired group and select Properties. The *Group Properties* will appear.

The screenshot shows a configuration window titled "Client". It contains two settings: "Inactivity Timeout" with a text input field containing the number "8" followed by "minutes.", and "Default Reconnect Mode" with a dropdown menu currently set to "Wireless".

<p>HINT The default group of the server is <i>Novice Users</i> and its <i>Reconnect Mode</i> is <i>None</i> by default. This must be changed to enable Network Reconnect.</p>
--



HINT Non-persistent users do not belong to a group by default. Assign a Default group to the *Default AutoCreated User* to set the *Reconnect Mode*.

- Select the Highest Reconnect Mode.

To set the Reconnect mode for a user:

- Right-click on the desired user and select Properties. The *Group Properties* will appear.

NOTE For Non-persistent users, the *Reconnect Mode* must be set at the group level

- Select the Highest Reconnect Mode.

NOTE The user setting has the highest precedence.

Main Configuration Settings (PtServer.ini)

LastSentMessagesMaxCount

When Network Reconnect is used in *Wireless* mode, PowerTerm WebConnect tracks the packets for every connection and saves them so any lost data can be restored after a reconnection.

If the value of *LastSentMessagesMaxCount* is too low the server may fail to reconnect because there is not enough data stored. However, if the value is too high, Network Reconnect may consume too much memory from the PowerTerm WebConnect server.

The default value (64 packets per connection point) should not be modified. Every time the server fails to reconnect, it automatically increases the *LastSentMessagesMaxCount* value. After a few failed connections, *LastSentMessagesMaxCount* will be automatically adjusted to an optimal value.

Client Configuration for Reconnect Mode

To enable Network Reconnect in a PowerTerm WebConnect component, add one of the parameters listed below to the command line, or in the corresponding HTML file (i.e., ApplicationZone.html).

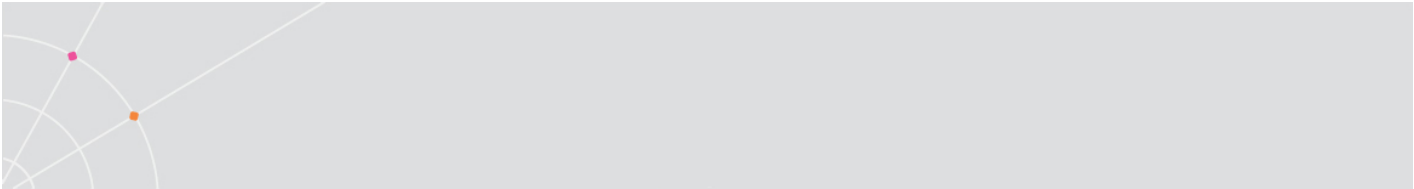
Client Parameters for Reconnect Mode:

/RM_NONE (*)

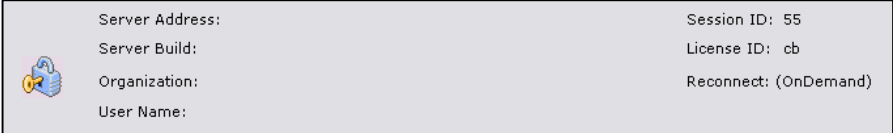
/RM_ON DEMAND

/RM_WIRELESS

/RM_INTERACTIVE - enables the user to select the mode during login (HostView clients only).



Once a component is connected to the server, the activated *Reconnect* mode appears in the bottom right of the *About* dialog:



If the Reconnect mode is not displayed, Network Reconnect is disabled.

If the network connection is interrupted during a session enabled with Network Reconnect, a connection dialog will appear while the client attempts to reconnect to the server.





26. UPGRADE INSTRUCTIONS

An existing configuration of PowerTerm WebConnect can be imported into the new version by using the *Upgrade* utility. The PowerTerm WebConnect installation and upgrade requires administrative access to the server.

NOTE If the web server components are installed on separate machines, the Ericom web components will also need to be updated on the web servers.

Areas covered by the upgrade

The following list of files and features that have been modified in an earlier version will be imported into the new environment as part of the upgrade utility:

- The main *Ptserver.ini* database file along with all supporting database files
- Load Balancer XML configuration file
- DeskView Connection Broker XML configuration file

Areas not covered by upgrade

The following list of files and features may have been modified in an earlier version, but will not be imported into the new environment as part of the upgrade utility:

- All web pages: *applicationzone.html*, *launch.asp*, etc.
- All ComPortal files: *comportal.ini*
- AccessNow config file(s): *config.inc* (under *AppPortal* folder)
- Ericom Secure Gateway configuration file
- Any updated files that were placed in the *Downloads* directory
- Custom logos and banners

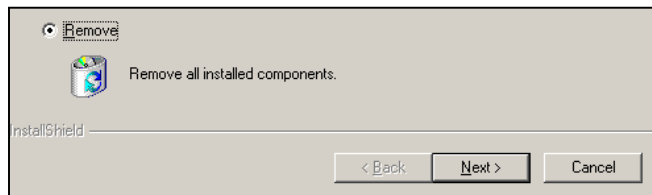
Any changes that were applied to these areas must be manually configured back into the new environment. Do *not* copy configuration files from old versions to newer versions as certain settings may not apply in the new version.

STOP Backup the entire *WebConnect* directory before uninstalling the application, so the modifications are not lost. When reapplying the modifications to the new version, refer back to the previous configuration files to verify accuracy.

Uninstall the Current Installation

Before installing the new version, first *uninstall* the existing version. The licensing will be maintained on the server and the configuration files will be backed up as part of the uninstallation process.

Stop the *PowerTerm WebConnect Server* service before running the uninstaller. To uninstall PowerTerm WebConnect, remove the application using the Control Panel | *Add/Remove Programs* (or *Uninstall Programs* link). At the first installer prompt select *Remove*.

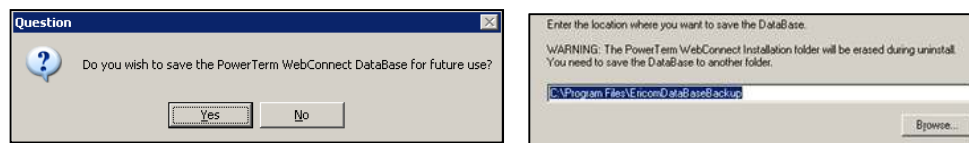


Backup the Previous Installation

Manual Backup (Recommended): simply copy the application folder to a backup drive.

- The default path is <Drive>\Program Files (x86)\Ericom Software\WebConnect X.X

Automatic Backup (Not required if Manual Backup has been performed): During the uninstallation of the current version, the administrator will be prompted to back up the current configuration. Simply specify a path for the backup files.



Four configuration folders will be backed up: *Database*, *DeskViewAdmin*, *DeskViewServer*, and *Load Balancer*.

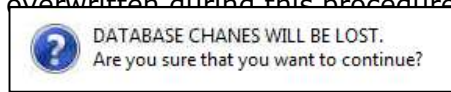
Import after new installation

Once the installation is completed, import the previously backed up configuration.

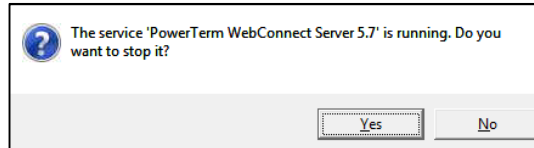
- Go to Start | Programs | Ericom Software | PowerTerm WebConnect | *PowerTerm WebConnect Upgrade Utility*



- Click Yes to the warning message. All existing configuration will be overwritten during this procedure.



- Click Yes to stop the Server service. All active users will be disconnected.



- Click Yes when prompted to use previous settings, and select the desired PtServer.ini file to import. Click OK to continue.

After the settings are imported, restart the PowerTerm WebConnect Server service for the settings to take effect.

Verifying the LoadBalancer.xml file

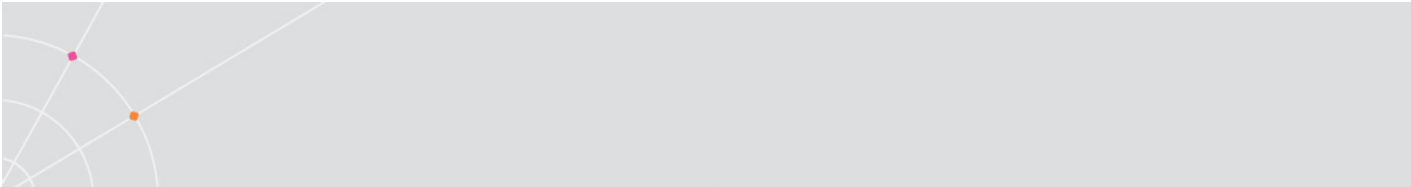
- Open the XML file and verify that the XML path is correct (update the version number in the path if needed):
`XMLFilePath="C:\Program Files (x86)\Ericom Software\WebConnect 5.X\Load Balancer\"`

Upgrading Terminal Server Components

Ericom Terminal server related components need to be updated manually or by using a third-party deployment tool.

NOTE TSagent, Ericom Blaze and Ericom AccessNow Servers have been merged into one application called Ericom AccessServer (3.3.1 and higher). This is the replacement for the Ericom AccessNow server and Ericom Blaze Server installations. If you have individual agents installed: AccessNow Server, Blaze Server, and TSagent,

- Terminal Server Agent – uninstall previous versions of the TSagent and install the Access Server (located under C:\Program Files (x86)\Ericom Software\WebConnect 6.0\AddOns\AccessServer). 32 and 64 bit versions of Access Server are available.
- Blaze Server – uninstall previous versions of the Blaze Server and install the Access Server (located under C:\Program Files (x86)\Ericom Software\WebConnect 6.0\AddOns\AccessServer). 32 and 64 bit versions of Access Server are available.
- AccessNow Server – uninstall previous versions of the AccessNow Server and install the Access Server (located under C:\Program



Files (x86)\Ericom Software\WebConnect 6.0\AddOns\AccessServer). 32 and 64 bit versions of Access Server are available. If the Access Server is already installed for Blaze use, it does not need to be installed again.

Updating the AccessNow Folder on Web Server

When Access Server is updated on the RDP Hosts, the corresponding web pages also need to be updated on the web server hosting the PowerTerm WebConnect *AppPortal* folder.

- To update the pages simply copy the "AccessNow" folder from the Access Server and copy it to the web server
- The AccessNow folder on the web server is located under: .. \Ericom Software\ WebConnect 6.0\web\AppPortal\AccessNow
- Rename the existing AccessNow folder (e.g. AccessNow-original) and copy the updated AccessNow folder into the same location.

Updating the Native Clients on the Broker

To update any component in WebConnect, please visit the online components page: <http://www.ericom.com/PowerTerm-WebConnect-Components.asp?ref=update>

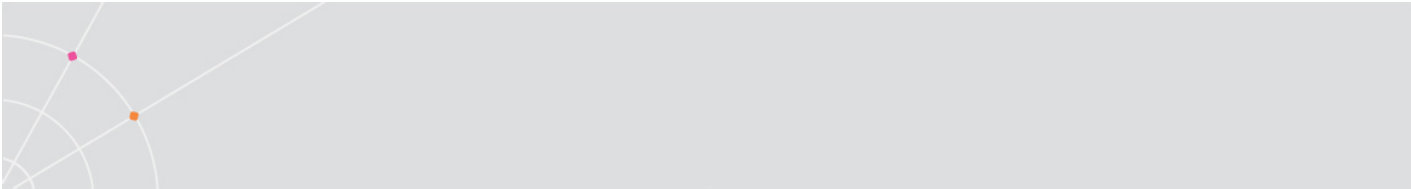
NOTE Back up the existing components before overwriting them with the latest versions for ease of rollback.

Applying Windows Updates/Patches

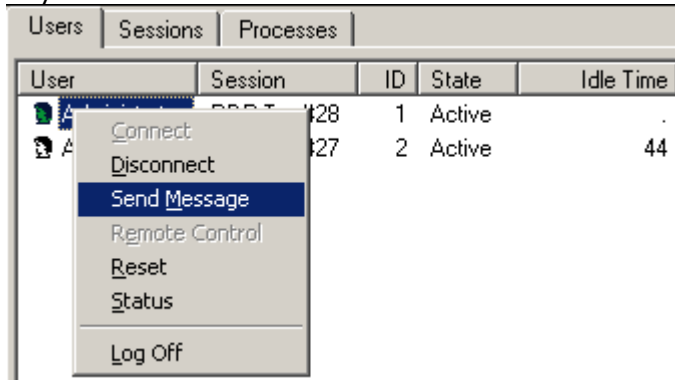
When applying server updates (i.e., Windows update) the Ericom environment should be updated off hours during a period with little impact to the end-users. Update the Terminal Servers first, and begin with servers that have no users logged in. Once the initial set of Terminal Servers is updated, update the Terminal Servers that have users logged on them, but send a broadcast message warning of possible server reboot. Once Terminal Servers are updated, apply the updates to the PowerTerm WebConnect servers.

Updating Terminal Servers

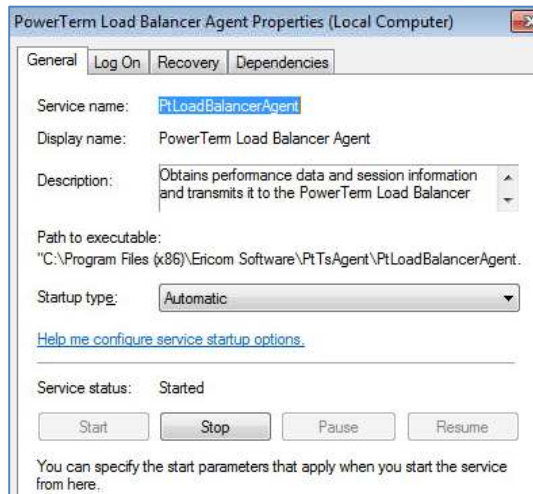
- Ensure that there are no users on the system before applying updates
- If there are idle users present, inform them that the server will be restarted for maintenance (send a message using Terminal Server Manager or call the user). Use the Terminal Server Manager to logoff



any active users.



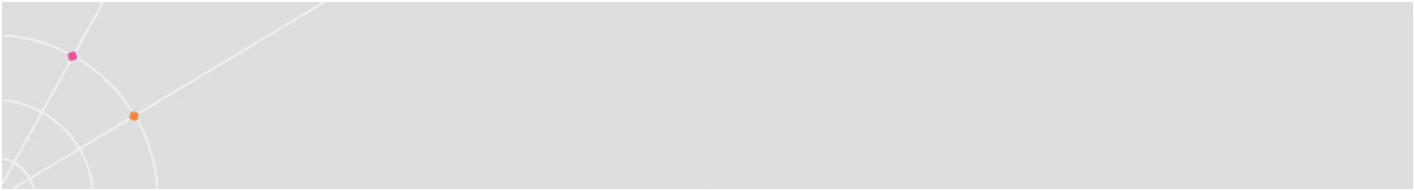
- Stop the Load Balancer agent service so new users will not logon.



- Apply necessary updates
- Reboot the server if required, or restart the Load Balancer Agent service once the updates are completed
- RDP to the server to ensure that it still accepts connections. Test PowerTerm WebConnect access.

Updating PowerTerm WebConnect

- Ensure that there are no users logged into PowerTerm WebConnect before applying updates.
- If there are idle users present, inform them that the server will be restarted for maintenance (send a message using the Admin Tool or call the user). Use the Admin Tool to logoff any active users.
- Apply Windows updates.



- Reboot the server if required. Reboot the Database server first and then the WebConnect servers immediately afterwards.
- After the reboot, login to PowerTerm WebConnect Admin Tool on a server to ensure that everything is operating properly.
- If PowerTerm WebConnect is using Cluster mode, login to the Admin Tool on the second WebConnect server and verify that the Monitor-mode message appears (this means that the servers are running in cluster mode). If the Monitor-mode message does not appear, verify that the Database server has rebooted properly.

27. Customizations

PowerTerm WebConnect's interfaces can be configured to incorporate the owner's logo and images to provide a private-label look and feel.

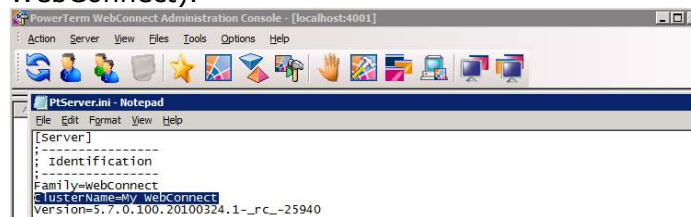
Use a custom logo in the Ericom web pages

There are three web pages where users usually navigate to in order to login to PowerTerm WebConnect. The logos at each of the pages are located in the following paths:

App Portal Logo C:\Program Files (x86)\Ericom Software\WebConnect x.y\web\AppPortal\Images\ericomlogo.gif
Application Zone logo C:\Program Files (x86)\Ericom Software\WebConnect x.y\web\images\BackgroundUp.jpg
Start page logo (place customer logo in the white space below the Ericom logo) C:\Program Files (x86)\Ericom Software\WebConnect x.y\web\images\left_column.jpg

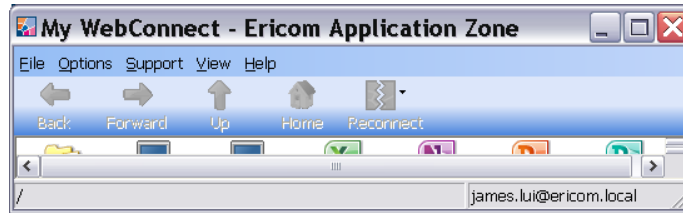
Create a custom Application Zone title

- From the Administration Tool, go to Files | Configuration | *Main*.
- Find the *ClusterName* setting and enter the custom name (i.e., My WebConnect).



- Close and save the file.
- Restart the *PowerTerm WebConnect Server* service

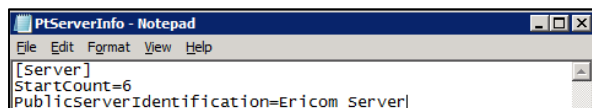
- After the restart, all Application Zones will use the new title.



Use a custom external PowerTerm WebConnect Server address

The PowerTerm WebConnect server can be given a custom name for external users. This protects the identity of the Ericom server.

To configure the external name, open the *PtServerInfo.INI* file under the bin directory. Edit the *PublicServerIdentification* field and enter the desired name. In this sample *PtServerInfo* entry, *Ericom Server* is used as the label displayed to end-users.



The custom label will be used in any dialog boxes referencing the PowerTerm WebConnect server.

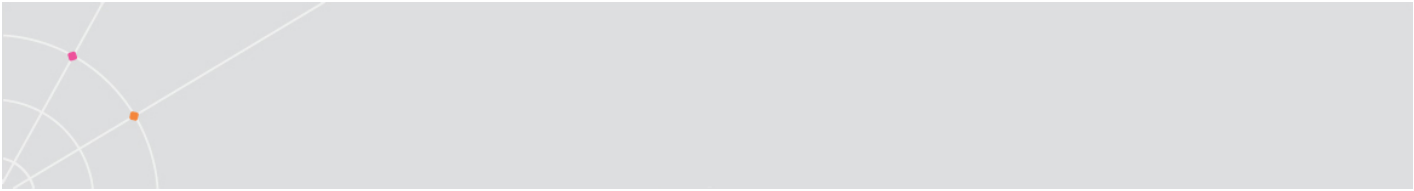


Changing this value requires a PowerTerm WebConnect Server service restart.

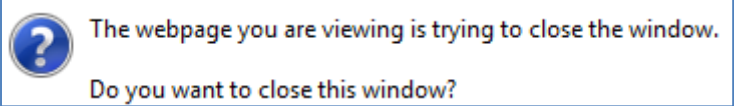
Closing the web browser automatically after Ericom is launched

Add the following code to the HEAD of the desired web page to closed the browser automatically after the PowerTerm WebConnect components are downloaded and installed (user will be prompted for confirmation).

```
<HTML>
<HEAD>
<TITLE>PowerTerm WebConnect </TITLE>
<SCRIPT language="JavaScript">
setTimeout("window.opener=window;window.close()",300000);
</SCRIPT>
</HEAD> ...
```



In this example, the window is closed after 300000 milliseconds, or 5 minutes. Leave enough time for the Ericom components to fully download before closing the browser. The user will be prompted to close the browser:



28. Appendix A – Environment Variables

This chapter covers all available environment variables that can be configured with PowerTerm WebConnect. Environment variables may be configured for users, groups, connections, and the server.

NOTE An empty value indicates that there is no initial value

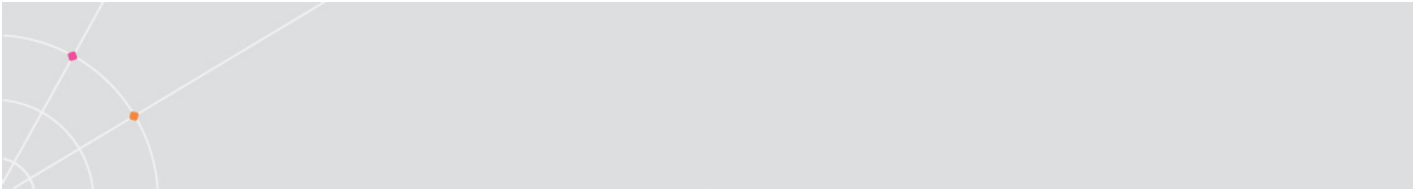
Variable name	Values	Description
AGENT_AllowMultiple	1 = on Default: 1 Upgrade: empty	Privilege to run multiple agents for the same user (from different IPs).
AGENT_ExitCleanMode	<i>DoNothing</i> (Leave icons) <i>CleanCredentials</i> <i>CleanApplications</i> <i>CleanAll</i> = Removes credentials and all the created shortcuts. <i>Disable</i> = The user cannot exit the agent. Default: empty = <i>CleanAll</i>	Specifies which Application Zone components to remove upon exit.
AGENT_SysTray	<i>Regular</i> <i>HoldUp</i> <i>Hide</i> Default: empty = The command line value will be used.	The state of the Application Zone systray agent.
AGENT_UserViewMode	<i>UserDefined</i> <i>Classic</i>	<i>UserDefined</i> (or empty) - This is the default value for the variable. The Application Zone will use the user's current view ("Classic" by default). <i>Classic</i> - The user is forced to work with the "Classic" view only. This environment variable has higher precedence over the /SNE flag which sets the mode in pagent.

AN_DefaultPort	<i>Sets the default port used by AccessNow</i>	Default value is 8080
BLAZE_SETUP_PARAMS	<i>Sets additional parameters for Blaze enabled connections</i>	Any Blaze parameter, refer to a .blaze file for possible options. Separate multiple values using a semi-colon `;`.
ClientIdleTimeoutMinutes	<i>Sets the timeout value for Application Zone</i>	Default is 0 (disabled) Any value greater than 0 will enable the timeout for the specified amount of minutes
MODE_SessionOverlap	Default: empty	Sets the session overlap mode for the very first session.
PRIV_ChangePassword	1 = On Default: empty	Enables the user to modify his/her password.
PRIV_CopyToFile	1 Default: empty	Enables the user to copy the screen contents to a file.
PRIV_CreateShortcut	Default: empty	Enables the user to create a shortcut.
PRIV_FileTransfer	Default: empty	Enables the user to use the File Transfer of the HostView clients.
PRIV_Keyboard	1 Default: empty	Enables the user to open and/or save the keyboard mapping of the emulator clients.
PRIV_KeyboardMap	1 Default: empty	Enables the user to view and/or modify the keyboard mapping of the emulator clients.
PRIV_Online	1 Default: empty	Enables the user to switch the emulator client off/on line.
PRIV_PowerPad	1 Default: empty	Enables the user to modify, open and/or save the Power pad and Function buttons of the emulator clients.
PRIV_RunDFT	Default: empty	Enables the user to run Ericom's DFT utility.

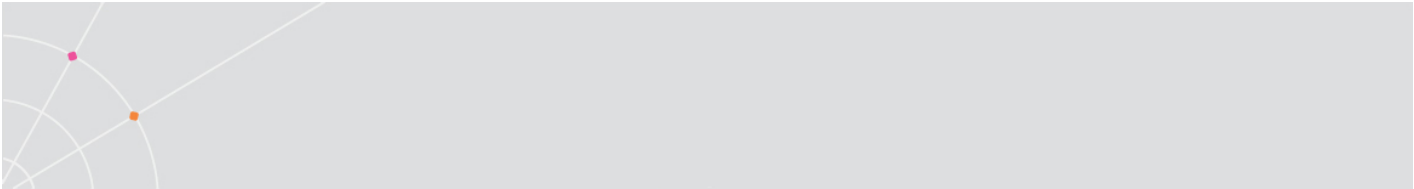
PRIV_RunQuickFTP	Default: 1	Enables the user to run PowerTerm WebConnect QuickFTP client.
PRIV_RunRDP	Default: 1	Enables the user to run PowerTerm WebConnect RemoteView client.
		Enables the user to run PSL commands and scripts, to edit and to record them.
PRIV_Script	Default: empty	The maximum resolution of the Desktop bitmap image to be attached to a message. 0 (zero) means than no image can be attached.
PRIV_SendImage_BitsPerPixel	0, 4, 8, and 16 Default: 4	The maximum size (in kB) of the compressed Desktop bitmap image. 0 (zero) means than no size limitation is applied.
PRIV_SendImage_MaxSizeK	Default: 32	Enables the user to use the messaging facility of PowerTerm WebConnect.
PRIV_SendMessage	0 = off 1 = single messaging target 2 = multiple messaging targets Default: empty	Enables the user to modify and/or save the setup of the emulator clients.
PRIV_Setup	Default: empty	For sessions running on a Terminal Server. Only evaluated if PRIV_CreateShortcut is enabled.
PRIV_TerminalCanCreateShortcut	Default: empty	Enables the user to use the trace facility of the emulator clients.
PRIV_Trace	(empty)	Enables the user to use the Universal Printing feature of the RDP client.
PRIV_UniversalPrinting	Default: empty	Enables the user to open a

	Upgrade: empty	new emulator client.
PRIV-NewTerminalWindow	1	Specifies Terminal Server authentication level (see Microsoft documentation)
RDP_AuthenticationLevel	Default: 0	Remove "@..." from user name leaving only the unqualified name
RDP_CutFullUserName	1 = on Default: 0	Disable RDP bulk compressor
RDP_DisableCompression	1 = on Default: 0	Disables the PrintScreen function in RemoteView sessions.
RDP_DisablePrintScreenKey	1 = on Default: 0 Upgrade: empty	Disables the Session Sharing of RemoteView sessions.
RDP_DisableSessionSharing	1 = on Default: 0 Upgrade: empty	Disables the Universal Printing feature of RDP client.
RDP_DisableUniversalPrinting	Default: 1 Upgrade: 1	The TSAgent logs off the session immediately when it receives notification from the session that it has become disconnected.
RDP_LogoffDisconnected	Default: 1	Force MS Seamless (RemoteApp) or Ericom True Seamless regardless of connection settings and host type.
RDP_ForceSeamless	MS-Seamless Ericom-Seamless Default: empty	Determines if a Full Desktop session will run in multi-monitor or open in a preset monitor.
RDP_FullScreenMonitor	Default: 0 Primary Monitor: 1 Secondary Monitor: 2 ...	Sets the RDP logoff timeout from the point where the user closes the last seamless application. Also sets the AccessNow and

		AccessToGo screen idle timeout logoff.
RDP_LogOffDelaySeconds	Default: 900 (seconds) Min value (AccessToGo and AccessNow sessions): 3 Min value (RemoteView and Blaze sessions): 30 Set to 3 for lowest value	Name of file to run before running the TSAgent.
RDP_PreTSAgentExe	Default: empty Upgrade: empty	Specifies what protocols to redirect, like http, https, etc.
RDP_RedirectSchemes	Default: empty Upgrade: empty	Specifies what URLs not to redirect.
RDP_RedirectExclude	Default: empty Upgrade: empty	Sets an alternate location for the script folder
RDP_ScriptFolder	Path to scripts folder (i.e., \\fileserver\scripts)	Suppress error message if connection to server is lost
RDP_Suppress_Service_Stopped_Message	1 = on Default: 0	Run with hidden Windows Explorer in seamless session. Useful for: Publishing folders and apps that don't work without Explorer
RDP_WithExplorer	1 = on Default: 0	Turns local cursor to an hourglass whenever mouse button is pressed. Improves perceived response time for slow connections. <i>Not supported by Blaze.</i>
RDP_WaitCursor	1 = on Default: 0	Enter the desired octets separated by semi colons. A range may also be specified. For example: 10.3.2;10.4;11 includes: 10.3.2.x and 10.4.x.x and 11.x.x.x Range: 131.100.2.1-131.100.2.120;192.168.1.3-192.168.1.199
SmartInternalIPRanges	Default: empty	Specifies the To e-mail



		parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_ERICOM	Default: tech.support@ericom.com	Specifies the Bcc e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailBcc	Default: empty	Specifies the Body e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailBody	Default: The attached file contains material required by Ericom to reconstruct the situation for which the user is requesting assistance.	Specifies the Cc e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailCc	Default: empty	Specifies the Subject e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailSubject	Default: empty	Specifies the e-mail address of Ericom Support
Support_MailTo	Default: tech.support@ericom.com	Specifies the terminal language (code page set) for HostView.
TerminalLanguage	R, REGIONAL or REGIONALS = Evaluates the current user's regional settings. E or ENGLISH = English terminal H = RTL languages terminal ?, I or INTERACTIVE = Asks the user for his preference. Default: empty	Enables the user to use the version of triCerac plug-in client. Used for multiple triCerac plug-in clients support.
TriceratUniversalPrinting Version	Default: empty Upgrade: empty	Replaces USE_CLIENT_activex and USE_CLIENT_exe
USE_CLIENT_HostView		If not empty, any new



		emulator client will be logged off immediately, displaying the specified text.
W2H_LoginDisabledReason	Default: empty	The text sent to the client requesting support when the request is accepted.
W2H_SupportAccepted		The text sent to the client requesting support when the request is rejected explicitly by the support.
W2H_SupportRejectedByUser		The text sent to the client requesting support when the request is rejected due to the timeout being exceeded.
W2H_SupportRejectedOnTimeout		



Useful Blaze_Setup_Params Values

NOTE These variables will have the highest precedence and override any previously configured settings. Separate multiple entries using a semi-colon `;`.

Value	Description
use HP Universal PS Printer Driver:i:	1 – enables Blaze universal printing - required for Windows 8 and 2012
disable menu anims:i:	1 – disables menu and window animations for better performance
convert unicode to scancode:i:	1 – uses scancodes for typing. Required for certain applications such as VMware vSphere client and Blaze client. Also required when connecting to Linux desktops over RDP

29. Appendix B – Administration Console

Action Menu




Command/Submenu	Toolbar Button	Description
New		Opens the <i>Publish Application</i> and the <i>Remote Desktop</i> wizards, as well as the <i>Add User/Group/Host Connection</i> dialogs.
Quick Access Dialog		Launches the Quick Access dialog.
Copy	-	Copies the object's property definition resulting in a mirror copy except for the name, which must be unique.
Delete	-	Deletes the selected object.
Shut Down	-	Shuts the selected object down.
Send Message	-	Enables you to write an instant message and send it to the selected object's members.
Properties	-	Opens the object's properties dialog.
Sessions	-	Displays the active sessions that are related to the selected object.
Exit	-	Exits the Administration Tool.

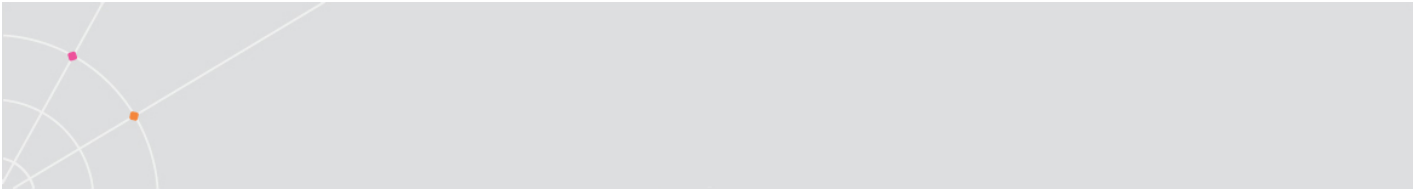
Server Menu






Command/Submenu	Description
Connect/Disconnect	Connects/Disconnects the Administration Console from the server.
Configuration	Opens the server's configuration dialog.
Default Settings	Opens the Property pages where you can define the

	default settings for all users in the system.
Default Power Pad	Opens the Power Pad & Function Buttons dialog.
Memo	Opens a Notepad so you can write text file memos.
Deployment & Performance Statistics	Displays the Deployment & Performance Statistics window.
Refresh ActiveDirectory Information	Manually refreshes the Active Directory Tree data. (Automatic refresh will occur at a pre-determined daily time.)
Reload the License	Refreshes the license file.
Directory Services	Opens the Directory Services dialog.
Send Message to All Users	Opens the Send Message dialog to send an instant message to all the system users.
Send E-Mail to All users	Opens the default e-mail application to send an e-mail to all the system users.
Attach Server's Machine	Attaches to a user's session upon request.
Start Server	Starts PowerTerm WebConnect Server.
Shut Down Server	Shuts PowerTerm WebConnect Server down but does not close Administration Console (recommended method).

View Menu

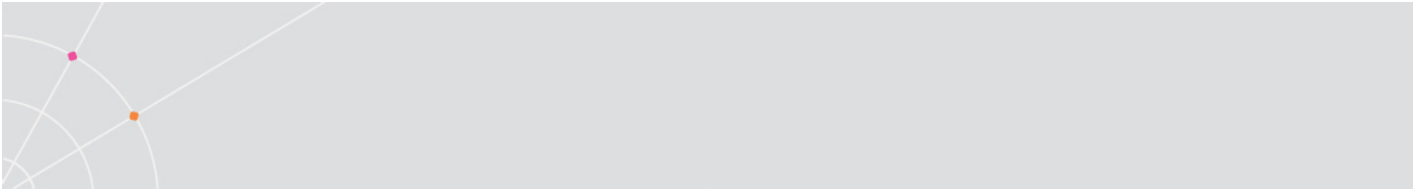
Command/Submenu	Toolbar Button	Description
Connections		Expands the Connections pane and hides the other two panes.
Users		Expands the Users pane and hides the other two panes.
Groups		Expands the Groups pane and hides the other two panes.
All Views	-	Displays all three panes.
Environment Variables	-	Opens the Environment Variables window, with all the environment variables in the system.



Client Sessions		Displays real-time information for current Client sessions.
Administrative Sessions		Displays real-time information for current Administrative sessions.
Terminal Server Sessions		Displays real-time information for current Terminal Server sessions.
Machines	-	Displays real-time information for machines currently in session.
Intruders		Displays all Intruder attempts.
Refresh I/O Information		Refreshes runtime information in all the Administration Tool's tables.
Auto Refresh I/O Information	-	Activates automatic refresh, defined in the Server properties.



Files Menu

Command/Submenu	Description
Configuration	<p>Five configuration files (PtServer*.ini) that are located in the \DataBase directory:</p> <p><i>Main</i>, contains the definitions of all the entities used by PowerTerm WebConnect Server, except for the host connector that are contained in the PtServer_Connections.ini file.</p> <p><i>Users</i>, contains the definitions of all the user entities used by PowerTerm WebConnect Server.</p> <p><i>Groups</i>, contains the definitions of all the group entities used by PowerTerm WebConnect Server.</p> <p><i>User/Group links</i>, contains the definitions of all the user-to-group links used by PowerTerm WebConnect Server.</p> <p><i>Connections</i>, contains the definitions of all the connection entities used by PowerTerm WebConnect Server.</p>
LOG files	<p>The log files are circular text files. Each execution of the server or starter opens a new log file. PowerTerm WebConnect maintains backup versions of these log</p>



	files: <i>Server, Starter, FAILOVER History.LOG, Audit Trail</i>
Put Background Bitmap	Takes the specified file and creates a special file that can be associated as an emulation session's background.
Get File	Imports files from the server to the local workstation.
Put File	Exports files from the local workstation to the server.

Tools Menu

Command/Submenu	Toolbar Button	Description
Run Event Viewer	-	This Microsoft utility will display the pertinent log information for the server's machine to which you are logged on.
Run FTP Client	-	Launches the FTP client, which provides a convenient way to transfer files.
Run HostView	-	Allows you to emulate the user's session and connection and thereby conduct a test on it.
Run RemoteView	-	Runs the selected RDP connection and allows you to test it.
Open Application Zone		Runs the Application Zone.
Run Load Balancer Administration Tool		Launches PowerTerm WebConnect Load Balancer Administration Tool.
Open File	-	Enables you to open files.

Options Menu

Command/Submenu	Description
Toolbar	Displays the toolbar providing easy accessibility for the frequently used features of the Administration Tool.
Status Bar	Displays the status bar at the bottom of the Administration Console main screen in which status messages and prompts can be shown.

Use Tooltips on List Header	Enables tips on list header when the text is truncated.
Use Tooltips on List Rows	Enables tool tips on list rows when the text is truncated.
Grid Style Views	Toggles the grid style mode of all the views.
Use Monospaced Font Views	Toggles the mono-spaced font mode of all the views.
Synchronize Updates with the Server	Determines whether the actions taken by the Administration Console are simultaneously updating the server. (NOTE This might slow down work, bringing it to a halt.)
Update Mode of the Display	Determines how frequently the screen should be refreshed, i.e. immediately, time delayed, or manually.
Postpone Display's Updates While Editing Properties	Delays the updating of the display while you are editing the object's properties.
Use Empty Default Password	Toggles explicit empty password requirement.
View Encrypted Variable's Values	Toggles the encrypted variable's values mode of all the views.
Dynamic Connection Attribute Text Color	Determines the title color of the Dynamic Connection Attribute fields.

Help Menu

Command/Submenu	Description
Help Topics	Launches the Administration Console online help.
Charts	Displays the HostView client data flow diagrams.
Send Mail to Support	Launches your local email application and starts a new message addressed to Ericom Support
About the Administration Tool	Displays the current version of Administration Tool, and Ericom contact information.

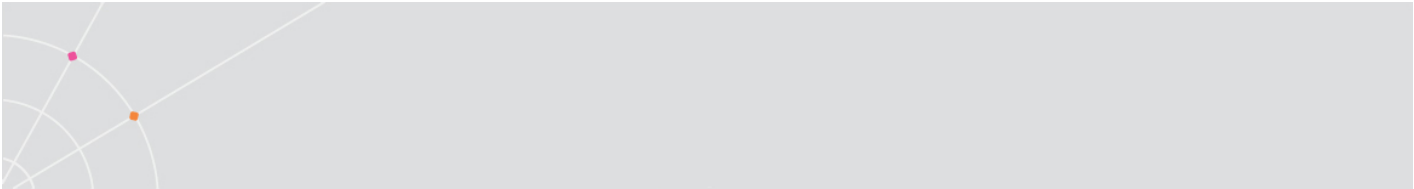
Information Panes

The following sections detail the fields of the various Information panes. You can view different types of information by right-clicking the pane.

Connections Pane

Connection Name	Target	Network	Terminal Type	Terminal Model	Comm-Type	Security
Example_As400	as400.ericom.com	Public	5250 Display	3179-2 (24x80)	TMS250	
Example_VT	vas.ericom.com	Public	VT420-7	VT420	TELMET	
localhost	localhost	Gateway	SCO-ANSI	ANSI	TELMET	

Field	Description
Connection Name	The connection's unique name. The Connection Name can only be modified at creation time. Once it has been set for the connection it cannot be changed. To redo a connection, just create a new copy and change the Connection Name, and delete any old ones that will no longer be used.
Display Name	A display name for the connection that is not necessary unique.
Alternate Connection	Specifies another connection to be used if this connection fails to connect to the host.
Created	Date and time the connection was created.
Modified	Date and time the connection was last modified.
Owner	Specifies the connection's owner.
Enabled	Specifies if the connection is activated or not.
Usage Type	Specifies how the connection will be used: <i>Hidden</i> , can only be activated from a login script. <i>Child</i> , owned by another connection. <i>Regular</i> , a regular connection. <i>Owner</i> , a regular connection which, when closed, will automatically shut down all associated connections (child connections, connections opened by the login script, etc.).
Target	Specifies the connection's target.
Network	Specifies the connection point type.
Terminal Type	Specifies the terminal type.
Terminal Model	Specifies the terminal model.
Comm-Type	Specifies the communication protocol used by the



	host. (Different protocols will display different parameters required.)
Security	Specifies the security protocol used by the host.

Users Pane

User Name	Alias Name	Path	Auth...	Created	Modified	Rights	Default G...	Free	Acce...	Acce...	Conc...	Enabl
< Generic Custom...						Client		No			Yes	Yes
< Portal >						Client		No	User	loca...	Yes	Yes
< Software Insta...						Client		No			Yes	Yes
Administrator			WebC...		08/23/07...	Admi...	Super Users	No	User	127....	No	Yes
Default AutoCrea...			WebC...			Client		No			Yes	No
Example			WebC...			Client	Novice Users	No			Yes	Yes
Guest			WebC...			Client	Novice Users	Yes			Yes	Yes

Field	Description
User Name	The user's unique name.
Alias Name	An alternative name or id for the user that is not necessarily unique.
Path	Specifies the AD path that identifies users for PowerTerm WebConnect.
Authentication	Specifies authentication type.
Created	Date and time the user was created.
Modified	Date and time the user was last modified.
Rights	Specifies the user's administrative rights.
Default Group	The user's default group.
Free	Specifies the user's connection accessibility.
Access Limit Mode	Specifies the access level.
Access From	Specifies the machines or IP addresses from which the user is allowed to access PowerTerm WebConnect.
Concurrent Machines	Specifies that the user is allowed to log on simultaneously from multiple computers.
Enabled	Specifies if the user is active.
Max. Concurrent Sessions	The maximum number of concurrent sessions that the user may have.
Highest Reconnect Mode	Specifies the reconnect level.

Sessions Count	The total number of sessions currently being used by the user.
First Entrance	The date and time of the first login of the user since the server was activated.
Last Entrance	The date and time of the last login of the user since the server was activated.
Logins History Count	The number of logins for a particular user since the server was activated.
Output Bytes	The total bytes of application traffic that were sent to all the clients used by this user since the server was activated.
Input Bytes	The total bytes of application traffic that were received from all the clients used by this user since the server was activated.
Output Messages	The total number application messages that were sent to all the clients used by this user since the server was activate.
Input Messages	The total number of application messages that were received from all clients used by the user.

Groups Pane

Group Name	Active Users Count	Sessions Count	First Entrance	Last Entrance
Advanced Users				
Expert Users				
Novice Users				
Super Users				

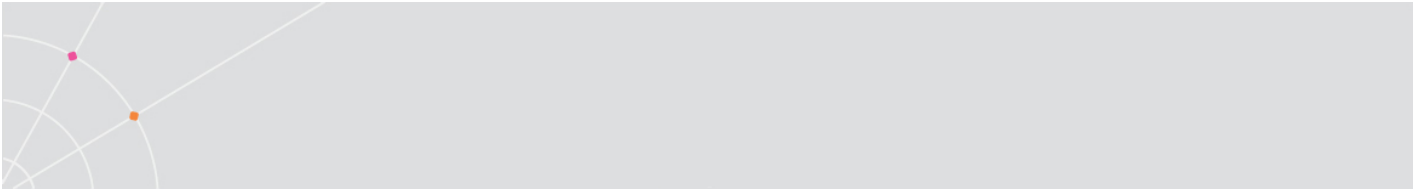
Field	Description
Group Name	The group's unique name.
Created	Date and time the group was created.
Modified	Date and time the group was last modified.
Enabled	Specifies if the group is activated.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions that the members of the group may have.
Highest Reconnect Mode	Specifies the reconnect level.

Allow Access From	Specifies the machines or IP addresses from which the user is allowed to access PowerTerm WebConnect.
Active Users Count	The total number of group members that are currently active.
Sessions Count	The total number of session that are currently being used by the entire group.
First Entrance	The date and time of the first login of any group member, since the server was activated.
Last Entrance	The date and time of the last login of any group member, since the server was activated.

Client Sessions Window

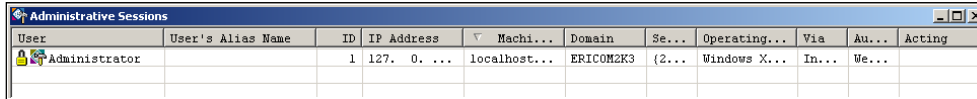
SID	ID	User	User's Alias Name	Machine / Acco...	Type	Acting	Connection Target

Field	Description
SID	Session identification as specified by the remote client.
ID	Unique internal identification.
User	The session user's unique name.
User's Alias Name	An alternative name or id for the session user that is not necessarily unique.
Group	The group currently associated with the session.
IP Address	The remote client's IP address.
Machine/Account	The remote machine's name and the user's account name in the remote operating system.
Domain	Specifies the client's domain.
Seat GUID	Specifies the client's workplace ID.
Operating System	The operating system used by the client.
Version	Specifies the PowerTerm WebConnect client's current version.
License	Specifies the license number.
Via	The connection point through which the remote client



	has connected to the server.
Type	An asterisk (*) after 'ActiveX' indicates that the server is used as a gateway between the host and the remote client.
Authentication Mode	Specifies authentication type.
Security	The security type used between the remote client and the host.
Acting	The text name that reveals the target to which the client is connected.
Connection Target	Specifies where the client is connected to.
Started at	Date and time of when the client started the connection.
Reconnect Mode	The user's reconnect level.
Reconnect Up-To	The maximum times the client can try to reconnect.
Reconnects Count	The amount of times the client tried to reconnect.
Last Output	Date and time of last transmission output.
Last Input	Date and time of last transmission input.
Output Bytes	The total bytes of application traffic that were sent to the session.
Input Bytes	The total bytes of application traffic that were received from the session.
Output Messages	The total of application packets that were sent to the session.
Input Messages	The total of application packets that were received from the session.
Output Packet Max. Size	The maximum size of an output packet.
Input Packet Max. Size	The maximum size of an input packet.
Channel Input Max. Size	The maximum packet size that has passed through the channel.
Gateway Input Max. Size	The maximum packet size that has passed through the gateway.
Buffered I/O Count	The number of bottlenecks that resulted from sending data to the session.

Administrative Sessions Window

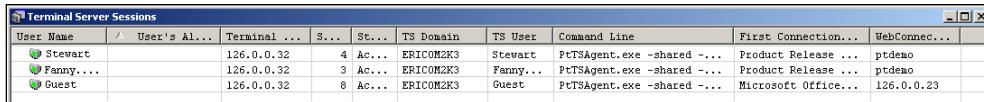


User	User's Alias Name	ID	IP Address	Machi...	Domain	Se...	Operating...	Via	Au...	Acting
Administrator		1	127. 0. ...	localhost...	ERICOM2K3	(2...	Windows X...	In...	We...	

Field	Description
User	The session user's unique name.
User's Alias Name	An alternative name or id for the session user that is not necessarily unique.
ID	The user's ID.
IP Address	The user's IP address.
Machine/Account	The remote machine name and the user's account name in the remote operating system.
Domain	Specifies the administrator's domain.
Seat GUID	Specifies the administrator's workplace ID.
Operating System	The operating system used by the administrator.
Via	The connection point through which the remote client has connected to the server.
Authentication Mode	Specifies authentication type.
Acting	The text name that reveals the target to which the client is connected.
Started at	The date and time of client's login to the server.
Reconnect Mode	The user's reconnect level.
Last Output	Date and time of last transmission output.
Last Input	Date and time of last transmission input.
Output Bytes	The total bytes of application traffic that were sent to the session.
Input Bytes	The total bytes of application traffic that were received from the session.
Output Messages	The total of application packets that were sent to the session.
Input Messages	The total of application packets that were received from the session.
Output Packet Max.	The maximum size of an output packet.

Size	
Input Packet Max. Size	The maximum size of an input packet.
Channel Input Max. Size	The maximum packet size that has passed through the channel.
Gateway Input Max. Size	The maximum packet size that has passed through the gateway.
Buffered I/O Count	The number of bottlenecks that resulted from sending data to the session.
Reconnect Up-To	The maximum times the administrator can try to reconnect.
Reconnects Count	The amount of times the administrator tried to reconnect.

Terminal Server Sessions



User Name	User's Alias	Terminal ...	S...	St...	TS Domain	TS User	Command Line	First Connection...	WebConnec...
Stewart		126.0.0.32	4	Ac...	ERICOM2K3	Stewart	PcTSAgent.exe -shared -...	Product Release ...	ptdemo
Fanny...		126.0.0.32	3	Ac...	ERICOM2K3	Fanny...	PcTSAgent.exe -shared -...	Product Release ...	ptdemo
Guest		126.0.0.32	0	Ac...	ERICOM2K3	Guest	PcTSAgent.exe -shared -...	Microsoft Office...	126.0.0.23

Field	Description
User Name	The session user's unique name.
User's Alias Name	An alternative name or id for the session user that is not necessarily unique.
Terminal Server	Specifies the connected
Session ID	The terminal server unique id number.
Status	Specifies if the connection is active or disconnected.
TS Domain	The terminal server's domain name.
TS User	The terminal server's user name.
Command Line	Specifies RemoteView's command line.
First Connection Name	The name of the application that first started the session.
WebConnect Server	Specifies through which PowerTerm WebConnect server the application is connected.

Machines Window

IP Ad...	Name	OS Ac...	Seat GUID	Int...	Sess...	First L...	Last L...	Logins His...	Lost Log...
127.0.0.1	localhost		{2CD06...}		1	08/23/0...	08/23/...	2	

Field	Description
IP Address	The remote client's IP address.
Name	The machine name.
OS Account	The user's account name in the remote operating system.
Seat GUID	Specifies the machine's workplace ID.
Intruders Count	The number of intruders currently detected.
Sessions Count	The total number of sessions that are currently being logged in from this machine.
First Login	Date and time of the first login from this machine.
Last Login	Date and time of the last login from this machine.
Login History Count	The number of logins.
Lost Logins Count	The number of unintentionally disconnected logins.

Intruders Window

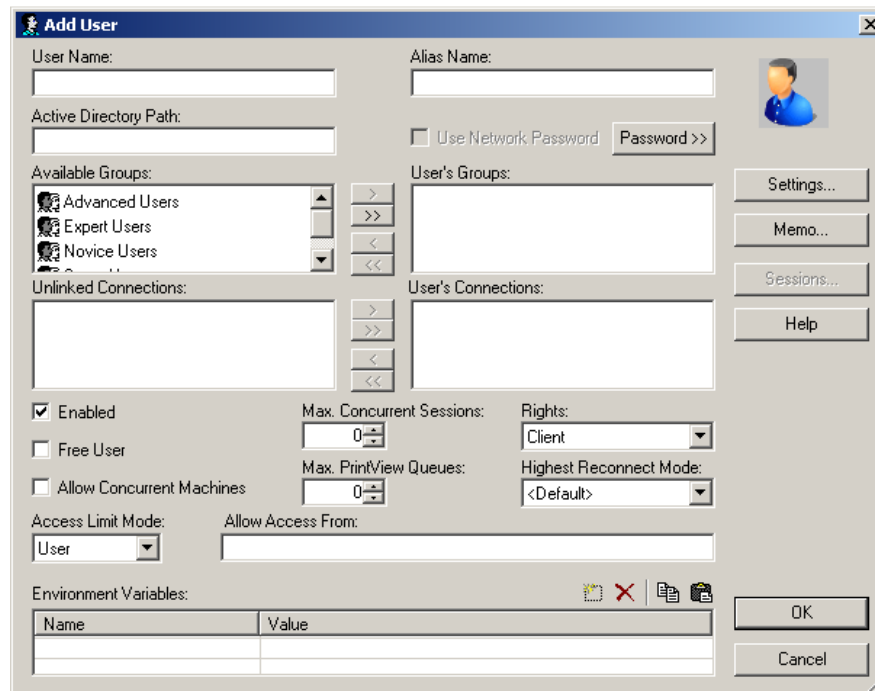
User Name	Machine	Reason	Attempts Count	Intrusions Count	First Attempt	Last Attempt

Field	Description
User Name	The intruder's user name.
Machine	The intruder's machine name.
Reason	The reason the intruder was detected.
Attempts Count	The number of times an intruder attempted to login to PowerTerm WebConnect Server.
Intrusions Count	The number of times the intruder was punished for attempting to enter the system.
First Attempt	The date and time of first try to enter the system.

Last Attempt	The date and time of last try to enter the system.
--------------	--

Properties Dialogs

User Properties Dialog

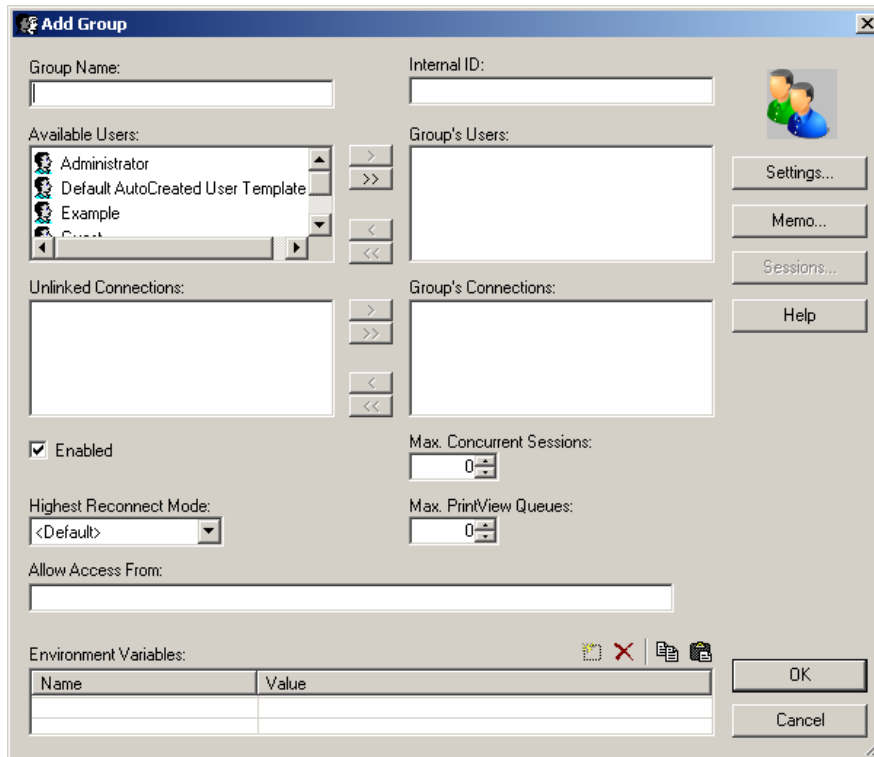


Field	Description
User Name	The user's unique name.
Alias Name	An alternative name or id for the user that is not necessarily unique.
Active Directory Path	Identifies users for PowerTerm WebConnect.
Use Network Password	Specifies that PowerTerm WebConnect Server authenticates the user with the network.
Password	Specifies a user password, unique for PowerTerm WebConnect Server.
Available Groups/Unlinked Connections	Lists all the groups and free connections that the user can be a member of.
User's Groups/User's	Lists all the groups and connections affiliated with

Connections	the user.
Enabled	Activates the user. (Only active users can connect to the server.)
Free User	Allows the user to connect to any accessible host and to specify connection properties.
Allow Concurrent Machines	Allows the user to log on simultaneously from multiple machines.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions the user may have.
Rights	Specifies the user's administrative rights, if at all.
Highest Reconnect Mode	Specifies the reconnect level.
Access Limit Mode	Specifies the access level.
Allow Access From	Specifies the machines or IP addresses from which the user is allowed to access PowerTerm WebConnect.
Environment Variables	Specifies variable names and associated values for the specific user.
Settings	Opens the Terminal Setup dialog to modify client settings for the user.
Memo	Opens a text file to enter free-form information about the user.
Sessions	Opens the Sessions information pane for the user.
Help	Opens PowerTerm WebConnect Administration Console online help.

Group Properties Dialog

For a more detailed description of the features, see chapter **Error! Reference source not found.**



Setting	Description
Group Name	The group's unique name.
Internal ID	An alternative name or id for the user that is not necessarily unique.
Available Users/Unlinked Connections	Lists all the users and free connections that can belong to the group.
Group's Users/Group's Connections	Lists all the users and connections affiliated with the group.
Enabled	Activates the group.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions the members of the group may have.
Highest Reconnect Mode	Specifies the reconnect level.
Allow Access From	Specifies the machines or IP addresses from which the user is allowed to access PowerTerm WebConnect.
Environment Variables	Specifies variable names and associated values for the group members.

Settings	Opens the Terminal Setup dialog to modify client settings for the group members.
Memo	Opens a text file to enter free-form information about the group.
Sessions	Opens the Sessions information pane for the group.
Help	Opens PowerTerm WebConnect Administration Console online help.

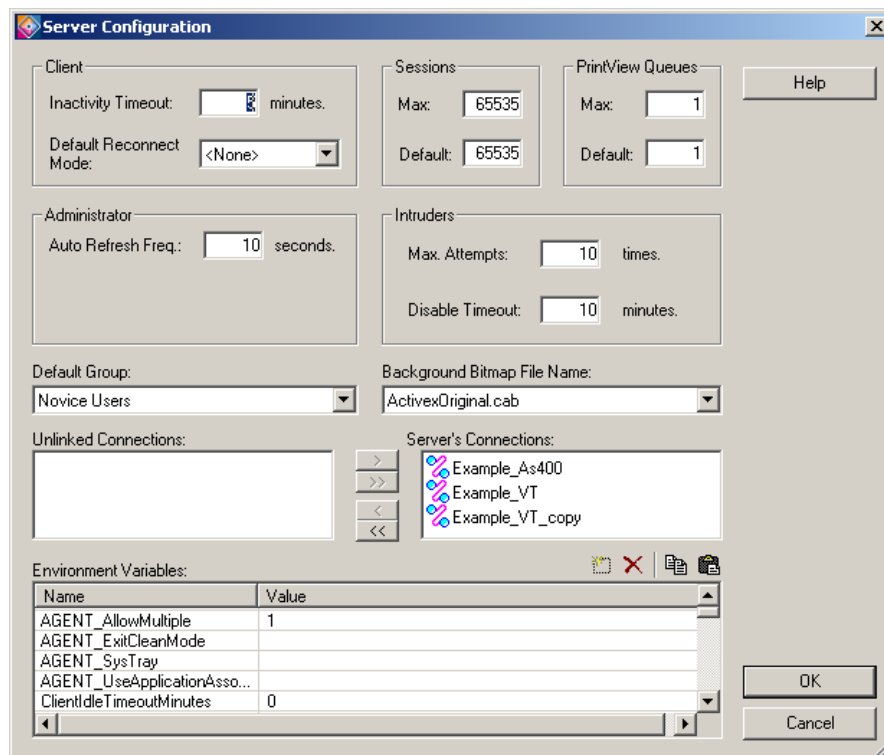
Connection Properties Dialog

Field	Description
Connection Name	The connection's unique name.
Display Name	A display name for the connection that is not necessary unique.

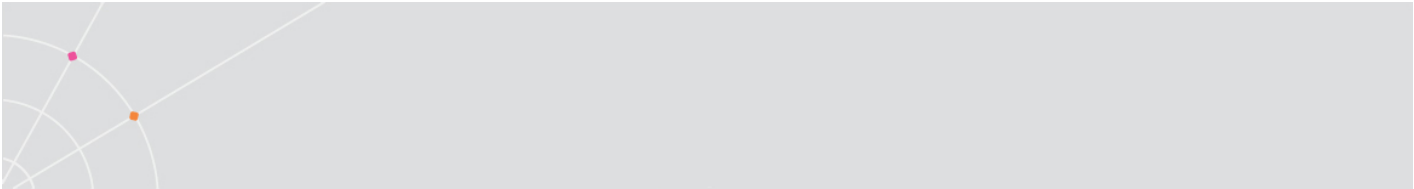
Enabled	Activates the connection.
Usage Type	Specifies how the connection will be used: <i>Hidden</i> , can only be activated from a login script. <i>Child</i> , owned by another connection. <i>Regular</i> , a regular connection. <i>Owner</i> , a regular connection which, when closed, will automatically shut down all associated connections (child connections, connections opened by the login script, etc.).
Owner	Specifies the connection's owner.
Alternate Connection	Specifies another connection to be used if this connection fails to connect to the host.
LD Groups	Opens the Add/Remove Objects for New Connection dialog.
Category	Specifies whether the connection belongs to a legacy host or to an RDP resource.
Terminal Type	Specifies terminal emulation type.
Terminal Model	Specifies terminal emulation model.
Communication Type	Specifies the communication protocol used by the host. (Different protocols will display different parameters required.)
Network Name	Specifies the connection point type. Network names are defined in the PtServer_Connections.ini file. The three predefined modes are: <i>Gateway</i> , connections accesses the host via Gateway mode. <i>No Gateway</i> , connections accesses the host via Direct mode. <i>Public</i> , connections accesses the host via Gateway mode if <i>Reconnect</i> is used. Otherwise connections will access the host via Direct mode.
Environmental Variables	Specifies variable names and associated values for the connection.
Settings	Opens the Terminal Setup dialog to modify client settings for the connection.
Key Mapping	Opens the Keyboard Mapping dialog to enable mapping

	keys with desired character or script.
Power Pad	Opens the Power Pad & Function Buttons dialog to define Power Pad and Function buttons.
Login Script	Opens the <i>Login Script.ps1</i> in Notepad to be edited as a text file.
Memo	Opens a text file to enter free-form information about the connection.
Help	Opens PowerTerm WebConnect Administration Console online help.

Server Configuration Dialog

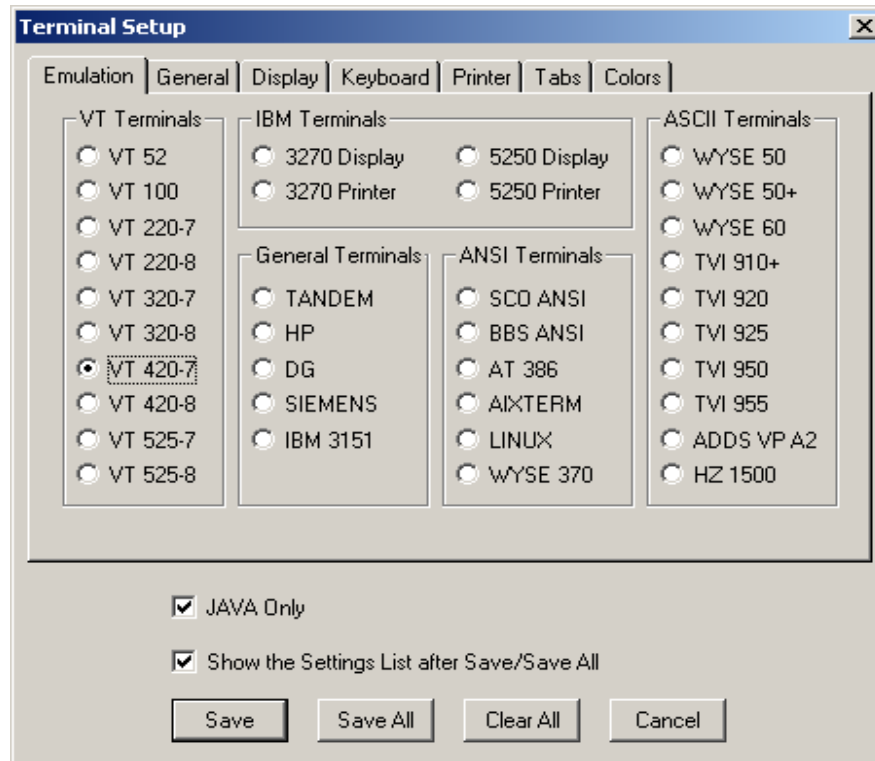


Setting	Description
Client Inactivity Timeout	Specifies the inactivity timeout for all clients.
Default Reconnect Mode	Specifies the default reconnect level.
Sessions: Max	Specifies the maximum session limit for all clients.
Sessions: Default	Specifies the default session limit for all



	clients.
Administrator Auto Refresh Freq.	Specifies the time interval for the Administration Tools auto refresh feature.
Intruders: Max. Attempts	The number of times a user can try to login before it is considered to be an intruder.
Intruders: Disable Timeout	Specifies the amount of time in minutes that PowerTerm WebConnect Server refuses to login a valid user after detecting an intruder.
Default Group	Specifies the default group for users that have no specified default group on user level.
Background Bitmap File Name	Sets a background bitmap for clients that support this feature.
Unlinked Connections	Lists all the free connections that can belong to the server.
Server's Connections	Lists all the connections affiliated with the server.
Environment Variables	Specifies variable names and associated values for the server.

Settings Dialog (for Emulation Clients)



- *Emulation*, displays supported terminal emulations and enables you to select a terminal type.
- *General*, defines parameters for the terminal emulation type.
- *Display*, (non-IBM emulations only) defines display settings for the emulation window.
- *Keyboard*, defines keyboard setup parameters.
- *Printer*, defines printer parameters.
- *Tabs*, (VT emulations only) defines tab stops in the work area.
- *Colors*, defines color settings for the emulation window.

NOTE The Emulation type that you select changes the tabs (property pages) displayed in the Terminal Setup dialog

General tab

Option	Description
NRC Set	Determines the communication and keyboard character set for 7-bit data only.

UPS Set	Determines the communication and keyboard character set for 8-bit data only
8 bit Controls	<p>This option is only enabled when UPS Set is specifies as Code Page 437 and up.</p> <p><i>Disable</i>, determines if 0x80 to 0xAF are displayed characters.</p> <p><i>Enable</i>, determines if 0x80 to 0xAD are control characters.</p> <p><i>0x9B</i>, all characters are displayed character except 0x9B, which is a control character.</p>
Online	Equivalent to Terminal <i>On Line</i> (Off Line).
New Line	Determines whether the <Enter> key generates only a carriage return or a carriage return/line fee combination.
CR->CRLF	Adds a line feed after each single carriage return (one that has no line feed following it) when in slave printing mode.
Use 8 Bit Data Characters	Select this parameter if the communication data is in 8-bit character format. Clear it for 7-bit characters. When cleared, the 8 th bit is truncated. If you receive 7-bit data, you can convert it to 8-bit data for printing on the slave printer.
User Defined Keys Locked	<p>Determines whether applications on the host system can override your user-defined keys (UDKs) when you have defined a function key that conflicts with how the host wants to use this key. UDKs let you use a single key for multiple keystrokes. 256 bytes are available to program the 15 UDKs. The key definitions are loaded sequentially (from F6 to F20) so that if you reach the 256-byte limit, more definitions cannot be loaded.</p> <p><i>Locked</i>, prevents UDKs from being overridden.</p> <p><i>Unlocked</i>, allows UDKs to be overridden.</p>
Cursor Keys	<p>Determines the behavior of the four arrow keys.</p> <p><i>Normal</i>, generates ANSI-standard control sequences for moving the cursor.</p> <p><i>Application</i>, generates modify application program functions.</p>

Keypad	<p>Determines the effects of the numeric keypad on your keyboard.</p> <p><i>Numeric</i>, keypad keys insert number.</p> <p><i>Application</i>, keypad keys generate control sequences that can be used by some applications.</p> <p><i>NumLock</i>, enables or disables the NumLock keyboard function in respect to the above Numeric and Application modes.</p>
Cursor coupling	<p><i>Vertical</i>, determines whether the user window pans with the cursor when the cursor moves past the top or bottom border of the user windows.</p> <p><i>Page</i>, determines if a new page appears in the display when the cursor moves to a new page.</p>
Status Line	<p><i>None</i>, displays an emulation screen without the status line.</p> <p><i>Indicator</i>, displays the status line.</p> <p><i>Host Writable</i>, displays the status line sent by the host.</p>
Label Line	Displays a status line on the top and bottom line of the emulation screen.
Show Response Time	Displays the number of seconds that elapsed between the time data was sent to the host and the host response time.
ID	Determines the ID returned by the emulation program to the host. Make sure the ID is understood by the host application.
\$=5B	<p>Determines whether the character 5B represents a '\$' or a cents sign.</p> <p>For RTL languages only.</p>
Cursor Ruler	<p>Select <i>Visible</i> to display full-screen, vertical or horizontal lines as cursor ruler (cross hair guide).</p> <p><i>Cross Hair</i>, displays the cursor ruler as a horizontal and vertical line.</p> <p><i>Horizontal</i>, displays the cursor ruler as a horizontal line only.</p> <p><i>Vertical</i>, displays the cursor ruler as a vertical line only.</p>

Cursor	<p>Controls the cursor appearance and functionality: <i>Block/Underline/Visible/Blink</i>, controls the cursor appearance.</p> <p><i>Ins Change</i>, when selected it enables toggling the cursor between underline and block appearance, by clicking the Ins (insert) button.</p>
Appearance	<p><i>Power GUI</i>, displays data in a window with 3D look & feel. Use system fonts larger than 10 pt for better results.</p> <p><i>Show Frame</i>, places a frame around the text area of the emulation.</p>
HLLAPI Names	<p>Specifies the name of an HLLAPI session.</p> <p><i>Short/Long</i>, enables you to specify the short and the long HLLAPI name</p>
Code Page	<p>Specifies the host and PC/Terminal (keyboard) terminal character sets.</p>
Alternate Size	<p><i>Enable</i>, select to override the terminal alternate size with a specific size.</p> <p><i>Rows/Columns</i>, type the required number.</p>

Display tab

Option	Description
Reverse Display Colors	Reverses the text and background colors in the work area.
Auto-wrap Characters	Wraps words at the end of a line and the cursor moves to the next line.
History Scroll Bar	Displays the vertical history scroll bar along the right edge of the emulation screen, which enables you to scroll through the data displayed previously on the screen. Selecting <i>Clear History</i> from the <i>Edit</i> menu can erase the History buffer.
Cursor Ruler	<p>Select <i>Visible</i> to display full-screen, vertical or horizontal lines as cursor ruler (cross hair guide).</p> <p><i>Cross Hair</i>, displays the cursor ruler as a horizontal and vertical line.</p> <p><i>Horizontal</i>, displays the cursor ruler as a horizontal line only.</p>

	<i>Vertical</i> , displays the cursor ruler as a vertical line only.
Cursor	Controls the cursor appearance and functionality: <i>Block/Underline/Visible/Blink</i> , controls the cursor appearance. <i>Ins Change</i> , when selected it enables toggling the cursor between underline and block appearance, by clicking the <i>Ins</i> (insert) button.
Ctrl Characters	<i>Display</i> , displays the control characters. <i>Interpret</i> , performs the regular terminal behavior as affected by control characters.
Power GUI	Displays data in a window with 3D look & feel. Use system fonts larger than 10 pt for better results.
Show Frame	Places a frame around the text area of the emulation.
Dimensions	Determines the number of characters (columns) per displayed line, and the number of lines to be displayed in the work area. Characters are scaled according to the selected values. Type a different value in the Other box instead of choosing one of the standard options (80 and 13). <i>Limit Font Size</i> , allows PowerTerm fonts to use only the optimal font size, especially for frames. Not recommended for normal text on large screens.
Scrolling	Determines the pace at which data is displayed in the work area as it arrives. If you select Jump, you should also determine the Jump Scroll Speed that is measured in number of line units where the higher the value, the faster the scrolling. <i>Unlimited</i> , displays data without delaying communication. <i>Page</i> , scrolls data by full screens. <i>Smooth</i> , is equivalent to a Jump Scroll Speed of 1.
Enabling Soft Fonts	Enables you to work with VT soft fonts. The fonts will be loaded from the host application.

Keyboard tab

Option	Description
--------	-------------

Capslock Mode	<p>Determines the behavior of the <i>Caps Lock</i> key.</p> <p><i>Caps (Unix)</i>, locks alphabet keys on main keypad in uppercase.</p> <p><i>Shift</i>, locks alphabet and numeric keys on main keypad in shift setting. Pressing the shift button on your keyboard will release shift-lock mode.</p> <p><i>Reverse (Win)</i>, has the same behavior as Caps Lock, however pressing the shift button on your keyboard reverses the caps operation.</p> <p><i>Always On</i>, enables you to toggle to a different application and turn Caps Lock mode off. On return to the emulation client it will automatically revert to Caps Lock on.</p>
Backspace Key Sends Delete	Determines whether the <Backspace> key sends 'Delete' or an actual backspace.
Backspace Deletes	Select to delete characters by pressing the <Backspace> key on the keyboard.
Auto Repeat	Repeatedly displays the character which key is being continuously pressed down.
Key Click	Gives off a click sound when you press a key on the keyboard.
Warning Bell	Determines whether the terminal sounds a bell tone when receiving the "bell" (ASCII 7) character. (For operating errors, mail messages, etc.)
Margin Bell	Determines whether the terminal sounds a bell tone when the cursor reaches the right margin.
Lock Numeric Fields	Determines whether the keyboard is locked when you try to enter non-numeric data.
Typeahead	Types data ahead, before the host responds.
Automatic Reset Key	If the keyboard is locked, a reset key sequence is generated prior to when you click on the tab key to advance to the next field.
Numpad Decimal Sends Comma	Specifies that the Numeric Pad's decimal key sends a comma instead of a decimal.
Use Emulator Alt Keys	Select to make an <Alt> key perform the terminal operation even if Windows OS has an operation mapped to the same key.
Local Echo	Determines whether keyboard input is displayed

	<p>(echoed) on your screen.</p> <p><i>Select</i>, to display the keyboard input even if the host system does not echo your input.</p> <p><i>Clear</i>, to send the keyboard input to the host system without being displayed on the screen (unless, invariably, the host system automatically echoes the characters).</p>
Use VT Keyboard Mode	Changes your keyboard into a Digital VT keyboard mode. In this mode, the PC keyboard operates as close to a VT keyboard as possible, and takes full advantage of LK450 Digital keyboards.
Non SNA System Wait	Determines whether the <i>System Wait</i> in the IBM 3270 emulation will act as a <i>System Wait</i> in a non-SNA terminal.
Answerback Message	<p>Specifies an answerback message and its display.</p> <p><i>Clear</i>, deletes its message.</p> <p><i>Conceal</i>, hides the message without deleting it.</p>

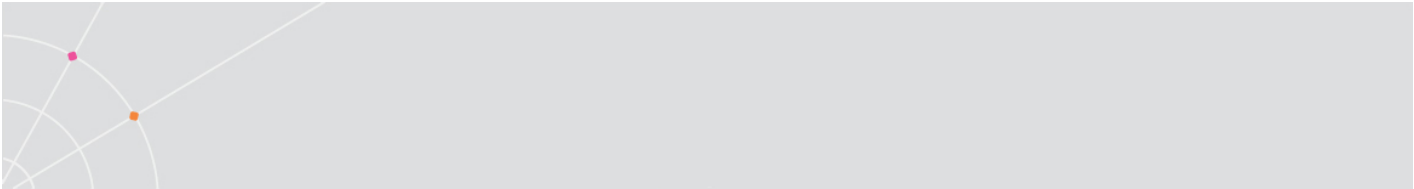
Printer tab

Option	Description
Print Device	<p>Allows you to select a printing output channel.</p> <p><i>None</i>, no destination was assigned. The Device Name is disabled. Printer data is received by the terminal, but discarded (not printed).</p> <p><i>Device</i>, senses printing to the device you designate in the Device name text box. This can be a device such as COM1, COM2, COM3, etc. in the Device Name text box, you can also specify communication parameters, for example: COM 1:9600,8</p> <p><i>File</i>, sends printing to the file specified in the File Name text field.</p> <p><i>AUX</i>, sends printing to the auxiliary port.</p>
Append Form Feed	Adds a form feed (page eject) after each printing job.
LF -> CRLF	Adds a line feed after each single carriage return (one that has no line feed following it) when in slave printing mode.

Print Line Graphics as Text	Converts line graphics to text. This speeds up printing on a slow dot-matrix printer.
Device Name	Specifies the printing device. Enabled when you select <i>Device</i> in <i>Print Device</i> . Default: LPT1
File Name	Specifies the file name. Enabled when you select <i>File</i> in <i>Print Device</i> . <i>File Creation</i> , determines whether you want <i>Append</i> or <i>Overwrite</i> mode.
Print Screen Data Conversion	Converts data to Host or UTF-8 character sets or prints in <i>Graphics</i> mode. <i>None</i> , does not convert data. Text mode is designated by selecting Host, UTF-8 character sets or None.
Slave Printer Data Conversion	Converts data to Host or UTF-8 character sets or prints in <i>Graphics</i> mode. <i>None</i> , does not convert data. Text mode is designated by selecting Host, UTF-8 character sets or None.
Slave Printer Job Delimiter	Specifies the job delimiter character that will divide the data into print jobs, thus disabling the escape sequences arriving from the host application.
Delay for Print Closing (Seconds)	The command to close the printer queue is delayed by the number of seconds that you determine. This command only takes effect if no open command is issued in the meantime. Important for printing to cut sheet printer (for example, inkjets/lasers) and network printers.

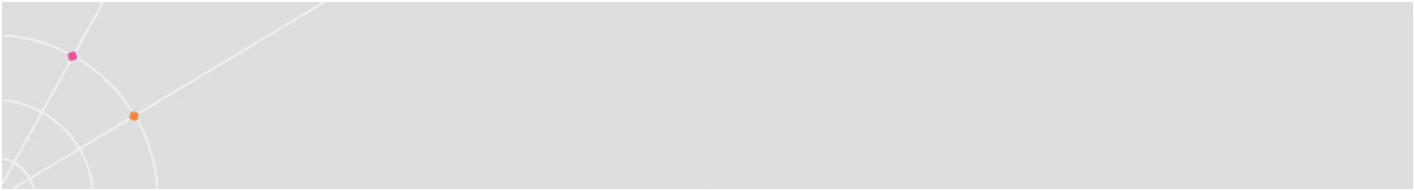
Tabs tab

Option	Description
Tabs Stops	Click anywhere within the <i>Tab Stops</i> area to set tab stops manually.
Set Every	Sets the tab stops at even intervals according to the number specified in the adjacent field.
Clear All	Clears all tab stops.



Colors tab


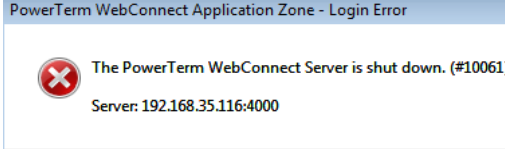
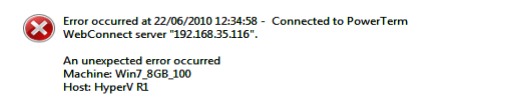
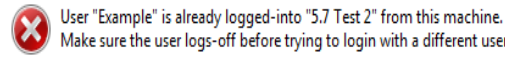
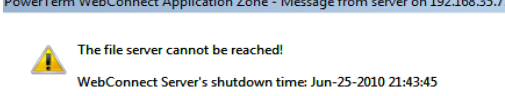
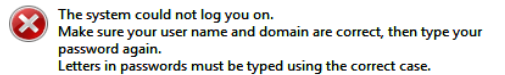
Option	Description
Preview box	Shows the result of your selections.
Enable Underline	Enables underlined characters. For data transmitted from the host with the Underline attribute, clear to disable displaying data with the underline.
Enable Blink	Enables blinking. For data transmitted from the host with the Blink attribute, clear to disable blinking data.
Coloring method dropdown list	<i>Default</i> , uses the default color type for each emulation type: -VT and Siemens – Attribute & ANSI colors -ANSI and HP – ANSI colors -All others – Attribute colors (i.e. not affected by setting to a different value). <i>Attribute</i> , colors based on the attributes. For example, you can select different colors for bold, for underline, and for bold/underline. <i>ANSI</i> , colors based on host-defined colors. For example, the host sends "red foreground on blue background" however you can select the default ANSI color. Different attribute do not affect colors. <i>Attribute & ANSI</i> , uses both Attribute and ANSI colors as explained above.
Column Separator	Displays a period as a column separator in fields with the column separator attribute.
ANSI 8 Color Mode	A regular terminal has 16 colors (8 colors with the Bold attribute applied to them and 8 colors without). The <i>Background</i> color never has the bold attribute (therefore it is "dark") while the <i>Text</i> (foreground) is always mapped to the color with the Bold (bright, light) attribute. <i>Selected</i> , each entity (text, background) can have any of the 8 colors mapped to them. <i>Cleared</i> , each entity (text, background) can have any of the 16 colors mapped to them.
Color Frame	Select to draw a frame on the screen.




Select Attribute	Select the attribute for which you want to define foreground and background colors. Attributes change according to the emulation type you selected in the Connection properties dialog. Generally, the attribute of the entire screen is <i>Normal</i> . The color for the Normal attribute determines the color of the entire work area.
Text	Select the color that will apply to the text (foreground) of the display.
Background	Select the color that will apply to the background of the text.
Bitmap Filename	Specify a bitmap file as the screen background.

30. APPENDIX C – TECHNICAL SUPPORT

WebConnect Troubleshooting Guide

Error Message	Reason
 <p>Credential token unknown</p>	<ol style="list-style-type: none"> 1) The address of the application shortcut does not match that of the Application Zone or Portal. Check that the Comportal.ini Address= field contains the correct PTWC address. 2) There is secondary ticket login attempt performed by Application Portal (although the user is already logged in). 3) The network socket has changed (i.e., a VPN is established to the same network) - restore the original connection or log off Ericom and relogin.
<p>PowerTerm WebConnect Application Zone - Login Error</p>  <p>Server is shut down 10061</p>	<ol style="list-style-type: none"> 1) The WebConnect Server is down 2) The WebConnect Server is not reachable 3) The WebConnect server is now in Failover mode
 <p>Unexpected error occurred</p>	<p>The VDI desktop that is being accessed is not in a Pool. Add the desktop to a new or existing pool</p>
 <p>User is already logged</p>	<p>Only one user can be logged into Application Zone on a system. In this message, the user "Example" is trying to logon from a system where an Application Zone is already running for another user.</p>
<p>PowerTerm WebConnect Application Zone - Message from server on 192.168.35.77:4...</p>  <p>File server cannot be reached</p>	<p>The user is connected to a WebConnect server in Failover mode and the shared database is no longer available. Restore the shared database to resolve.</p>
 <p>System could not log you on</p>	<p>The credentials entered are not authorized; verify the spelling of the username and password.</p>

Authentication Server Troubleshooting Guide

Error Message	Reason
 Ericom Authentication Server error (code 10030001): The RADIUS server did not respond. RADIUS server did not respond	Passcode may be invalid. Verify connectivity to 2FA server. Verify that 2FA server is accepting connections from the correct address of the authentication server.
Unable to connect to https:// Reason: Ericom Authentication Server error (code 10030002): Authentication error: ACCESS_REJECT Authentication error: Access_Reject	The "Authentication Method" is not correctly set in the Administration console. Possible user enrollment issue on the 2FA server. Check 2FA server log for errors.
Entering the password and passcode in the password field does not work	Verify that the 2FA server is <i>not</i> set for "challenge response".

ESG Failover Log Verification

If multiple ESG's are used under the variable SecureGateway, the failover function may be verified by looking in the ESG log. Look for the failed entry and then the successful one. For example:

```
Unable to connect to Ericom PowerTerm WebConnect Server.
```

```
Info : Failed Resolving host name / IP address  
"esg1.acme.com:443"
```

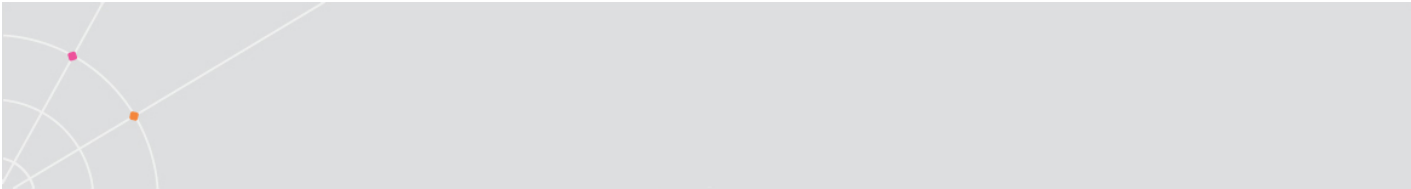
```
Reason: The requested name is valid, but no data of the requested  
type was found
```

```
Requesting to connect to WebConnect Server on esg2.acme.com:4343  
(Resolved to 127.0.0.1)
```

```
Created new session from [::ffff:192.168.1.3] to 127.0.0.1:4000
```

Requesting Technical Assistance

- Send an email to support@ericom.com
- Include images of any error messages
- Include steps on how to reproduce an observed problem
- Specify how many users are affected: one, some, or all

- 
- Specify how many users would be using PowerTerm WebConnect if it becomes an accepted solution
 - Specify the Operating System of the end-user's device (i.e., Android tablet)
 - Specify the Operating System of the PowerTerm WebConnect server (i.e., Windows 2008)
 - Specify the Operating System of the Terminal Server (i.e., Windows 2008)

Technical Support Debug Logs

HINT Ending the log at the point where the problem occurs will expedite the troubleshooting process. If Ericom Support cannot identify the occurrence of the problem, new logs will be requested.

PowerTerm WebConnect Server

In the event of problems related to the PowerTerm WebConnect Server (i.e., connections are lost) the PtServer.log debug log is required for Ericom Support to diagnose the issue.

To create the debug log, open the Main Configuration (PtServer.ini) and modify the *LogFlags* parameter; all values are separated by a space.

Values used to track user activity: *Run, Load, Clients, Connect*

Values used for debugging purposes: *DbgLoadConn, DbgLoadGroup, DbgLoadUser, DbgLogin.*

PowerTerm WebConnect Client

In the event of problems related to the PowerTerm WebConnect client (i.e., applications are not being launched) the ptagent.log and ptrdp.log is required for Ericom Support to diagnose the issue.

To create the debug log, add the parameter /LOG to the ptagent command line or HTML. The ptagent.log will be created upon login, and the ptrdp.log will be generated upon launching of a published application or desktop. On Windows 7, the logs are located at C:\Users\<<userid>\AppData\Local\Ericom

PowerTerm Terminal Server Agent

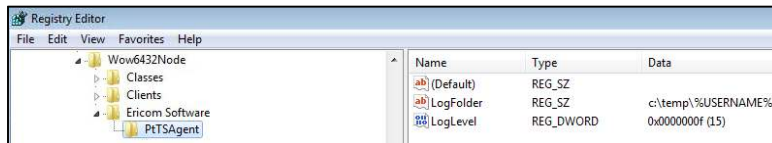
In the event of problems related to the TS Agent (i.e., seamless windows are not appearing properly) a debug log is required for Ericom Support to diagnose the issue.

To create the debug log, the following Registry keys must be updated:

- *LogLevel* – set to 'F'

- *LogFolder* – by default this key is not present in the Registry and is set to %USERPROFILE%.

NOTE To make the log files easier to find, set the *LogFolder* to C:\Temp\%USERNAME%. Make sure that all users being logged have write access to C:\Temp or the configured directory.



PowerTerm Load Balancer

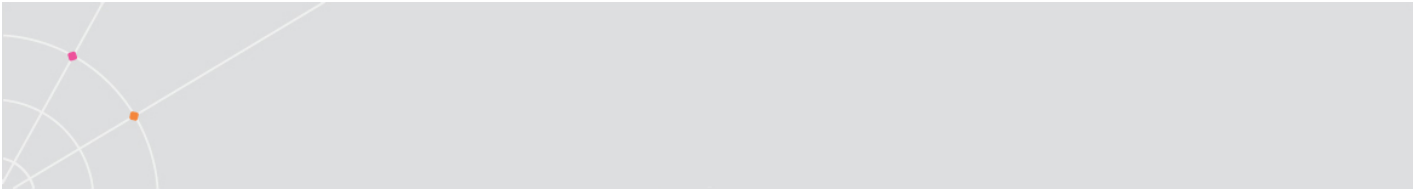
In the event of problems related to the Load Balancer (i.e., one TS server is not receiving connections), send the *PtLoadBlanacerServer.log* and the *LoadBalancer.XML* file to Ericom Support for review. Specify the names of the affected servers. The logging level of the Load Balancer Agent is configured in the Registry if more data is needed (HKLM\Ericom\PtLoadBalancerAgent).

Error message	Explanation
The connection to the Load Balancer has been lost.	The Load Balancer Server service may have stopped. Restart the service.
Failed to add the server.	A server with the same address exists.
Host is not found.	The server that was specified does not exist.

Reporting issues to Ericom Technical Support

To expedite handling of technical support requests, send the following information in the initial request correspondence.

- Send relevant logs based on the nature of the problem (i.e., ptrdp log for client related problems or tsagent.log for seamless window appearance issues).
- Send the Main Configuration file (ptserver.ini). For VDI users, send the Database.XML file.
- Provide the steps to reproduce the problem. If the problem is affecting only a certain application, provide a download link to an evaluation version of the application so Ericom Support may load it for testing and verification.
- Provide a recording of the problem if possible.
- Provide bitmaps of any error messages or the problem itself.
- Inform Ericom Support if the problem is widespread to all users, or only affecting certain users. If just certain users, is there a



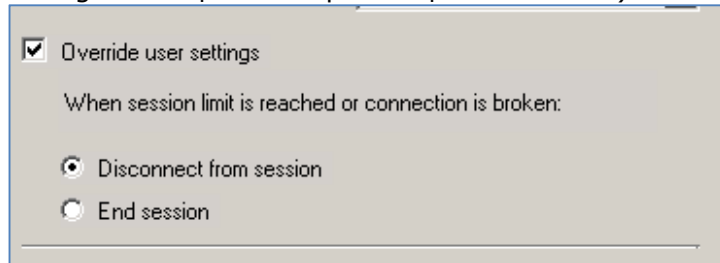
common characteristic among the users (i.e., part of the same Active Directory OU).

- Email all pertinent information requested above to tech.support@ericom.com and a support ticket will be generated. Any missing information will result in a delay in handling of the ticket as more information may be requested.

31. APPENDIX D - TERMINAL SERVER TIPS

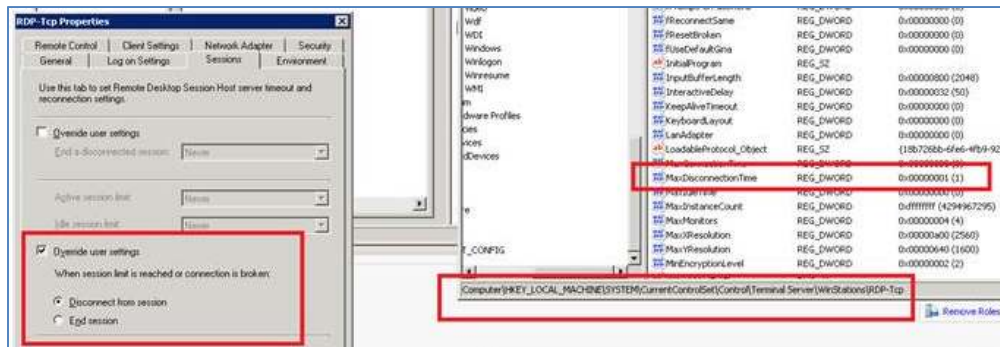
Forcing Disconnected Sessions to Logoff (Windows 2008 R2)

- First set this under the Windows 2008 RDS configuration (RDS Configuration | RDP Properties | Sessions tab):



- Launch Regedit.exe and navigate to:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
- Set fInheritMaxDisconnectionTime to 0
- Set MaxDisconnectionTime (this value is in milliseconds) to 1, so after 1ms of disconnecting - the session is terminated

A reboot is not necessary, but test the change to ensure that it is operating properly.



Hiding/Preventing Access to Drives

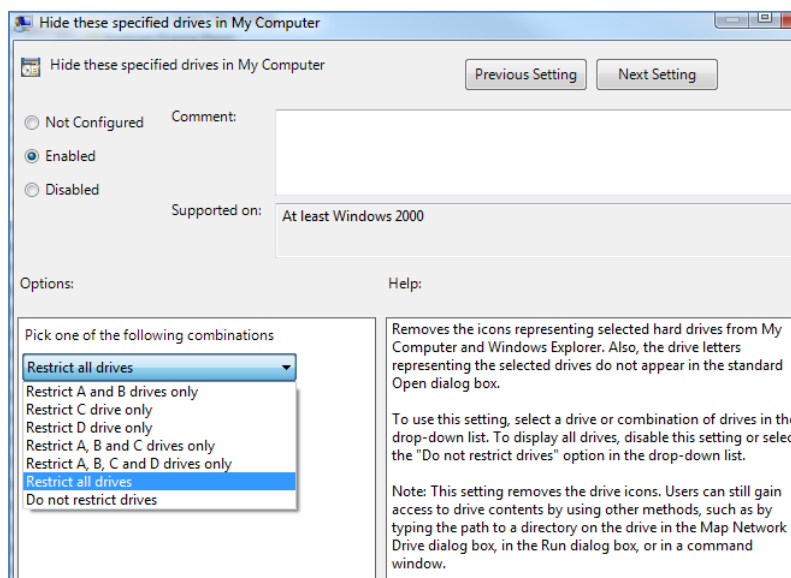
NOTE This content is copied from:
<http://blogs.msdn.com/b/rds/archive/2011/05/26/how-to-restrict-users-from-accessing-local-drives-of-an-rd-session-host-server-while-using-remoteapp-programs.aspx>

Use Group Policy settings to hide and restrict access to drives on the RD Session Host server. By enabling these settings you can ensure that users do not inadvertently access data stored on other drives, or delete or damage programs or other critical system files on drive C.

The following settings are located in the Group Policy Management Console under **User Configuration\Policies\Administrative Templates\Windows Components\Windows Explorer**:

Hide these specified drives in My Computer. You can remove the icons for specified drives from a user's My Computer folder by enabling this setting and using the drop-down list to select the drives you would like to hide. However, this setting does not restrict access to these drives.

Prevent access to drives from My Computer. Enable this setting to prevent users from accessing the chosen combination of drives. Use this setting to lock down the RD Session Host server for users accessing it for their primary desktop.



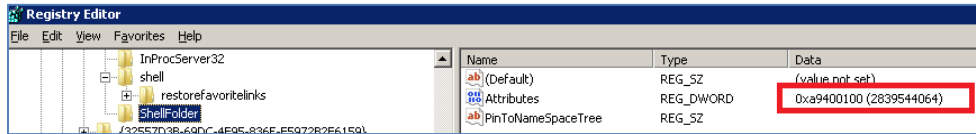
Hiding Favorites from Windows Explorer

The following instructions are derived from this Internet link, please visit this link for detailed instructions:

<http://www.askvg.com/how-to-remove-favorites-from-windows-7-explorers-navigation-pane/>

- Click **Start**, click **Run**, type **regedit**, and then click **OK**.
- Locate: **HKEY_CLASSES_ROOT\CLSID\{323CA680-C24D-4099-B94D-446DD2D7249E}\ShellFolder**

- After you select the subkey that is specified in step 2, right-click **Attributes**, and then click **Modify**.
- Change the **Attributes** value to **a9400100**



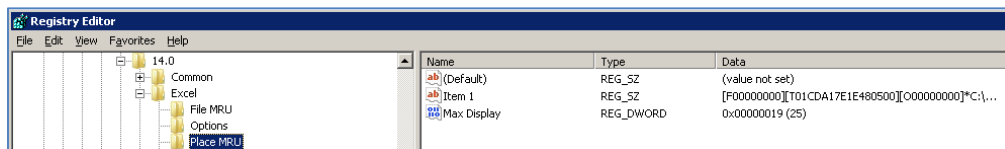
Removing Recent documents list from Excel

The following instructions are derived from this Internet link:

<http://support.microsoft.com/kb/983006/en-us>

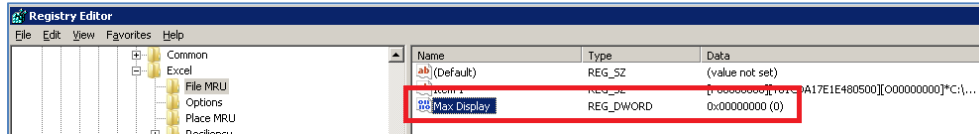
These instructions are similar across all Microsoft Office products. To get started, use Excel and save any file so the proper Registry keys will be generated.

- Exit all Office programs.
- Click **Start**, click **Run**, type **regedit**, and then click **OK**.
- Locate:
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU
- After you select the subkey that is specified in step 3, right-click **Max Display**, and then click **Modify**.
- Click **Decimal**, and in the **Value data** box, type 0 to represent the number of places that you want to list in Recent Places, and then click **OK**. By default, **Max Display** is set to 25.



- Locate:
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\File MRU
- After you select the subkey that is specified in step 6, right-click **Max Display**, and then click **Modify**.
- Click **Decimal**, and in the **Value data** box, type 0 to represent the number of places that you want to list in Recent Files, and then click **OK**. By default, **Max Display** is set to 25.

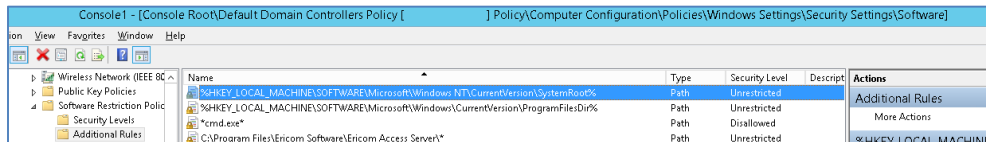
- Repeat steps 3 through 8 for each Office program for which you want to change the number of places that you want to list in Recent Places.
- On the File menu, click Exit to exit Registry Editor.



Restricting Application Launch

Restrict which applications may be launched on the Terminal Server by defining *Software Restriction Policies* in the user's Group Policy Object.

This image shows a sample location in Group Policy where the *cmd.exe* application is *Disallowed*.



This may also be defined on the local server's *Computer Policy* (Windows Settings | Security Settings | Software Restriction Policies) by setting *Path* rules:

Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies\Additional Rules

Windows 2003 sessions are in 8-bit colors

Applications and desktops sessions to Windows 2003 sessions unexpectedly display using 8-bit colors. This is a known Microsoft issue and is covered in this article: <http://support.microsoft.com/kb/942610>



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 or 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