PowerTerm® WebConnect

Version 5.6.1

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 Ltd. 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 express prior written permission of Ericom® Software Ltd.

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

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

- Information in this document is subject to change without notice. Corporate and individual names, and data used in examples herein are fictitious unless otherwise noted.
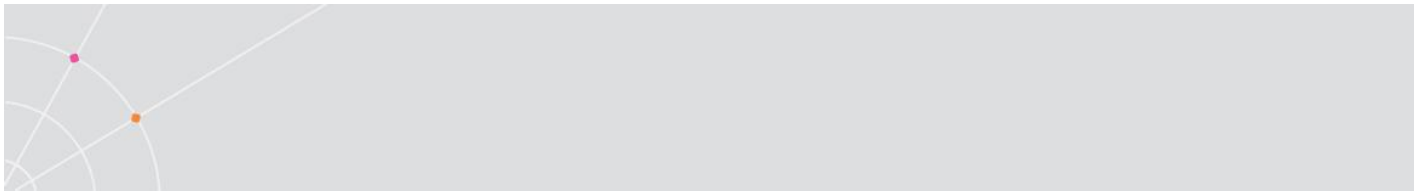
Copyright © 1999-2008 Ericom® Software Ltd.

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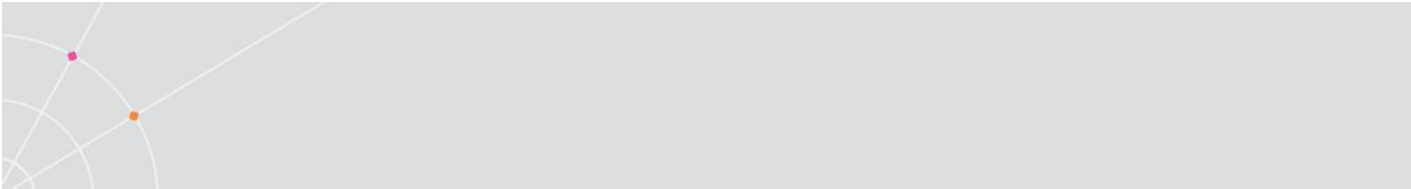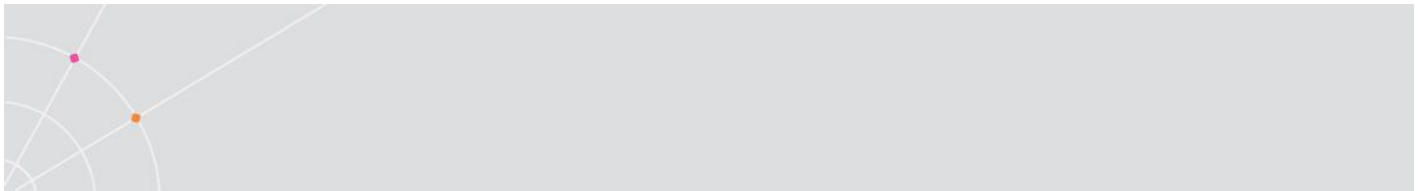
Table of Contents

About this Document

This manual explains PowerTerm WebConnect concepts, as well as how to use the PowerTerm WebConnect Administration Tool and other components of Ericom Software's PowerTerm WebConnect product. It is intended for Administrators of PowerTerm WebConnect. If you need information on using a particular PowerTerm WebConnect Client component, please see the respective user's guide and/or online help.

The document contains the following chapters:

Chap. 1	Introduction	Introduces PowerTerm WebConnect and its Administration Tool.	Pg. 15
Chap. 2	Installing, Starting, and Stopping PowerTerm WebConnect Server and Administration Tool	Explains how to configure PowerTerm WebConnect Server and get its Administration Tool up and running.	Pg. 21
Chap. 3	The Administration Tool: General Reference	A reference guide to PowerTerm WebConnect Administration Tool's menus and dialogs.	Pg. 43
Chap. 4	Directory Services	Explains how to access User, Group and resource information from an external Directory Services.	Pg. 51
Chap. 5	Defining Users and User Groups	Explains how to define Users and User Groups.	Pg. 96
Chap. 6	Defining Connections	Explains how to define connections and use the Publishing Application Wizard.	Pg. 135
Chap. 7	Monitoring Settings, Status, and History	Explains how the administrator monitors the system's activity.	Pg. 160

	Performance	of PowerTerm WebConnect.	
Chap. 24	Useful scripts	Shows examples of different scripts.	Pg. 338
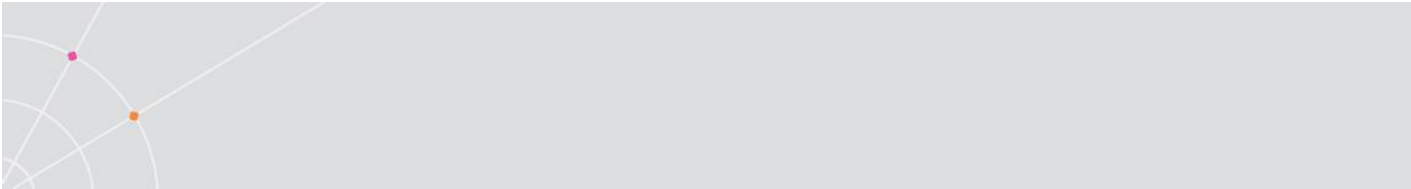
1. Introduction

PowerTerm® WebConnect provides various clients that allow users to interact with centralized computational resources, such as Microsoft Windows Terminal Servers and legacy hosts, using a regular PC, without the need to preinstall the clients. These clients include, among others, PowerTerm WebConnect HostView (which emulates a legacy application terminal), PowerTerm WebConnect RemoteView (for accessing Windows Terminal Servers), and the PowerTerm FTP Client.
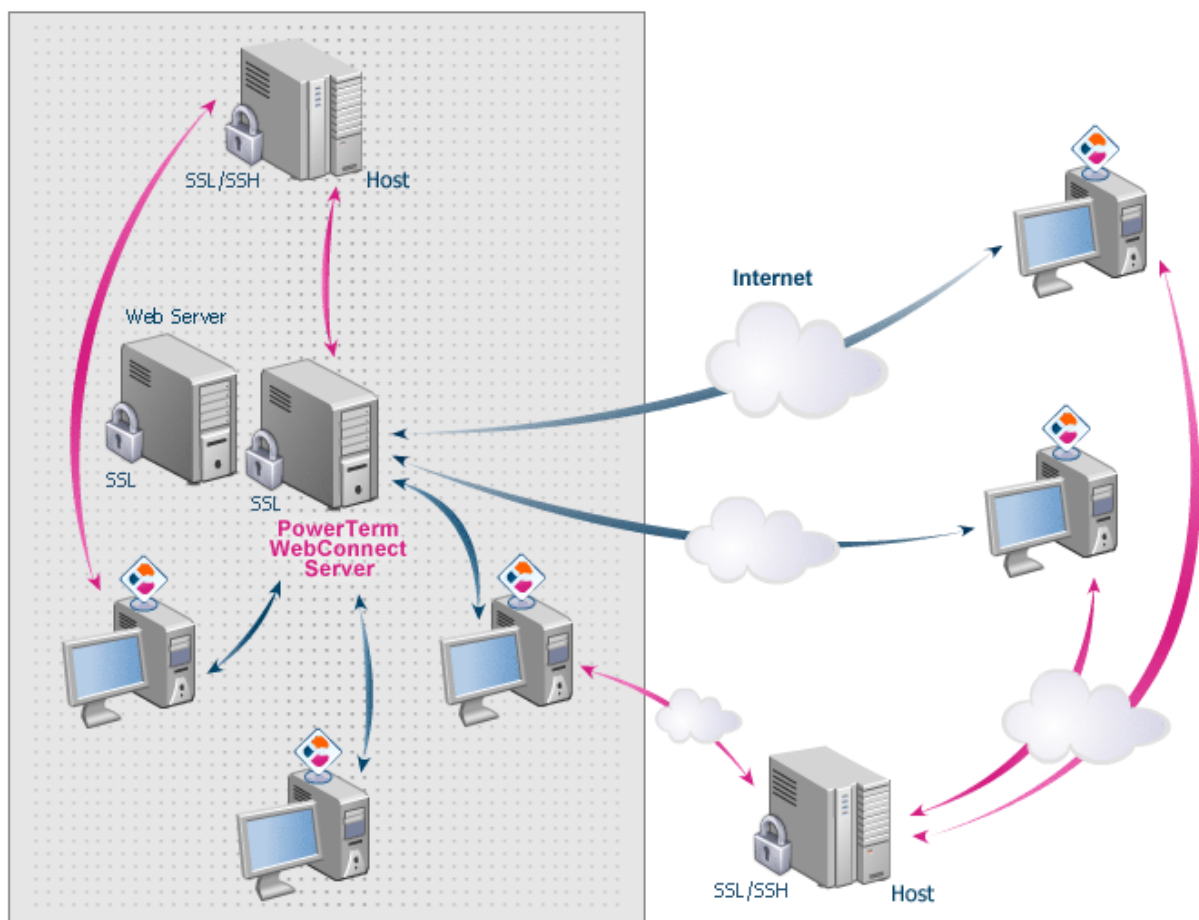
PowerTerm WebConnect Administration Tool is the management console that connects to PowerTerm WebConnect Server, allowing administrators to create and control users, define how users connect to the server, and monitor their online activity in real time.

The Administration Tool can also be used to configure the PowerTerm WebConnect Server and change settings in clients deployed throughout the organization.

PowerTerm WebConnect as Gateway

PowerTerm WebConnect Server is able to provide gateway service for its fat clients (HostView and WebView) while a socket-based (TELNET, RLOGIN, TN3270 or TN5250) predefined connection is used.

The fat client, in comparison to the Java client, is sometimes dependent on PowerTerm WebConnect Server in order to connect to a host. In such a case, when the fat client cannot "see" the host (since the client and the host are located on two distinctly separate networks) then PowerTerm WebConnect Server can act as a gateway. In order to acquire this capability you must specify the network name of the predefined connection's target (the IP address).

PowerTerm WebConnect Server can be accessed by a client from several different connection points, as specified in the server's INI file. Each connection point represents a logical or physical network, i.e. Intranet and Internet. The **NetworkName** attribute of each connection point specifies the name the system administrator assigns to the logical or physical network. The server keeps track about each client's accessed connection point. This information can be examined in the **Via** column of the **All Session's** list view.

The following table shows how PowerTerm WebConnect Server decides how the connection works:

Connection's Network Name	Comparision*	Visible	Decision How Connection Works	
			Telnet/Rlogin	Other
Public** or empty	N/A	Yes	Direct	Direct
Otherwise	Equal	Yes	Direct	Direct
	Not equal	No	Uses gateway	N/A***
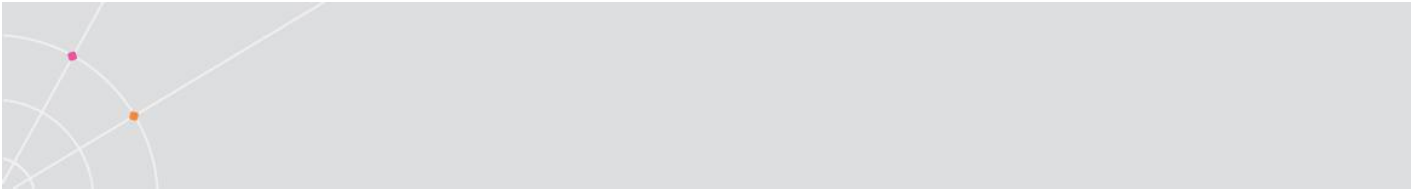
* Between the **Connection Network Name** and the **Session Network Name**.

** Non-case sensitive

*** The connection does not appear in the user's pre-defined connections list.

> NOTE   A "free connection" is never allowed to use the gateway for security reasons.

An asterisk (*) appears on the title bar of a PowerTerm WebConnect HostView client that uses Gateway, for example:

```
HostView Client*

EXE Client*
```

Monitoring User Activity and System Status

The Administration Tool provides numerous views that allow you to monitor server and client activity. The views show:

- Runtime information about computers, users, and groups: Time of first and last use, number of previous logins and sessions, IP address and traffic volume.

- Client session information: Session duration, client type, source IP address, user operating system, and traffic volume for the session. Session information can be viewed for all users, for a group, or for a single user.

- Monitoring PrintView (LPD) client print queues: View information about all the LPD print queues registered with the server.

- Security oversight: View detailed information about possible attempts at a security breach (for instance, when users enter an incorrect password or connect from a disallowed IP).

- Server statistics and logs (see chapter 7.7)

Configuring Client Behavior
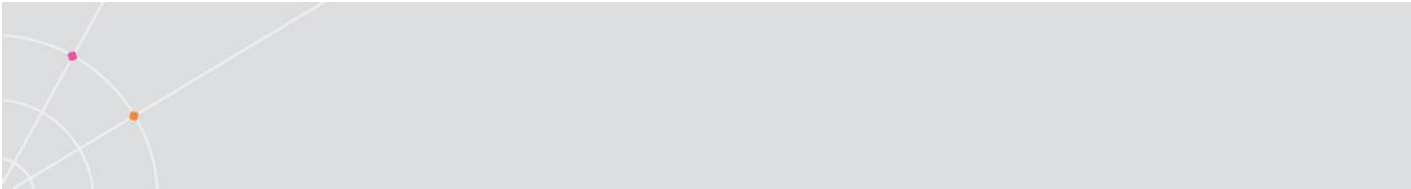
The Administration Tool's user and connection objects can be used to control the way PowerTerm WebConnect clients look and behave, allowing you to offer different levels of client functionality to different types of users. For example, in a library running an emulation of book-search terminals, readers can view a condensed (minimal option) client, while librarians receive more extensive options, and technicians are given full functionality.

It is important to understand that users do not need to download different client software to achieve different functionality. All users can download and use the same client, and the client software changes its functionality and appearance according to the instructions received from the server.

When a user connects, the server verifies whether any client-specific settings have been defined in the User's Default Group or in the Connection object. If so, the server transmits these specialized settings to the client.

PowerTerm WebConnect clients include:

- **RemoteView** for accessing Windows Terminal Server application from Windows and Linux desktops.

- **HostView** for accessing character-based applications running on legacy systems including IBM Mainframe, IBM AS/400, OpenVMS, Unix, Linux, Tandem from Windows and Linux desktops.

- **WebView** a programmable emulation client.

- **Java emulation client**

- **SupportView** for remote desktop support.

- **PrintView** for managing print queues.

- **QuickVNC** for remote desktop connectivity.

- **PowerTerm WebConnect for Thin Clients**

The Relationship between Clients and Connections

PowerTerm WebConnect provides a variety of clients to allow users to connect to various types of centralized computing resources. Different clients are designed to be used to connect to different types of resources. For example, PowerTerm WebConnect HostView is an emulation client, and is intended to connect to legacy hosts systems. PowerTerm WebConnect RemoteView supports the Remote Desktop Protocol, and is intended to be used as a client for Microsoft Terminal Servers.
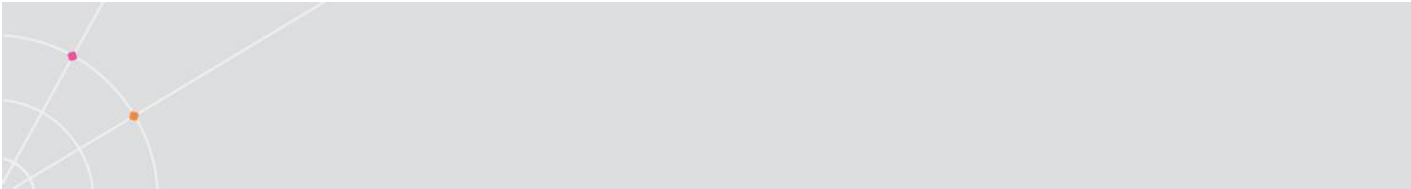
Some clients can be used to connect to the same server type. The difference between these clients can be the platform on which they run (for example HostView for Windows vs. HostView for Linux). Another difference is the user experience provided (for example HostView opens an independent emulation window while WebView embeds the emulation window in the browser).

Since the connection objects specify the protocol used to connect to the server, PowerTerm WebConnect clients can only use those connections that specify a protocol that the clients implement. For example, PowerTerm WebConnect RemoteView can only use a connection that has the RDP Type. It cannot use a connection that has the TELNET Type.

By default, when a client is launched, it lists only those connections that it can use. Alternatively, a client can be activated for a specific connection. In such a case, you must ensure that the connection is one supported by the client. You also need to make sure that the user is allowed to activate the clients that match the connections the user needs to use.

Emulation Clients

The PowerTerm WebConnect Emulation Clients, which include the HostView client (for Windows and Linux) and the Java client, allow users to perform operations on a host server. On the user's end, these clients display a representation of the host server's

terminal interface and, at the same time, translate the user's commands into the legacy protocol to be transmitted and processed by the host.

The following aspects of the emulation clients can be customized:

- Menus and menu options: Entire menus or specific menu commands can be made available for some users, but be removed for others (or the system default can be changed, using the server object). This is accomplished by using several pre-supplied environment variables, which are linked to functionality in the emulation clients. Environment Variables can be defined at the Server, Group, and User level.

- Emulation display and settings: Attributes such as display colors, number of rows and lines, cursor shape, and tab stops can be redefined for specific users, or for all users. This is done using the Settings dialog, identical to the settings dialog of the client software, which can be invoked from server, group, or user objects. Communication and printer settings can also be customized for some or all users, through the Settings dialog.

- Function buttons: Using the Connection object, you can define a customized Power Pad for any user using this connection. A Power Pad is a floating panel of function buttons, which the user launches by clicking on the desired button. The number of buttons (Rows and Columns), button labels, and the function that each button performs can all be customized. Functions Buttons (Soft Keys) that appear at the bottom of the emulation screen can also be defined in the same manner as the Power Pad.

- Keyboard mapping: There is often a need to map keys on the user's modern keyboard to reflect keys that appeared in the original terminal keyboard (e.g. F13). Keyboard Mapping can also be used to help automate functions. This mapping can be customized for anyone using a specific connection (i.e. using the connection object).

PrintView (LPD) Queues

The PrintView Client allows transparent printing (passes all characters, including escape sequences, that arrive at the port directly to the printer without translation) from the host server to a printer, which may be at a remote location from the host. The host (LPR) sends print jobs from specific queues to the PrintView Client (LPD), running on a PC that has access to a conveniently located printer. The PrintView Client, which may be in another network or even in another geographic location, prints the job on the local printer.

For this process to work, PrintView queues corresponding to the host's queues must be defined on the PrintView Client, and then registered with the server. This can also be done in reverse: the queues can be defined on the PowerTerm WebConnect Server and then reproduced to a PrintView Client. To learn how to do this, see chapter 8.4.
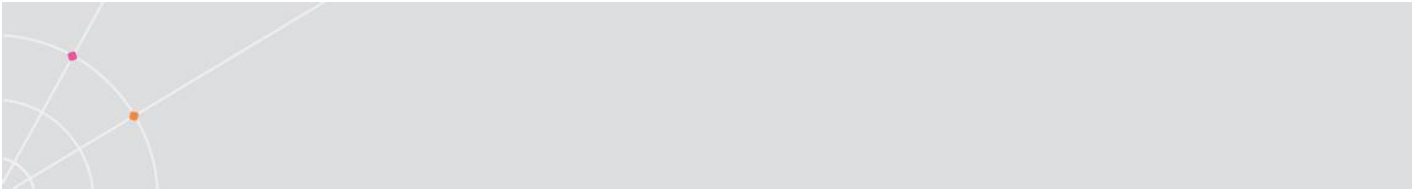
Testing

The Administration Tool's testing feature enables you to verify whether all the users and connections with their particular properties do indeed function according to design. Once you have defined different user, group, and connection objects, you can test them to confirm the behavior for which they were designed. For information on how to test a user, see chapter 5.3.7.

2. Installing, Starting, and Stopping PowerTerm WebConnect Server and Administration Tool

PowerTerm WebConnect Administration Tool and PowerTerm WebConnect Server can be installed on the same machine though it is not recommended. However, PowerTerm WebConnect Administration Tool and PowerTerm WebConnect Server must be located in the same network.

> CAUTION   Change of main hardware components in PowerTerm WebConnect Server will produce license errors. Please contact Ericom's Technical Support before proceeding.

MSI Installation

PowerTerm WebConnect provides Microsoft Windows Installer packages (MSI files) for all its clients. These packages are located on the PowerTerm WebConnect server in the **AddOns** folder. MSI is the preferred format for packaging software installations for Windows environments. MSI support is built into Windows Server 2003 family, Windows XP, Windows 2000, and Windows Me, and is also provided as a service pack to Windows NT 4.0 and Windows 98. In addition, MSI is supported by network configuration management services such as Microsoft Systems Management Server (SMS).

Each PowerTerm WebConnect client is packaged in a separate MSI for maximal flexibility, with minimal impacts on the system when the clients are provisioned to the users' workstations. In addition, the PowerTerm WebConnect MSIs support both manual and automated installation. Various installation configurations, such as the installation location, can be specified manually via the user interface, or using standard command-line parameters.

Installing PowerTerm WebConnect clients using MSI is most appropriate when:

- The organization uses a network configuration management service such as Microsoft SMS.

- Security settings prohibit web-based installation of client software.

- Bandwidth constraints or support requirements dictate a staggered distribution of the client software to the users' workstations.

> NOTE   PowerTerm WebConnect clients installed using MSI can only be upgraded using MSI. Such clients will not automatically update themselves from the web server of PowerTerm WebConnect server, even if a newer version of these clients is placed on those servers.

2.1. Installing PowerTerm WebConnect Server on Windows

PowerTerm WebConnect and its components are by default installed under `C:\Program Files\Ericom Software\WebConnect X.x` (where `X.x` is the version number). A number of sub folders are also created according to the PowerTerm WebConnect edition you have. Some of the folders are:

- **AddOns**, where the msi installations of different PowerTerm WebConnect clients and components can be found.

- **DataBase**, where your defined connections, groups, and other types of components are stored.

- **Help**, where you can find manuals and guides to the different PowerTerm WebConnect clients.

> NOTE PowerTerm WebConnect **Server** is by default installed under `C:\Program Files\Ericom Software\`**PowerTerm** `WebConnect X.x`.
> In this folder you will find server related executables and some dll files, e.g. the hlappi32.dll.

2.1.1. System Requirements

Please read the ReadMe.txt attached to the installation, or on the Ericom Website (www.ericom.com/systemreq.asp) for the most up-to-date requirements.

2.1.2. Installing the server (Windows)

Follow the Installation Wizard instructions.

PowerTerm WebConnect Application Portal

PowerTerm WebConnect provides a web interface for accessing published applications. This web interface, called the Application Portal, is implemented using ASP. As a result, for the Application Portal to work, ASP must be enabled on the web server on which it is installed.

> NOTE ASP processing is disabled by default on Microsoft IIS version 6, and may be manually disabled on previous versions of IIS. The PowerTerm WebConnect installation checks for ASP processing, and attempts to enable it if it is disabled. If the Application Portal does not work properly, please verify that ASP processing is indeed enabled.

2.2. Installing PowerTerm WebConnect Server on Linux

2.2.1. System Requirements

Please read the ReadMe.txt attached to the installation, or on the Ericom Website www.ericom.com/systemreq.asp, for the most updated requirements.

2.2.2. Installing the server (Linux)

> NOTE To use LDAP with PowerTerm WebConnect Server on Linux, the server machine must be configured for PING to hosts by NAME (not IP only).

For Intel processor:

1. Copy or FTP the installation file WebConnect-5.6-0.i586.rpm

2. From the command line, type: rpm -i WebConnect-5.6-0.i586.rpm

> NOTE On RedHat 7.2 (only) you need to install libgcc-3.0.4-1.i386.rpm before installing PowerTerm WebConnect Linux Server. You can find this rpm at ftp://rpmfind.net/linux/redhat/updates/7.2/en/os/i386/libgcc-3.0.4-1.i386.rpm
>
> NOTE On Slackware you might need to run the following from the command line:
>
> rpm2tgz WebConnect-5.6-0.i586.rpm
>
> installpkg WebConnect-5.6-0.i586.tgz

For PowerPC64 processor:

Use the installation file WebConnect-5.6-0.ppc64.rpm and continue as described above with the corresponding file name (i.e. *.ppc64.*).

> NOTE All PowerTerm WebConnect clients are published via the Web server. Therefore you need to manually configure the Web server to publish the path
> `/opt/WebConnect5.6/web`
> The name of the virtual directory must be WebConnect5.6. After configuring the virtual directory, you can substitute a valid IP address for <servername> and launch any client from
> http://<servername>/WebConnect5.6/ClientURLs.html

For Ubuntu

1. Copy or FTP the installation file webconnect_5.6-0_i386.deb

2. From the command line, type: dpkg -i webconnect_5.6-0_i386.deb

2.3. Starting and Stopping the PowerTerm WebConnect Windows Server

The PowerTerm WebConnect server must be running in order for clients to connect to it and in order to establish connections to the host systems. Typically, the administrator is responsible for this. Likewise the web server must be installed and running in order to download the client installation.

By default, the PowerTerm WebConnect Windows server is installed as an NT Service, with the Automatic startup type. This means that during system startup, the service control manager automatically starts PowerTerm WebConnect server.

The PowerTerm WebConnect server can also run as a user program. In order to accomplish this, you must pass the parameter /run to PtServer.exe.

Use the Administration Tool to launch the PowerTerm server whenever the PowerTerm WebConnect Server process is replaced by the PowerTerm WebConnect Server Starter (see Shutdown). This can also be done in remote mode.

NOTE   You should not start the server from the NT Services UI when the starter is running. In order to stop the starter running as an NT service, you can run the server with the command line parameter /kill.

To shut down the server from the Administration Tool:

Select Server | Shut Down. The PowerTerm WebConnect Server is installed as an NT service, but you can run it as a regular program.

To start the server as an NT service:

Run the 'PtServer.exe' with the /start command line parameter.

OR
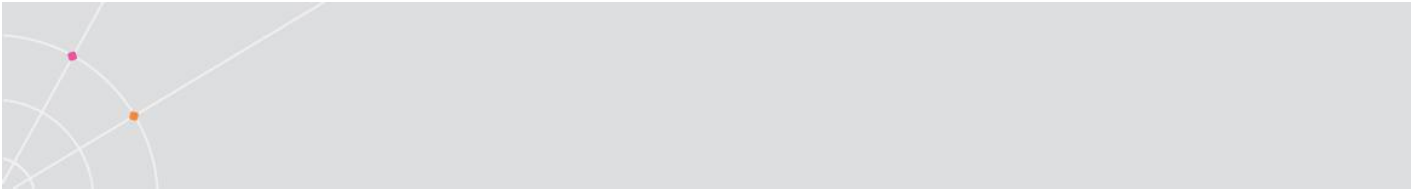
1. Open Start | Settings | Control Panel | Services.

2. Select the PowerTerm WebConnect Server [version number].

3. Click Start.

To start the server as a regular program:

Run PtServer.exe with the parameter /run.

2.4. Automatic Server Discovery

NOTE   Only for PowerTerm WebConnect Windows edition.

> This feature is by default not active and therefore has to be configured if you want to use it.

PowerTerm WebConnect allows for automatic server discovery if the PowerTerm WebConnect client (e.g. a thin client) does not know where the server is located. Both PowerTerm WebConnect Server and the client have to be on the local network. The server broadcasts a signal every X seconds via the UDP/IP protocol and thus the client can automaticly detect where the server is.

To configure the server side:

1. Open the **PtServer.ini** file. You can open the file through the PowerTerm WebConnect Administration Tool, **Files | Configuration | Main**.

2. Scroll down to **BroadcastConnectionPoint** and add your desired value:
    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

To configure the client side:

In the client's command line add

/broadcast – Listen to 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 you have to add **[=listen_port]** to **/broadcast** and **/broadcastlist** for the client.

2.5. Starting and Stopping the PowerTerm WebConnect Linux Server

The PowerTerm WebConnect Server is installed as a Linux service, but you can run it as a regular program.

> NOTE   You must be in the PowerTerm WebConnect directory to activate the command.
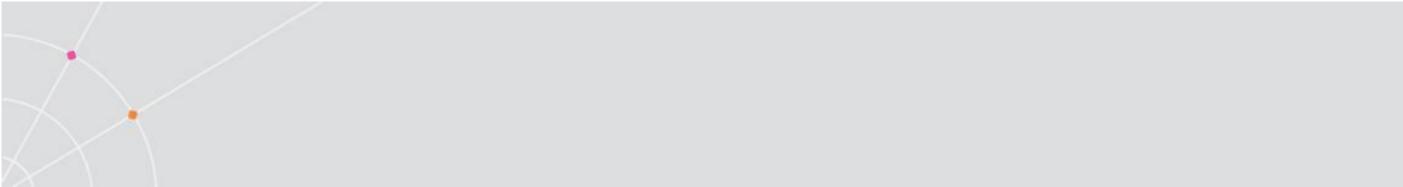
To start the server as a service:

Run ./wcctl -start

To start the server as a regular program:

Run ./wcctl –program

To stop the server:

Run ./wcctl -stop

2.6. Configuring PowerTerm WebConnect Server

2.6.1. Working with PtServer.ini

PowerTerm WebConnect is highly customizable, and designed to meet needs of any network, in order to make the most of both hardware and software. Most system managers will find that the configuration of the default installation makes the most of the resources available or strikes the best balance where different consideration conflict. However, some tweaking will always be necessary. This section explains the configuration of PowerTerm WebConnect through the **PtServer.ini** file.

NOTE   **PtServer.ini** is the only ini file that requires any editing. Editing any other configuration file will most likely crash the PowerTerm WebConnect server.

Parameters that control PowerTerm WebConnect Server are read from different sources as part of the server's startup routine, and are stored in memory. One of the sources is the PtServer.ini file, where parameters are stored as text. During startup, the server locates the file, parses the contents and obtains the different parameters and values.

Administrators can access some of the parameters stored in PtServer.ini through a GUI (graphical user interface). Other parameters can only be changed by editing the text in the PtServer.ini file, according to the guidelines described in this section. Some of the parameters accessed through the GUI can also be changed by editing the text in the PtServer.ini file but not all; for instance, several of the values that are GUI-controlled are encrypted and serialized and will not make any sense when viewed.

The recommended way to access PtServer.ini is through PowerTerm WebConnect Administration Tool:

1. Open the Administration Tool: Start | All Programs | Ericom Software | PowerTerm WebConnect (version number) | PowerTerm WebConnect Administration Tool.
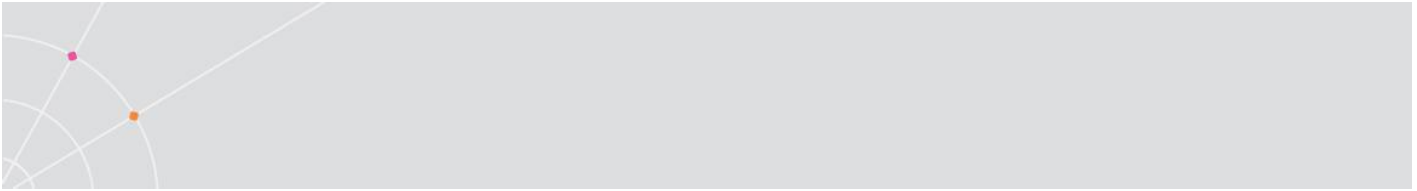
2. Select Files | Configuration | Main from the Menu bar. The PtServer.ini file will open in the default text editor, and the Administration Tool will become disabled until the editor is closed.

Another way to access PtServer.ini is to open a text editor and open the PtServer.ini directly. The default location of the file is:

Windows C:\Program Files\Ericom Software\WebConnect x.y\DataBase\PtServer.ini

Linux /opt/WebConnect x.y/DataBase/PtServer.ini
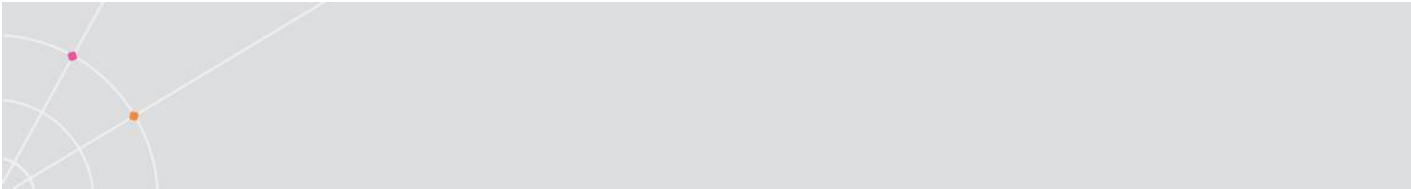
where 'x' and 'y' are the major and minor version numbers.

As mentioned, the recommended way to access the PtServer.ini file is through the Administration Tool. This approach has the following advantages:

- Changes are affective immediately
  When the Administration Tool opens the PtServer.ini file in the text editor, the Administration Tool becomes disabled. As soon as the editor is closed the Administration Tool becomes enabled again and PowerTerm WebConnect parses the PtServer.ini file. In this way, almost all changes to the PtServer.ini file become immediately affective. The few cases where the changes will not take affect until the PowerTerm WebConnect server is restarted are documented in the relevant sections of this manual.

- PtServer.ini file can be moved
  The PtServer.ini file can be placed in any location according to the system's needs and preferences. When accessed through the Administration Tool, the user does not need to know or find the correct location of the file.

- Automatic backups
  Whenever a change is made to PtServer.ini, the Administration Tool creates a back up file. This is important since a wrong value can cause PowerTerm WebConnect Server to malfunction. In extreme cases, using the wrong value could even stop the server entirely. If a recent change was unsuccessful, reverting back to the oldest working PtServer.ini from a backup becomes relatively easy. Backup files are located in the same directory as PtServer.ini and use the file naming format **PtServer.bck-nnn.ini**, nnn being numbers in the range 000 to 999.

The only time administrators should have to access PtServer.ini directly is when a previous change was not successful, causing the server to stop working. If this should happen, administrators will not be able to access the Administration Tool and will have to reset the changes by opening the PtServer.ini in a text editor, keeping the following points in mind:

- PowerTerm WebConnect Server should not be restarted until the file has been saved.

- The file must be saved to the file system for the changes to take affect. This requires the administrator making the changes to have read and write permissions to the file.

- Administrators must exercise caution when working with PtServer.ini; a wrong value can cause the PowerTerm WebConnect server to malfunction. In extreme cases, using the wrong value could even stop the server entirely. Before making any changes to the file, it is recommended to make a backup of a copy that is known to have worked.

- Administrators are warned to use plain text editors rather than word processors. In many cases the latter add formatting tags that do not appear in the visible document, but can still cause values to go unrecognized by the PowerTerm WebConnect parser. Examples of plain text editors include Notepad for Windows or VI for Linux.

Once the PtServer.ini file is open in the text editor the administrator can add, delete or change the file, as long as the syntax rules are strictly followed.

Syntax
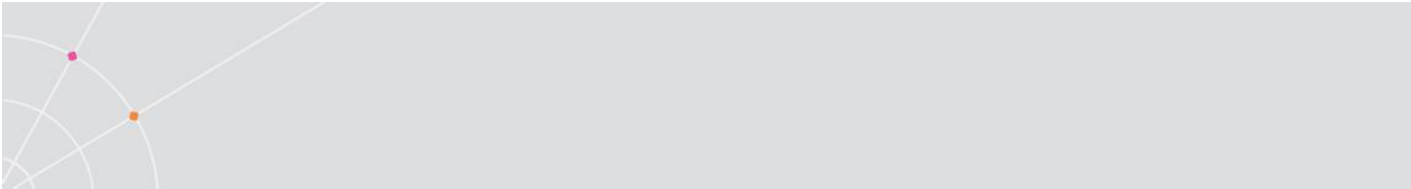
Entities in the PtServer.ini are defined by lines. Each line defines one and only one of the following entities:

- **Comments**
  Lines starting with a semi colon (;) are comments. Comments contain helpful information for administrators. Some of the information lists changes since earlier versions, and some of the information breaks the PtServer.ini to related groups, making it easier for administrators to find entries.

- **Section Headers**
  Lines starting with a square bracket opener and ending with the square bracket closer ('[' and ']' respectively) define a section header. Section headers define a section so that all entries between two headers (or from the last header until the end of the PtServer.ini) relate to the section named by the section header. Administrators must be careful when making changes to section headers; using wrong section headers might cause features to malfunction or could even crash the server.

  Section headers are not case sensitive.

  The particular order of the sections is not significant, but the last section will always override values of previous sections, if they share the same text in the header.

  PtServer.ini can store multiple sets of parameters, in a manner similar to the way database tables store multiple records. In relational database tables each record

holds the same set of columns as all the other records, but the values per column might differ. In this analogy, the PtServer.ini can have tables (=sets of sections) in which the columns (=parameters) can appear more than once, each time receiving a potentially different value.

Section Headers that contain an equal sign (=) define sections that are records of tables. The table's name will be on the left side of the first equal sign, and might appear several times in the PtServer.ini file. The record's name will be on the right of the first equal sign. An example of a table from the PtServer.ini created by the default installation would be the 'ConnectionPoint' table that contains the records 'Internet' and 'Internal Use'.

- **Entries**
  Lines that are neither comments nor section headers and contain an equal sign (=) are entries. Entries always contain one parameter and value pair separated by the equal sign (more precisely: the first equal sign from the left). Administrators must be careful when making changes to entries; using wrong parameter names or wrong values might cause features to malfunction or could even crash the server.

  Parameter names are not case sensitive. Values are usually case insensitive as well (the few exceptions where values are case sensitive have been documented in the relevant sections of this manual).

  The particular order of the entries within the section is not significant, but the last entry will always override previous entries, if they share the same parameter name. White spaces around values (right after the equal sign or right before the new line character) will be trimmed. White space within the value (between words inside the value) will not be trimmed. Do not add extra white space to the parameter name. Parameters that do not appear as an entry, or parameters whose value was left blank, will be assigned a default value. In most cases PowerTerm WebConnect will add an entry with the default value, if the entry was not found.
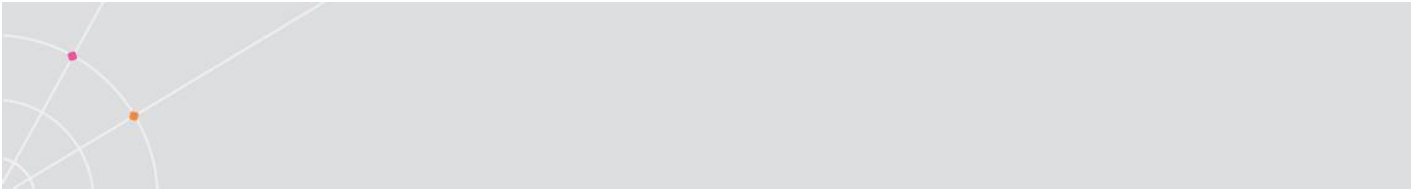
- **Junk**
  Lines that have not met any of the above criteria are considered junk and are ignored.

Example

The following is an extract from a PtServer.ini that was created during the default installation of PowerTerm WebConnect:

```
[Starter]

RestartbyAuthorized=AdminTool

AutoRestartTimeoutSeconds=10
```

```
[PoolUser=]

Count=0

LeadingCharacter=ZERO

CopyFrom=
```

The example shows two sections: 'Starter' and 'PoolUser='.

The 'Starter' section has two entries. The value for the 'RestartbyAuthorized' parameter has been set to 'AdminTool' and the value for the time to wait for the restart ('AutoRestartTimeoutSeconds') has been set to 10 seconds (for more details about the meaning of these parameters check the relevant part of this manual).

The 'PoolUser=' section defines a table 'PoolUser'. In this listing, table 'PoolUser' has only one, unnamed, record. Within the record, the 'CopyFrom' parameter has been assigned an empty value. Deleting this line would not have any affect, since the server will need to use a default value for this parameter either way.

2.6.2. Modifying the WebConnect Server's Configuration via the Interface

This capability is designed for controlling and tuning the server's activity. It is recommended to exercise caution when modifying the configuration's attributes because every change is immediately applied.

To modify the PowerTerm WebConnect Server's Configuration:

1. Select Server | Configuration. The Server Configuration dialog appears.
2. Modify the desired attributes.
3. Add or delete connections.
4. Create or modify Environment Variables (see section 8.2.2).
5. Click OK on completion of all modifications to the Server Configuration. The server's configuration has been modified according to the new attributes.

2.6.3. Modifying the Server's Address Manually

The default address used by the PowerTerm WebConnect components such as the Administration Tool, RemoteView and HostView client, is the first known address of the computer where the server runs. It can be either an explicit IP address or a host name that is convertible to a valid IP address (via DNS). This default can be modified, as explained below:

To modify the server's address:

1. Launch the Administration Tool.

2. Select Files | Configuration | Main. The PtServer.ini opens in Notepad.

3. Locate entry [ConnectionPoint=Internet].

4. Modify Address=... to the desired address.

5. Save and close the Notepad. The modifications will be automatically applied to the server.

6. Set the desired value of the address parameter in all of the relevant HTML files, using the following syntax:
   The PowerTerm WebConnect clients (except WebView) received the server's address via their command-line. When launched from an HTML page their command-line is specified using the Parameters property. So, if the server's address was changed this property must be updated accordingly. For clients launched from ClientURLs.html using the Windows Downloader, modify the following line in the _X.html files in the web/Windows subdirectory:
   Syntax
   ```
   <PARAM NAME="Parameters" VALUE="Server-Address /NOSELFUPDATE
   /RUN=Component">
   ```
   Example
   ```
   <PARAM NAME="Parameters" VALUE="www.ericom.com /NOSELFUPDATE
   /RUN=HostView">
   ```
   This will instruct the client to connect to a PowerTerm WebConnect server whose name is www.ericom.com.

For clients launched from ClientURLs.html using the Java Downloader

There are two ways to customize the specific Java Downloader parameter:

- All PowerTerm WebConnect clients will connect to the same PowerTerm WebConnect Server. You have to customize the **server** parameter in the **PtAgentSettings.js** file. It is located in:
  Windows: `<WebConnect Installation>/web/windows`
  Linux: `<WebConnect Installation>/web/linux/ix86`
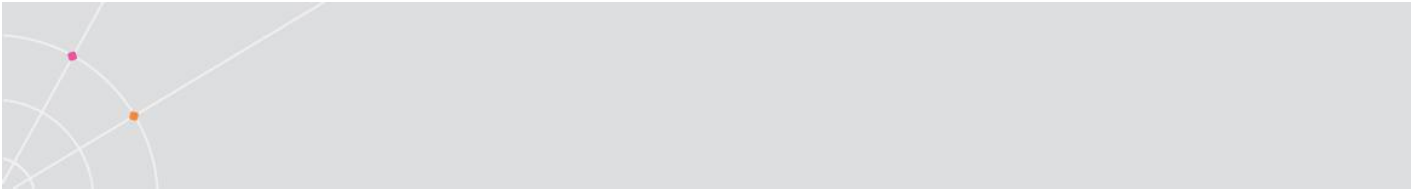
  Default:
  ```
  var server = location.hostname;
  ```

  Example:
  ```
  var server = "145.93.222.34";
  ```

- Different PowerTerm WebConnect clients will connect to different PowerTerm WebConnect Servers. You have to modify the **server** value in the corresponding

_J.html file. It is located in:
Windows: `web/windows`
where the file name is HostView_J.html, RemoteView_J.html, etc.
Linux `web/linux/ix86`
where the file name is Agent_J.html

Example: (Edit HostView_J.html)

```
//--------------------------------------------------
// Head Actions
//--------------------------------------------------
var component = "HostView";
server = "145.93.222.34"; // add here
// Identify browser
…
```

You can pass the server's address to the Administration Tool as a command line parameter, using the following syntax:

```
-host= Address
```

In this way, you can create a Desktop Shortcut for the Administration Tool, or modify an existing one, adding the specific address as a parameter in the Target field of the Shortcut property page.

Example:
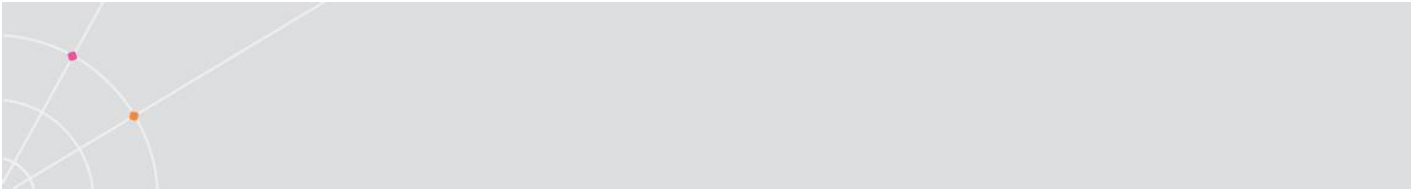
```
"C:\Program Files\Ericom Software\PowerTerm WebConnect\bin\PtAdmin.exe" –host=12.156.6.177
```

2.6.4. Modifying the Server's TCP/IP Port Manually

The default port used by the PowerTerm WebConnect components is port 4000. Unless a different port number is explicitly specified, this number will be used. Another port in use for the Starter and the Local system PowerTerm WebConnect Administration Tool is port 4001. These defaults can be modified. (For more default ports in use by PowerTerm WebConnect, please see

To modify the server's TCP/IP port:

1. Launch the Administration Tool.

2. Select Files | Configuration | Main. The PtServer.ini opens in Notepad.

3. Locate the entry [Server]PortNo=new-port-number and enter the server's TCP/IP port.

4. Save and close the Notepad. The modifications will be automatically applied to the server.

5. Set the desired value of the applet parameter port in all of the relevant HTML files, using the following syntax:
The PowerTerm WebConnect clients (except WebView) receive the server's port number via their command-line. When launched from an HTML page their command-line is specified using the Parameters property. So, if the server's port was changed this property must be updated accordingly. For clients launched from ClientURLs.html using the Windows Downloader modify the following line in the _X.html files in the web/Windows subdirectory:
Syntax

```
<PARAM NAME="Parameters" VALUE="Address:Port /NOSELFUPDATE
/RUN=Component">
```

Example

```
<PARAM NAME="Parameters" VALUE="www.ericom.com:5000 /NOSELFUPDATE
/RUN=HostView">
```

This will instruct the client to connect to a PowerTerm WebConnect server whose name is www.ericom.com using port 5000.

For clients launched from ClientURLs.html using the Java Downloader

There are two ways to customize the specific Java Downloader parameter:

- All PowerTerm WebConnect clients will connect to the same PowerTerm WebConnect Server. You have to customize the **server** parameter in the **PtAgentSettings.js** file. It is located in:
Windows: `<WebConnect Installation>/web/windows`
Linux: `<WebConnect Installation>/web/linux/ix86`

  Default:
`var server = location.hostname;`

  Example:
`var server = "145.93.222.34:5000";`

- Different PowerTerm WebConnect clients will connect to different PowerTerm WebConnect Servers. You have to modify the **server** value in the corresponding **_J.html** file. It is located in:
Windows: `web/windows`
where the file name is HostView_J.html, RemoteView_J.html, etc.
Linux `web/linux/ix86`
where the file name is Agent_J.html

Example: (Edit HostView_J.html)

```
//-----------------------------------------------
// Head Actions
//-----------------------------------------------
var component = "HostView";
server = "145.93.222.34:5000"; // add here
// Identify browser
…
```

You can pass the port number to the Administration Tool as a command line parameter, using the following syntax:

```
-port=port-number
```

This way you can create a Desktop Shortcut for the Administration Tool, or modify an existing one, adding your specific port number as a parameter in the Target field of the Shortcut property page.

Example:

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

2.6.5. Setting the WebConnect Server's Process Priority

A process' priority determines how much CPU resources the operating system allocates to the process, relative to other processes running on the computer. Processes with a higher priority are allocated more CPU time and therefore often execute more quickly than processes with a lower priority.

To set the WebConnect Server's process priority:

1. Launch the Administration Tool.

2. Select Files | Configuration | Main. The PtServer.ini opens in Notepad.

3. Set the entry ProcessPriority=<Default> located in the MISC section.

4. Save and close the Notepad. The modifications will be automatically applied to the server.

The supported values for ProcessPriority are: Normal, High, Realtime, and <Default>. The meaning of the values Normal, High, and Realtime are identical to those of Windows NT/2000/2003 process priorities. The meaning of <Default> is dependent on whether

the WebConnect server is running as an NT Service (in which case the process priority will be set to High) or as a regular program (in which case the process priority will remain Normal).

NOTE   Assigning a process Realtime priority can adversely affect the behavior of the entire system, and should be done with discretion.

2.7. Cluster Administration

Introduction

PowerTerm WebConnect can be configured to operate in a clustered environment, whereby a site is comprised of multiple PowerTerm WebConnect Servers, however, only a single live copy of the PowerTerm WebConnect database may exist. All servers access this central database that may be stored anywhere on the network.
The new functionality does not provide a mechanism for load balancing between the PowerTerm WebConnect Servers.
To maintain database integrity, only a single server may be responsible for updates at any one time.
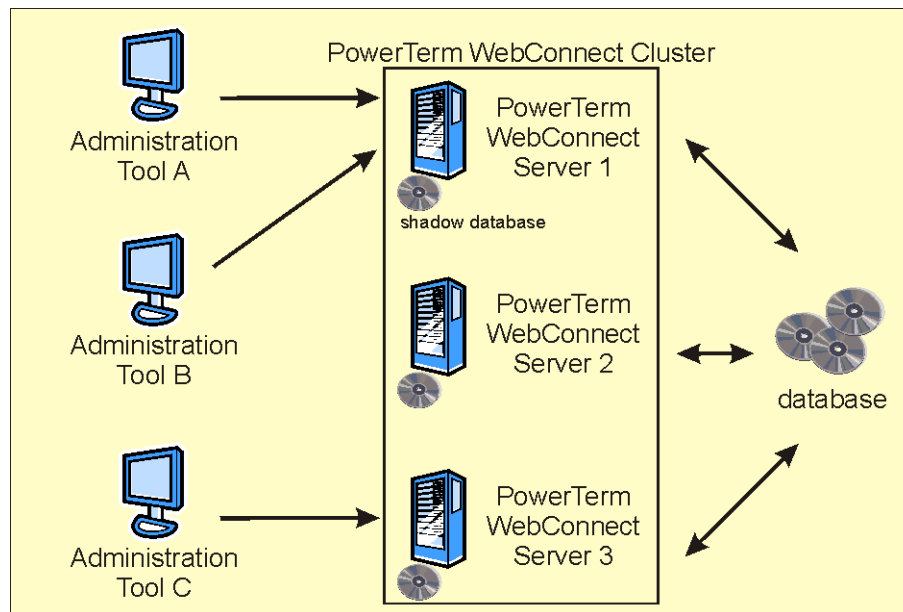
A PowerTerm WebConnect Cluster Administration

As can be seen in the above diagram, there are three PowerTerm WebConnect Servers in the cluster, Servers 1, 2, and 3. These servers all reference the single database. In this configuration, even though there are three Administrators trying to access the database,

only Server 1 will be able to update the database. Both Administrators A and B will have write permission.

In the above configuration, if an administrator is connected to Server 1 that is in update mode, Administrator C will receive an error message as shown below when he connects to Server 2 or Server 3.
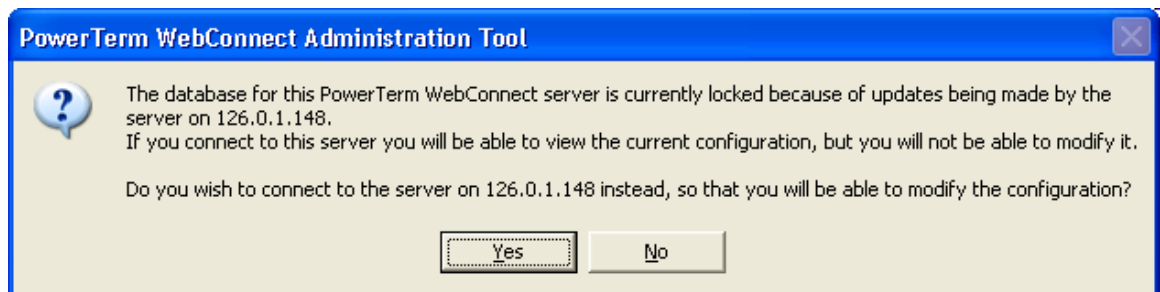
Message indicating that another Server is currently updating the Database

If the Administrator clicks on No, the Administration Tool will then connect to the database, but will only have read access. In this case, there will be two indications that this Administration Tool will not have write access:

- The title of the window will indicate that the Administration Tool is in Monitor Mode only.

- There will be a small, solid blue circle in the left hand corner of the toolbar at the bottom of the window.

Clicking on **Yes** will redirect the Administrator to the server that is currently in update mode.

In the event that the main database is not available for whatever reason (network failure, lack of permissions, etc.), the Administration Tool that currently does have write access will automatically be switched to Monitor Mode. Although switching to monitor mode is automatic, it will not be done immediately. The switch will occur the next time the server tries to access the database, such as, when the administrator tries to update an entity, or when the update/synchronize process (described below) is attempted.

NOTE   Switching to Monitor Mode does not mean that the server starts working with the Shadow Database (described below).

Switching to Monitor Mode of course means that no update is possible during this time. The indicators as described above as well as the message shown below will be displayed.
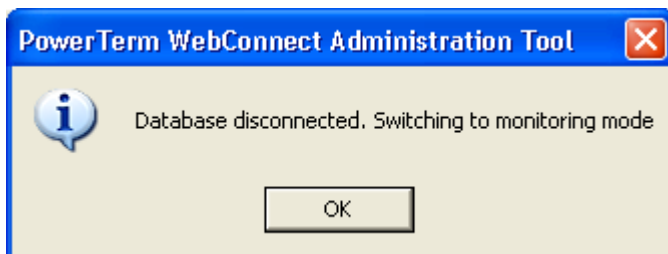
Message notifying the administrator that the Main Database is offline

When trying to run the update process, the server will discover that the database is again available (see below). When the server discovers that the database is once again available, it will immediately update its data against the database, even if prior to the database failure it was in Update Mode.

A shadow copy of the main database is copied to each PowerTerm WebConnect Server and is synchronized as detailed below. In addition, a copy of the database is stored in memory on each PowerTerm WebConnect Server and is updated according to the parameters detailed below. This copy is volatile and is lost if the server is shut down for any reason.

The Shadow Database is used when the server starts and cannot find the real database. This is in order to allow servers to start and work with a slightly old database rather than not being able to start at all. Since the server tries to update against the real database, when the database again becomes available, the data on the server will be brought up to date.

NOTE   Synchronization refers to the shadow database, while updating refers to the volatile copy of the database stored in memory.

In single PowerTerm WebConnect Server configurations, the database may be stored in either binary or ASCII format. In a clustered PowerTerm WebConnect Server environment, the database can only be stored in binary format.

In a PowerTerm WebConnect clustered-server environment, any Users that are auto-created are volatile and therefore cease to exist once the User is logged off.

2.7.1. Enabling Cluster Mode

Running in Cluster Mode is akin to running multiple servers with the same database. This means that each server needs to be activated separately and each server needs to have its own pool of licenses. To enable the Cluster mode, you have to configure both PowerTerm WebConnect Server and PowerTerm Load Balancer.

Configuring PowerTerm WebConnect Server

In a default installation, the database is stored in a directory called \Database within the same parent directory as the \Bin directory. For example, c:\program files\Ericom\Database and c:\program files\Ericom\bin. For multiple PowerTerm WebConnect Servers to be able to operate in cluster mode, the Administrator must:

1. Create a folder that can be accessed with as network path. (On Windows systems it means that the folder should be shared.)

2. Copy the database folder from the installation folder to the shared folder. The database's version must be appropriate for the version of PowerTerm WebConnect Server that will use it. (Though it does not have to be the same.)

3. Copy the Downloads folder to the shared folder.

4. Set-up full permissions to access the new folders to all the servers that will need to use the shared database.

5. Create a file called PtServer.ptr on the bin directory of each Server. This file must contain the full network (UNC) path to the central database.

Switching the database to another location while the servers are running is not possible.

To move the database to another location:

1. All the servers using the old location must be shut down.

2. The database must be copied to the new location.

3. All PtServer.ptr files must be updated with the new location.

Cluster mode can only be enabled if the full network path is defined in the PtServer.ptr file, **and** license file exists in the local \bin folder. If the full network path is defined in the PtServer.ptr file and the license file exists in this network path, then the PowerTerm WebConnect Server will operate in Failover mode.

Configuring PowerTerm Load Balancer

PowerTerm Load Balancer is configured through its Administration Tool:

For more information about PowerTerm Load Balancer, please see "PowerTerm Load Balancer, Administrator's Manual", included in PowerTerm Load Balancer installation.
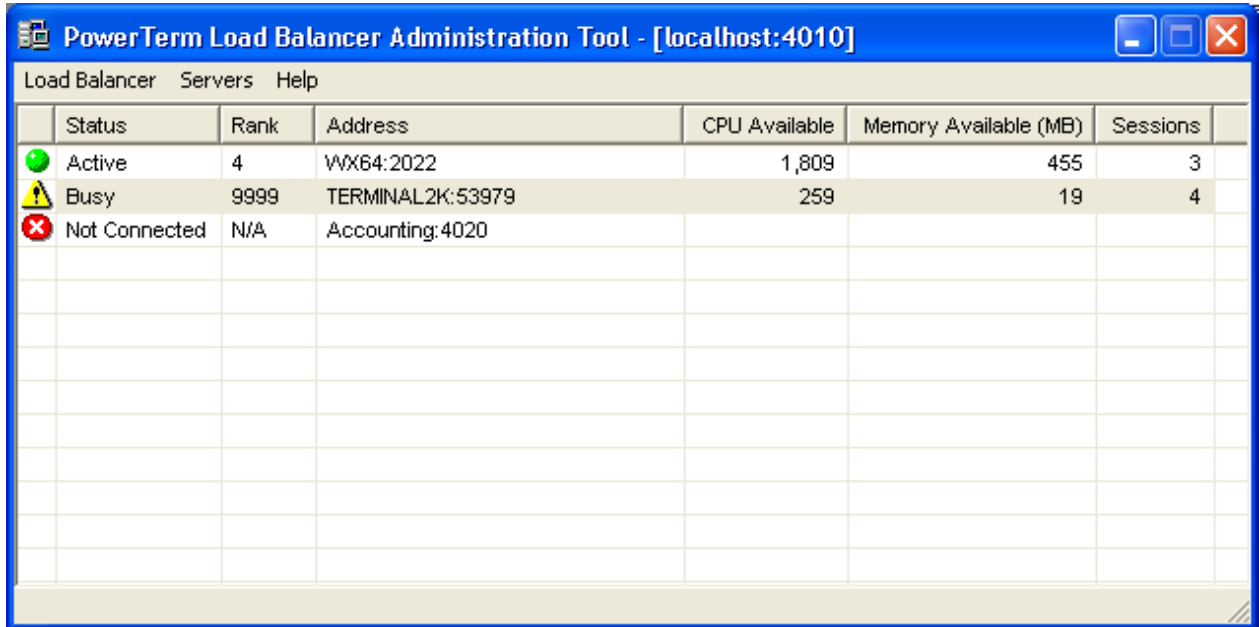
In PowerTerm Load Balancer, the Configuration file is by default specified at 'Default Location', which is the PowerTerm Load Balancer installation folder. To work in Cluster mode you need to specify the path, on a local or remote machine, for the Configuration file to be shared.

NOTE   All the servers that will use the shared database need full permissions to access the Configuration file path.

To specify the Configuration file location:

1. Open PowerTerm Load Balancer Administration Tool.

2. Select Load Balancer | Options. The Options dialog appears:
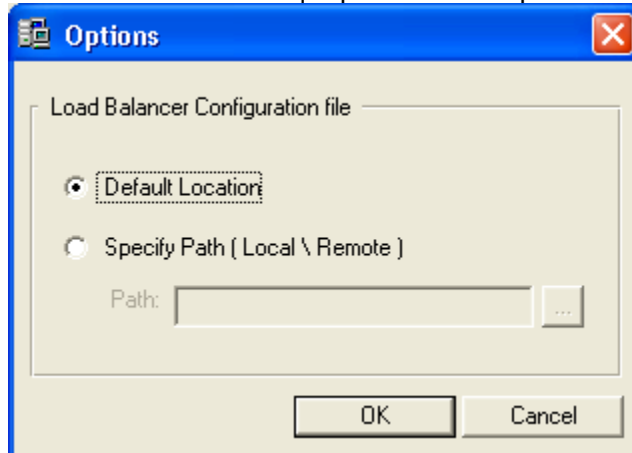
3. Select the desired location for the Configuration file and click OK. A notification message appears.

4. Click OK and re-run Load Balancer Administration Tool.
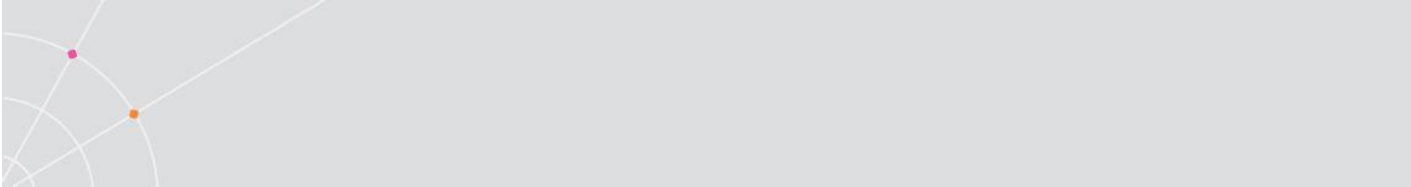
2.7.2. PtServer.ini parameters
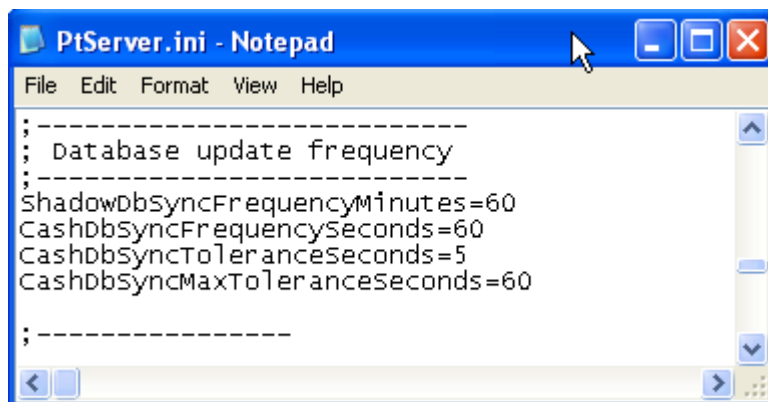
Database Update Parameters in a Clustered Environment

The following parameter contained in the PtServer.ini file is used to control the synchronization of the shadow database:

- ShadowDbSyncFrequencyMinutes—synchronize interval in minutes for copying to the shadow database.
  Default—60

The following parameters contained in the PtServer.ini file are used to control the updating of the database copy in memory:

- CashDbSyncFrequencySeconds—update interval in seconds for copying the database to memory.
  Default—60

- CashDbSyncToleranceSeconds—update 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

2.7.3. The PtServer.ptr File

The PtServer.ptr file must contain an entry with the following format:

\\ERICOM_main\WebConnect\DataBase\PtServer.ini

2.7.4. Limitations

Only sessions connected to a particular PowerTerm WebConnect Server will be visible, not sessions connected to any other servers.
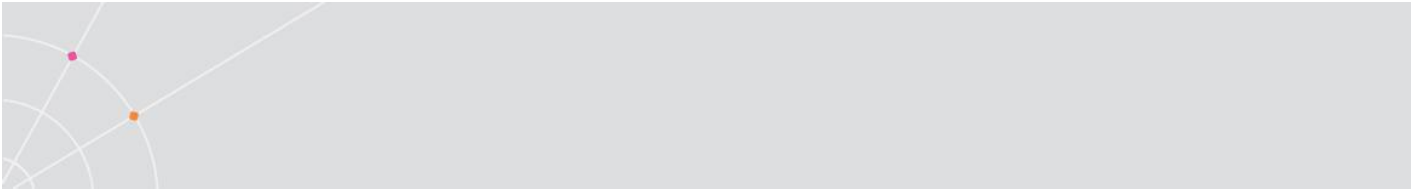
Help or assistance will not be available from an administrator or the helpdesk if they are connected to a different server in the cluster.

2.8. Launching and Closing the Administration Tool

There are several ways to launch the Administration Tool. Select the one most convenient for you:

- From Windows **Start** menu select **Programs | Ericom Software | PowerTerm WebConnect 5.x | PowerTerm WebConnect Administration Tool**. (If you changed the Program Folder during installation, the Start menu path may vary accordingly.)

- Double-click **PtAdmin.exe**, located in the bin directory of the PowerTerm WebConnect installation folder.

- Rather than installing, you can choose to download the Administration Tool to any Windows computer. Please refer to the "PowerTerm WebConnect Sample URLs" page:
  http://<web_server>/WebConnect5.x/ClientURLs.html

A few things to remember:

- When you launch the Administration Tool for the first time, the **Connection** dialog is displayed with the user "Administrator". No password is required, just click **Connect**. (For security reasons, we advise to fill in your password at your earliest convenience.)

- In the **Connection** dialog, displayed when launching the Administration Tool, the **Host Name** is "localhost" by default. This is correct only if the Administration Tool runs on the same machine as the server. If the Administration Tool runs on a different machine, you need to enter the IP address/Host name of the PowerTerm WebConnect server.

- (PowerTerm WebConnect Windows edition only) The Administration Tool will, by default, deny any connection attempts from any computer other than the local machine.

To close the Administration Tool:

1. Select **Action | Exit**. A confirmation dialog appears.

2. Click **Yes**. The Administration Tool closes.

NOTE   Closing the Administration Tool does not stop the PowerTerm WebConnect server to which it is connected.

3. The Administration Tool: General Reference

The administrator manages published applications, user sessions, and server configuration through PowerTerm WebConnect Administration Tool. Also performing operations such as multiple application publishing, sending messages to logged-on users, shutting down sessions and monitor user activity is done in the Administration Tool.

There are multiple ways to launch the Administration Tool (see 2.8).

NOTE   Launching the Administration Tool from the system tray (not available in Windows Vista) or using the Administration Tool launched directly after completed installation will not allow you to activate certain features.

After you launched the Administration Tool and connected the server, you will receive the **Quick Access** dialog where you can select desired activity:
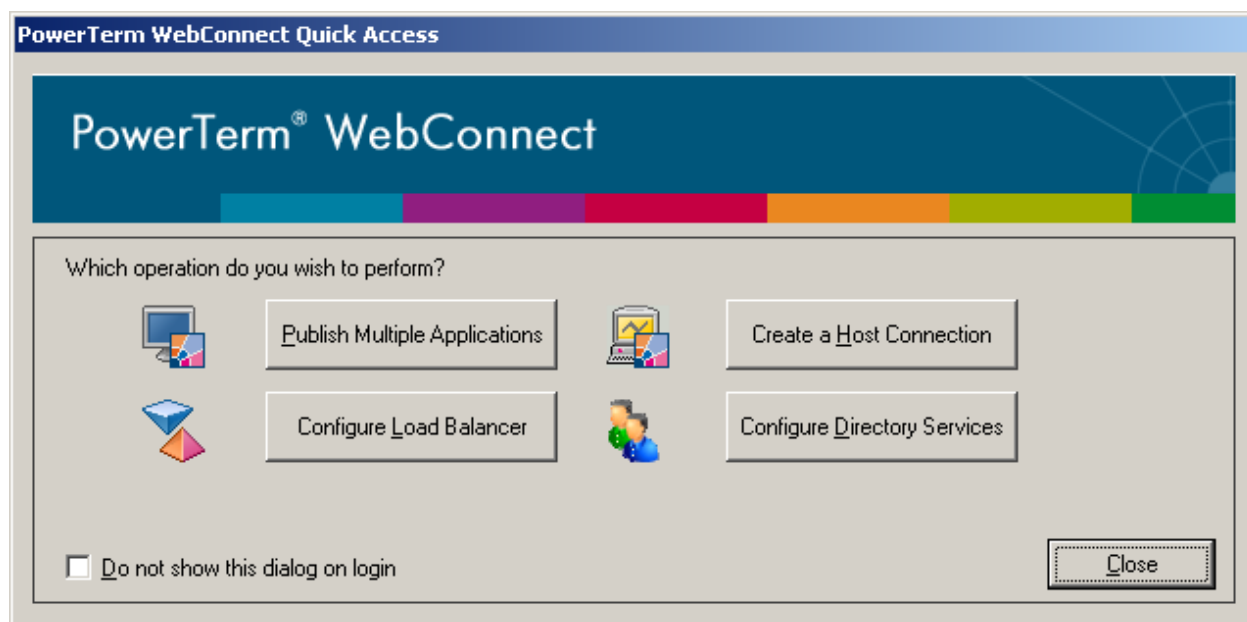
- **Publish Multiple Applications**, opens the **Publish Multiple Applications wizard**.

- **Configure Load Balancer**, opens **PowerTerm Load Balancer Administration Tool**.

- **Create a Host Connection**, opens the **Add Connection dialog**.

- **Configure Directory Services**, opens the **Directory Services dialog**.

Close the Quick Access dialog to enter the Administration Tool main screen:

By default the Connection pane is displayed when you first open Administration Tool, with three predefined example-connections:

- Example_As400

- Example_VT

- localhost

The interface consists of:

- **Menus** and a **toolbar**, to customize and refresh the information tables; launch wizards to publish applications, create new groups, users and connections; run other PowerTerm WebConnect clients.

- **Information panes**, to show properties and real-time information for all users, groups, connections, as well as sessions and intruders.

- **Wizards** and **Properties dialogs**, to create new or modify existing published applications, users, groups, connections as well as to define system defaults using the "master group" – the server object.

3.1. Menus and Toolbar

The following sections detail the commands of all the Administration Tool's menus, with their corresponding buttons where applicable.

3.1.1. Action Menu

Command/Submenu	Toolbar Button	Description
New		Opens the **Publish Application** and the **Remote Desktop** wizards, as well as the **Add User/Group/Host Connection** 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.

3.1.2. Server Menu

Command/Submenu	Toolbar Button	Description
Connect/Disconnect	-	Connects/Disconnects the Administration Tool 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 Tool (recommended method).

3.1.3. 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.
PrintView Queues	-	Displays real-time information for current PrintView queues.
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.

3.1.4. Files Menu

Command/Submenu	Toolbar Button	Description
Configuration	-	Five configuration files (PtServer*.ini) that are located in the \DataBase directory: **Main**, contains the definitions of all the entities used by PowerTerm

		WebConnect Server, except for the host connecter that are contained in the PtServer_Connections.ini file.
		Users, contains the definitions of all the user entities used by PowerTerm WebConnect Server.
		Groups, contains the definitions of all the group entities used by PowerTerm WebConnect Server.
		User/Group links, contains the definitions of all the user-to-group links used by PowerTerm WebConnect Server.
		Connections, contains the definitions of all the connection entities used by PowerTerm WebConnect Server.
Defaults	-	**PtDef.pts**, contains the default setup attributes used by PowerTerm WebConnect clients.
		ByPass.pts, contains the setup attributes that will overwrite any other setup settings. (The default file supplied with the PowerTerm WebConnect installation is empty.)
		CommDef.ini, contains the default communication attributes used by PowerTerm WebConnect clients.
		PtLpd.ini, is used by PtServer.exe as the default PowerTerm WebConnect PrintView client configuration template.
		LoginToWebConnect.psl, is the script that runs every time a client has successfully logged in to PowerTerm WebConnect Server.
LOG files	-	The log files are circular text files. Each execution of the server or
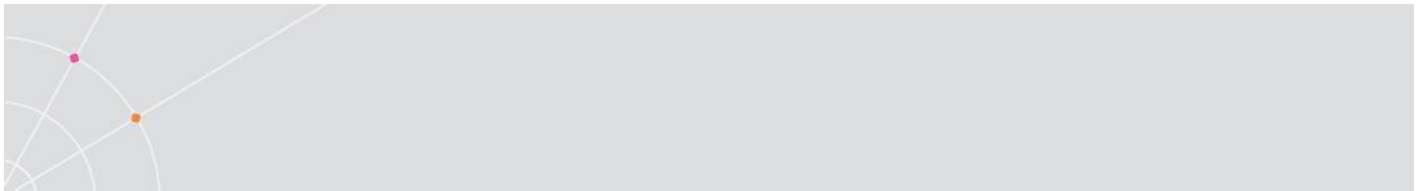
Command/Submenu	Toolbar Button	Description
		starter opens a new log file. PowerTerm WebConnect maintains backup versions of these log files: **Server** **Starter** **FAILOVER History.LOG** **Audit Trail**
Put Background Bitmap	-	Takes the specified file and creates a special file that can be associated 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.

3.1.5. Tools Menu
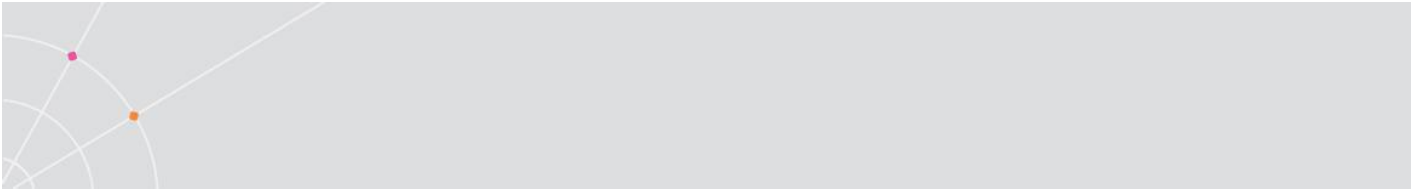
Command/Submenu	Toolbar Button	Description
Run Event Viewer	-	This Microsoft utility will display the pertinent log information for the server's machine to which you are logged on.
Run FTP Client	-	Launches the FTP client, which provides a convenient way to transfer files.
Run HostView	-	Allows you to emulate the user's session and connection and thereby conduct a test on it.
Run PrintView	-	Launches the PrintView Queues window that shows definition and runtime information on all the print queues registered with the server.
Run RemoteView	-	Runs the selected RDP connection and allows you to test it.
Run QuickVNC	-	Runs the selected VNC connection
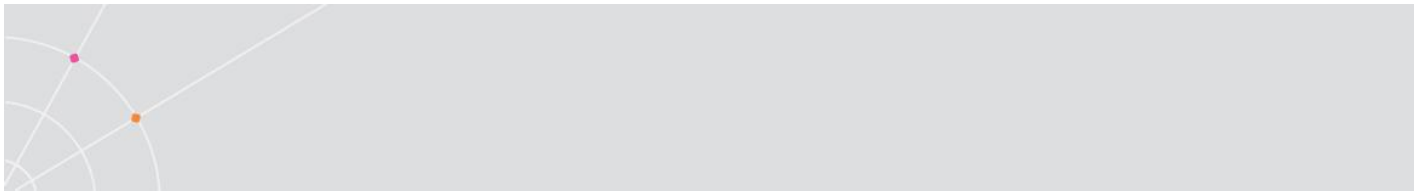
Command/Submenu	Toolbar Button	Description
		and allows you to test it.
Open Application Zone		Runs the Application Zone.
Run Load Balancer Administration Tool		Launches PowerTerm Load Balancer Administration Tool.
Open File	-	Enables you to open files.

3.1.6. Options Menu

Command/Submenu	Toolbar Button	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 Tool main screen in which status messages and prompts can be shown.
Use Tooltips on List Header	-	Enables tool tips on list header when the text is truncated.
Use Tooltips on List Rows	-	Enables too 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 Tool 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	-	Delays the updating of the display

Updates While Editing Properties		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.

3.1.7. Help Menu

Command/Submenu	Toolbar Button	Description
Help Topics	-	Launches the Administration Tool online help.
Release Notes	-	Displays PowerTerm WebConnect's new features and modifications for the current version, in addition to the last few versions.
Charts	-	Displays the HostView and Java client topographies and the PrintView client and VNC data flow.
Send Mail to Support	-	Opens an email form addressed to Ericom support so you can ask any questions to the Support team.
About the Administration Tool	-	Displays the current version of Administration Tool and Ericom contact information.

3.2. 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.
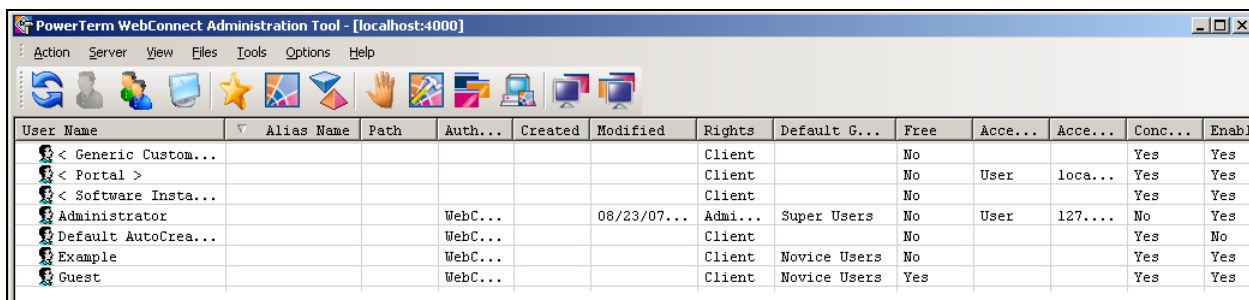
3.2.1. Connections Pane

Field	Description
Connection Name	The connection's unique name.
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:
	Hidden, can only be activated from a login script.
	Child, owned by another connection and triggered by it.
	Regular, a regular connection.
	Owner, 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.

3.2.2. Users Pane

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
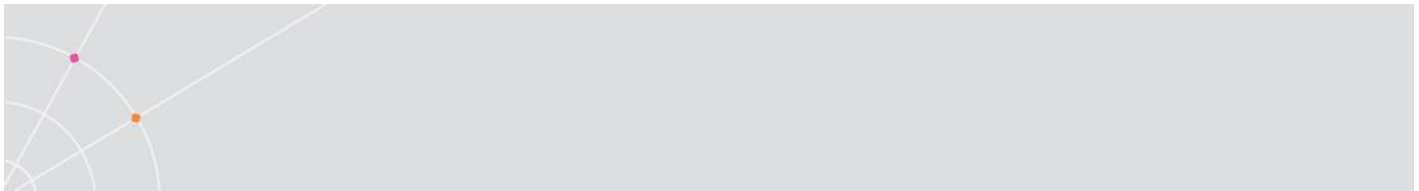
	accessibility.
Access Limit Mode	Specifies the access level.
Access From	Specifies the machines or IP addresses from which the user is allowed to access PowerTerm WebConnect.
Concurrent Machines	Specifies that the user is allowed to log on simultaneously from multiple computers.
Enabled	Specifies if the user is active.
Max. Concurrent Sessions	The maximum number of concurrent sessions that the user may have.
Max. PrintView Queues	The maximum number of PrintView queues that the user is allowed to have at any given time.
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 the clients used by this user since the server
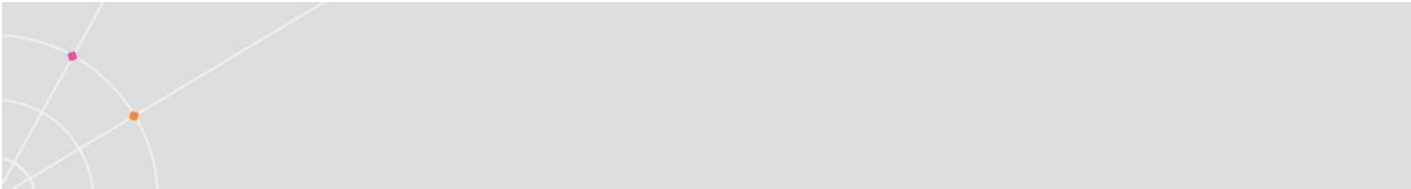
	was activated.

3.2.3. Groups Pane
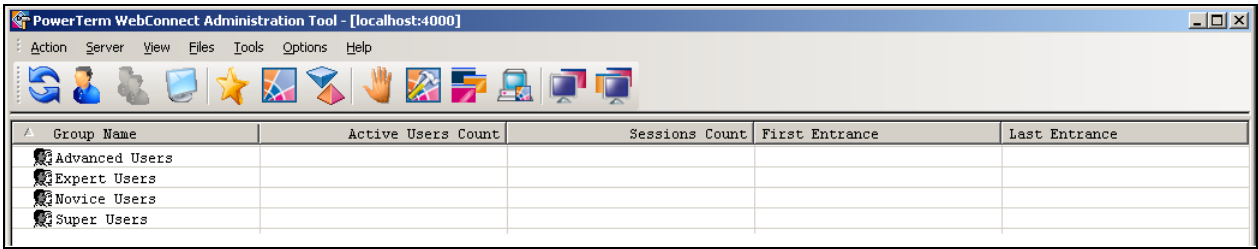
Field	Description
Group Name	The group's unique name.
Created	Date and time the group was created.
Modified	Date and time the group was last modified.
Enabled	Specifies if the group is activated.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions that the members of the group may have.
Max. PrintView Queues	Specifies the maximum number or PrintView queues that the members of the group may have at any particular time.
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.
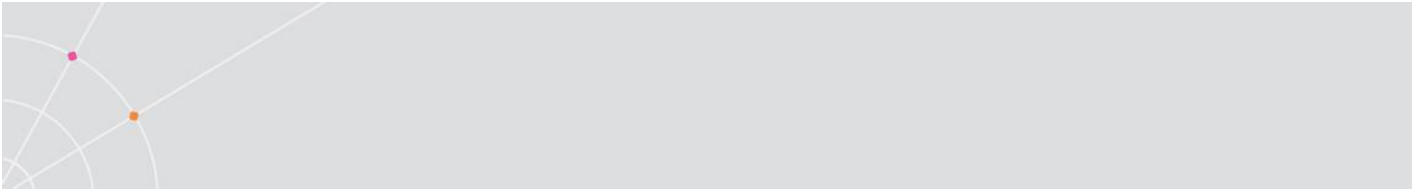
Last Entrance	The date and time of the last login of any group member, since the server was activated.

3.2.4. Client Sessions Window

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. NOTE: The Java client does not supply this information.
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	Specifies if the client is a HostView or a Java client.
	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.	The maximum packet size that has passed through the gateway.
Bufferized I/O Count	The number of bottlenecks that resulted from sending data to the session.

3.2.5. Administrative Sessions Window

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. NOTE: The Java client does not supply this information.
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
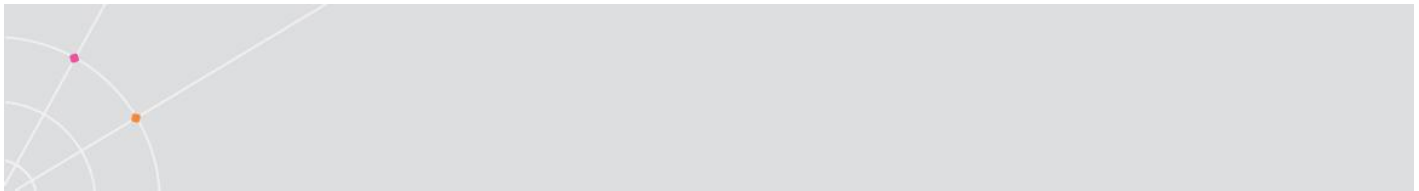
	which the client is connected.
Started at	The date and time of client's login to the server.
Reconnect Mode	The user's reconnect level.
Last Output	Date and time of last transmission output.
Last Input	Date and time of last transmission input.
Output Bytes	The total bytes of application traffic that 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. 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.
Bufferized 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.

3.2.6. Terminal Server Sessions

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.

3.2.7. PrintView Queues Window

Field	Description
Queue Name	The name of the PrintView queue.
User Name	The name of the user.
User's Alias Name	An alternative name or id for the user that is not necessarily unique.
PrintView Client ID	Specifies the client's ID.
Enabled	Indicates if the queue is activated.
Routed Commands	The number of jobs that the queue received.
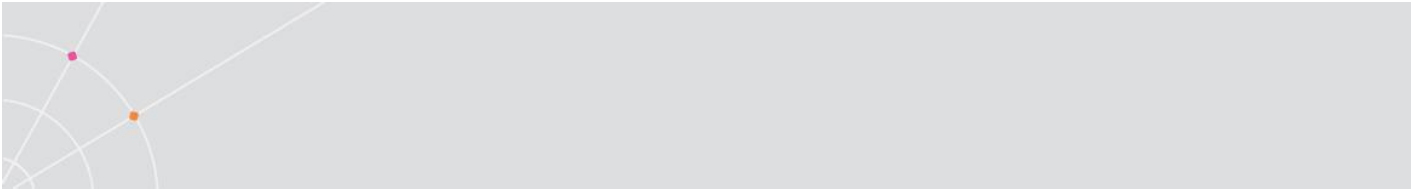
Routed Bytes	The number of bytes routed through the server.
First Command	The time of the first command that was received from PowerTerm WebConnect Server for this queue.
Last Command	The time of the last command that was received from PowerTerm WebConnect Server for this queue.

3.2.8. Machines Window

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.

3.2.9. Intruders Window
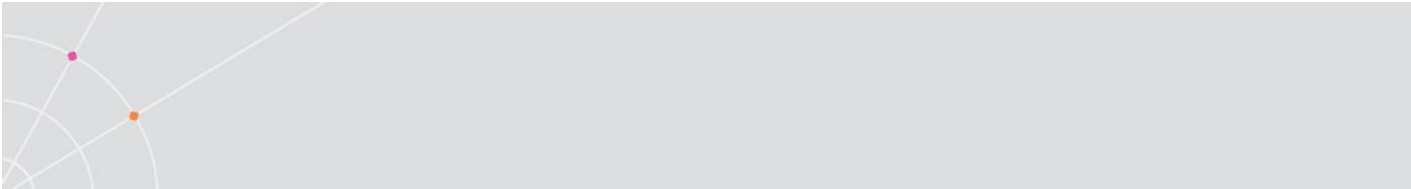
Field	Description
User Name	The intruder's user name.
Machine	The intruder's machine name.
Reason	The reason the intruder was detected.
Attempts Count	The number of times an intruder attempted to login to PowerTerm WebConnect Server.
Intrusions Count	The number of times the intruder was punished for 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.

3.3. Properties Dialogs

The following sections detail the fields of the various Properties dialogs.

3.3.1. User Properties Dialog

For a more detailed description of the features, see chapter 5.3.

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.
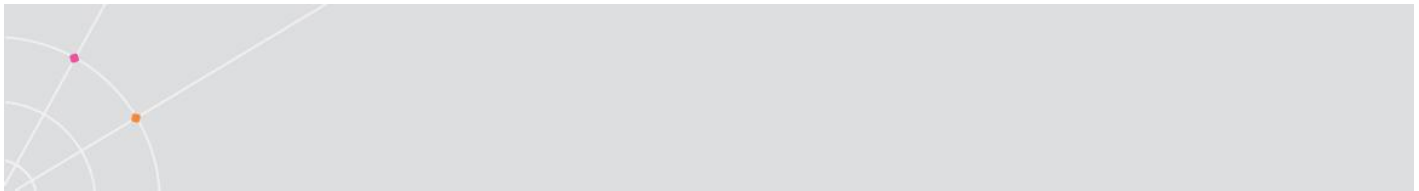
Available Groups/Unlinked Connections	Lists all the groups and free connections that the user can be a member of.
User's Groups/User's Connections	Lists all the groups and connections affiliated with the user.
Enabled	Activates the user. (Only active users can connect to the server.)
Free User	Allows 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.
Max. PrintView Queues	Specifies the maximum number or PrintView queues the user may have at any particular time.
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 customize 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 Tool online help.

3.3.2. Group Properties Dialog

For a more detailed description of the features, see chapter 5.4.

Field	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.
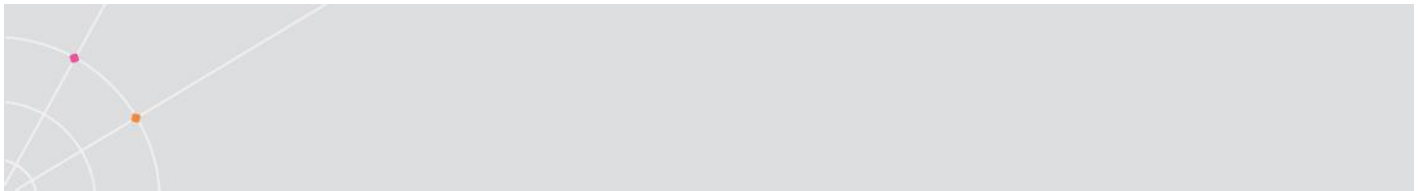
Group's Users/Group's Connections	Lists all the users and connections affiliated with the group.
Enabled	Activates the group.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions the members of the group may have.
Max. PrintView Queues	Specifies the maximum number or PrintView queues that the members of the group may have at any particular time.
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 customize 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 Tool online help.

3.3.3. Connection Properties Dialog

For a more detailed description of the features, see chapter 6.1.

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:

	Hidden, can only be activated from a login script.
	Child, owned by another connection and triggered by it.
	Regular, a regular connection.
	Owner, 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 SBC resource using RDP or VNC protocols.
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:
	Gateway, connections accesses the host via Gateway mode.
	No Gateway, connections accesses the host via Direct mode.
	Public, connections accesses the host via Gateway mode if **Reconnect** is used. Otherwise connections will access the host via Direct mode.
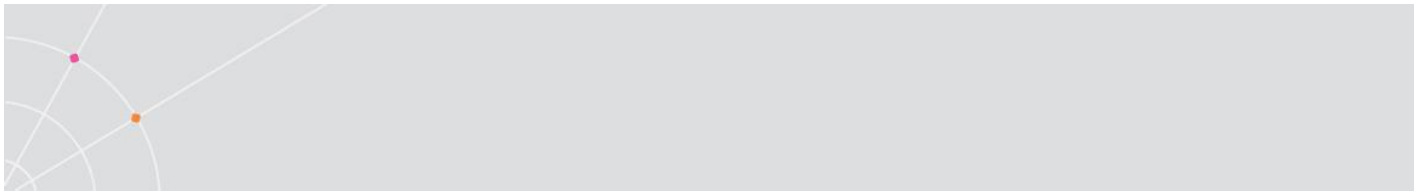
Environmental Variables	Specifies variable names and associated values for the connection.
Settings	Opens the Terminal Setup dialog to customize client settings for the connection.
Key Mapping	Opens the Keyboard Mapping dialog to enable mapping keys with desired character or script.
Power Pad	Opens the Power Pad & Function Buttons dialog to define Power Pad and Function buttons.
Login Script	Opens the **Login Script.psl** 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 Tool online help.

3.3.4. Server Configuration Dialog

Field	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
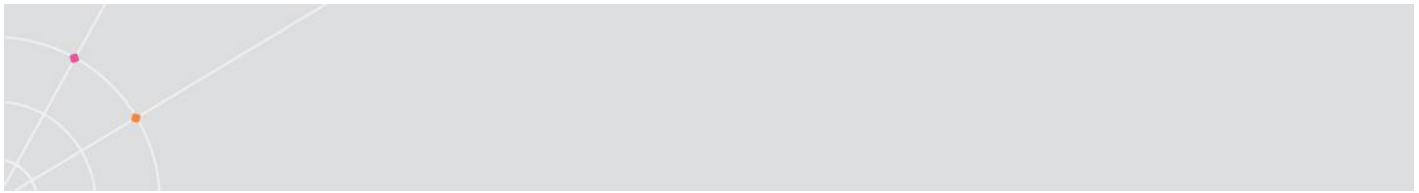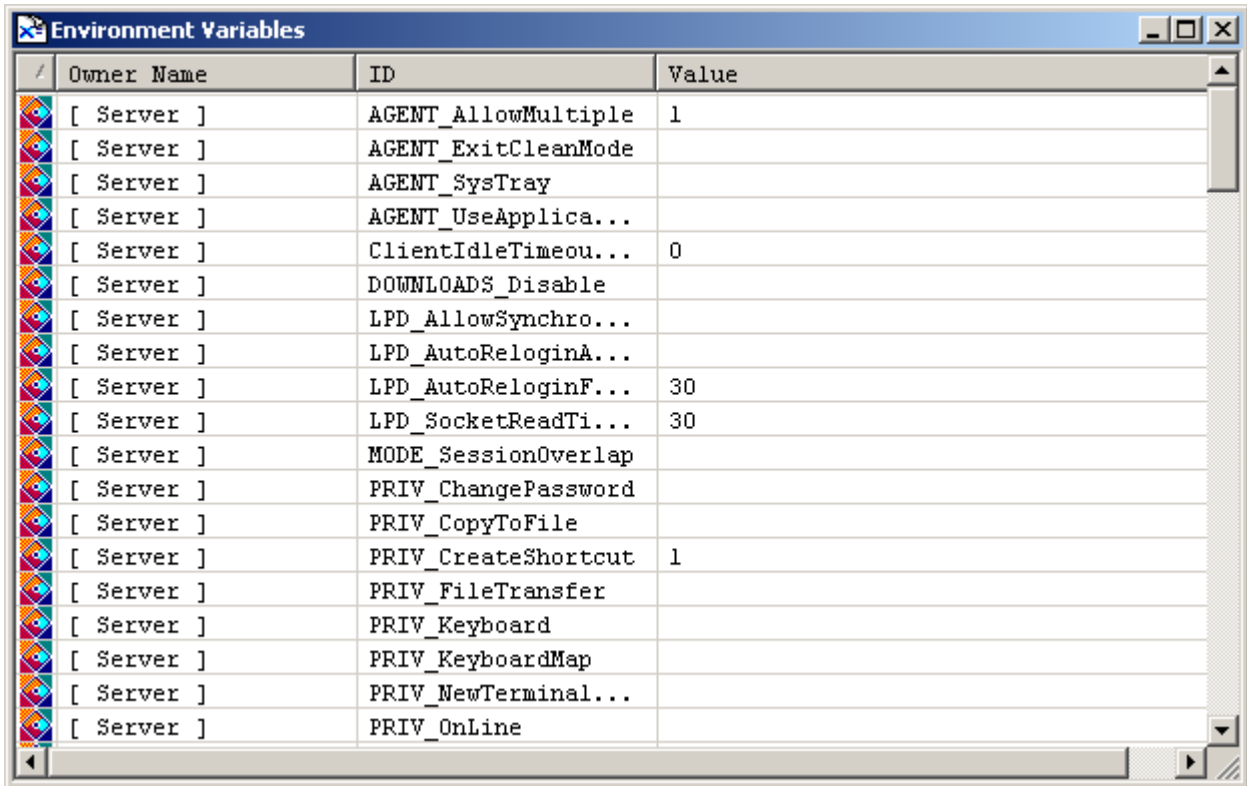
	clients.
PrintView Queues: Max	Specifies the maximum number of RemoteView queues that a user is allowed to have at any given time.
PrintView Queues: Default	Specifies the default RemoteView queue a user is allowed to have at any given time.
Administrator Auto Refresh Freq.	Specifies the time interval 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.
Help	Opens PowerTerm WebConnect Administration Tool online help.

3.3.5. Deployment and Performance Statistics Dialog
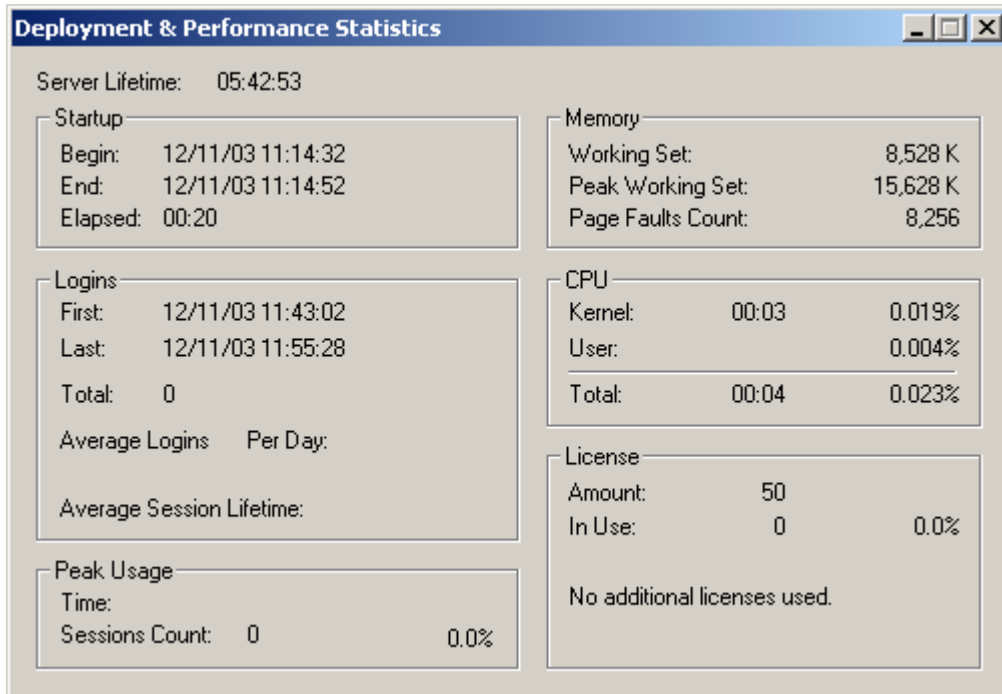
The Deployment and Performance Statistics dialog, displays real-time information for the PowerTerm WebConnect server. These statistics are similar to the ones that appear in the Performance tab of the Windows Task Manager. For more information see chapter 7.7.1.

3.3.6. Environment Variables Tables

Owner Name	ID	Value
[Server]	AGENT_AllowMultiple	1
[Server]	AGENT_ExitCleanMode	
[Server]	AGENT_SysTray	
[Server]	AGENT_UseApplica...	
[Server]	ClientIdleTimeou...	0
[Server]	DOWNLOADS_Disable	
[Server]	LPD_AllowSynchro...	
[Server]	LPD_AutoReloginA...	
[Server]	LPD_AutoReloginF...	30
[Server]	LPD_SocketReadTi...	30
[Server]	MODE_SessionOverlap	
[Server]	PRIV_ChangePassword	
[Server]	PRIV_CopyToFile	
[Server]	PRIV_CreateShortcut	1
[Server]	PRIV_FileTransfer	
[Server]	PRIV_Keyboard	
[Server]	PRIV_KeyboardMap	
[Server]	PRIV_NewTerminal...	
[Server]	PRIV_OnLine	

The Environment Variables window shows all the environment variables in the system, whether they are defined for users, groups, or the server object. It allows you to edit any of the variables. For more information see chapter 8.2.

3.3.7. Settings Dialog (for Emulation Clients)
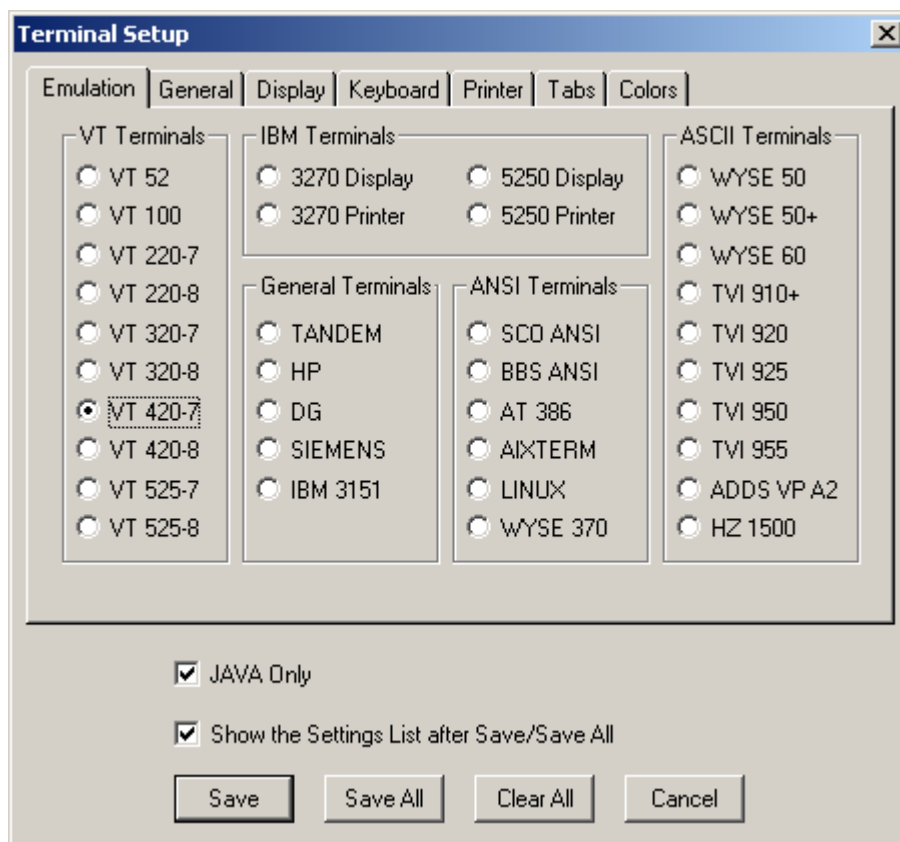
- **Emulation**, displays supported terminal emulations and enables you to select a terminal type.

- **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 and their options!
>
> NOTE The Java Only checkbox enables only the relevant fields for PowerTerm WebConnect Java client.

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	This option is only enabled when UPS Set is specifies as Code Page 437 and up. **Disable**, determines if 0x80 to 0xAF are displayed characters. **Enable**, determines if 0x80 to 0xAD are control characters. **0x9B**, all characters are displayed character except 0x9B, which is a control character.
Online	Equivalent to **Terminal	On Line (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 8th 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	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.
	Locked, prevents UDKs from being overridden.
	Unlocked, allows UDKs to be overridden.
Cursor Keys	Determines the behavior of the four arrow keys.
	Normal, generates ANSI-standard control sequences for moving the cursor.
	Application, generates customized application program functions.
Keypad	Determines the effects of the numeric keypad on your keyboard.
	Numeric, keypad keys insert number.
	Application, keypad keys generate control sequences that can be used by some applications.
	NumLock, enables or disables the NumLock keyboard function in respect to the above Numeric and Application modes.
Cursor coupling	**Vertical**, determines whether the user window pans with the cursor when the cursor moves past the top or bottom border of the user windows.
	Page, determines if a new page appears in the display when the cursor moves to a new page.
Status Line	**None**, displays an emulation screen without the status line.
	Indicator, displays the status line.
	Host Writable, displays the status line

	sent by the host.
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 you select an ID that the host application recognizes.
$=5B	Determines whether the character 5B represents a '$' or a cents sign. For RTL languages only.
Cursor Ruler	Select **Visible** to display full-screen, vertical or horizontal lines a as cursor ruler (cross hair guide). **Cross Hair**, displays the cursor ruler as a horizontal and vertical line. **Horizontal**, displays the cursor ruler as a horizontal line only. **Vertical**, displays the cursor ruler as a vertical line only.
Cursor	Controls the cursor appearance and functionality: **Block/Underline/Visible/Blink**, controls the cursor appearance. **Ins Change**, when selected it enables toggling the cursor between underline and block appearance, by clicking the Ins (insert) button.
Appearance	**Power GUI**, displays data in a window with 3D look & feel. Use system fonts larger than 10 pt for optimized results. **Show Frame**, places a frame around the text area of the emulation.
HLLAPI Names	Specifies the name of an hllapi session.
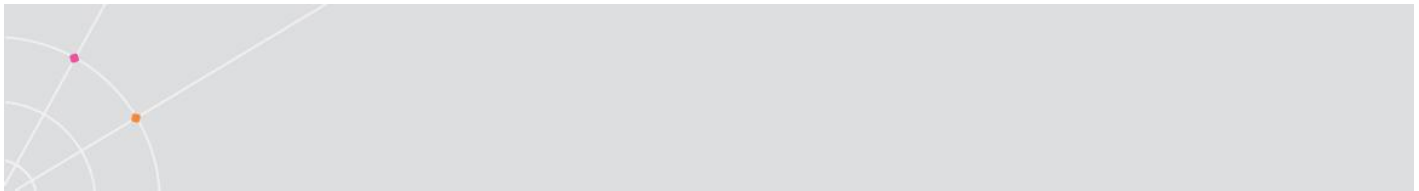
	Short/Long, enables you to specify the short and the long hllapi name
Code Page	Specifies the host and PC/Terminal (keyboard) terminal character sets.
Alternate Size	**Enable**, select to override the terminal alternate size with a specific size.
	Rows/Columns, type the required number.

Display tab

Option	Description
Reverse Display Colors	Reverses the text and background colors in the work area.
Autowrap 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. NOTE Selecting **Clear History** from the **Edit** menu can erase the History buffer.
Cursor Ruler	Select **Visible** to display full-screen, vertical or horizontal lines a as cursor ruler (cross hair guide).
	Cross Hair, displays the cursor ruler as a horizontal and vertical line.
	Horizontal, displays the cursor ruler as a horizontal line only.
	Vertical, displays the cursor ruler as a vertical line only.
Cursor	Controls the cursor appearance and functionality:
	Block/Underline/Visible/Blink, controls the cursor appearance.

	Ins Change, when selected it enables toggling the cursor between underline and block appearance, by clicking the **Ins** (insert) button.
Ctrl Characters	**Display**, displays the control characters.
	Interpret, 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 optimized 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).
	Limit Font Size, allows PowerTerm fonts to use only the optimal font size, especially for frames.
	NOTE 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.
	Unlimited, displays data without delaying communication.
	Page, scrolls data by full screens.
	Smooth, is equivalent to a Jump Scroll
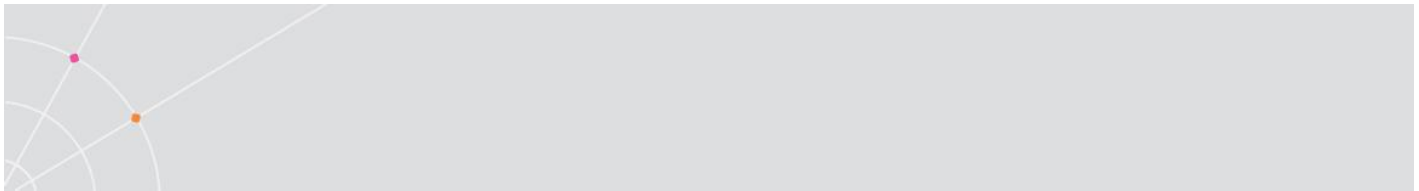
	Speed of 1.
Enabling Soft Fonts	Enables you to work with VT soft fonts. The fonts will be loaded from the host application.

Keyboard tab

Option	Description
Capslock Mode	Determines the behavior of the **Caps Lock** key.
	Caps (Unix), locks alphabet keys on main keypad in uppercase.
	Shift, locks alphabet and numeric keys on main keypad in shift setting. Pressing the shift button on your keyboard will release shift-lock mode.
	Reverse (Win), has the same behavior as Caps Lock, however pressing the shift button on your keyboard reverses the caps operation.
	Always On, 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.
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 (echoed) on your screen. **Select**, to display the keyboard input even if the host system does not echo your input. **Clear**, to send the keyboard input to the host system without being displayed on the screen (unless, invariably, the host system automatically echoes the characters).
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 **System Wait** in the IBM 3270 emulation will act as a **System Wait** in a non-SNA terminal.
Answerback Message	Specifies an answerback message and its
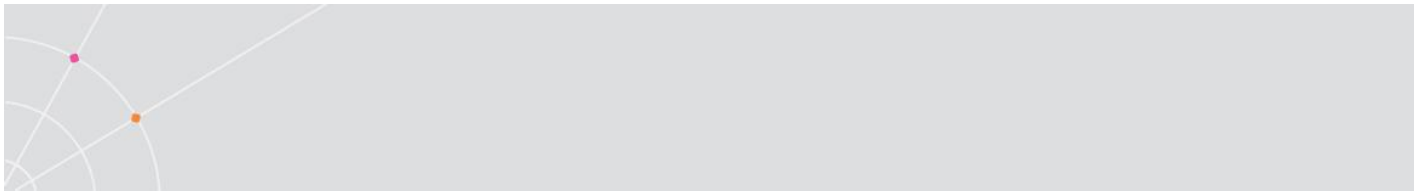
display.

Clear, deletes its message.

Conceal, hides the message without deleting it.

Printer tab

Option	Description
Print Device	Allows you to select a printing output channel.
	None, no destination was assigned. The Device Name is disabled. Printer data is received by the terminal, but discarded (not printed).
	Device, 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
	File, sends printing to the file specified in the File Name text field.
	AUX, sends printing to the auxiliary port.
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 **Device** in **Print Device**.
	Default: LPT1
File Name	Specifies the file name. Enabled when you select **File** in **Print Device**.
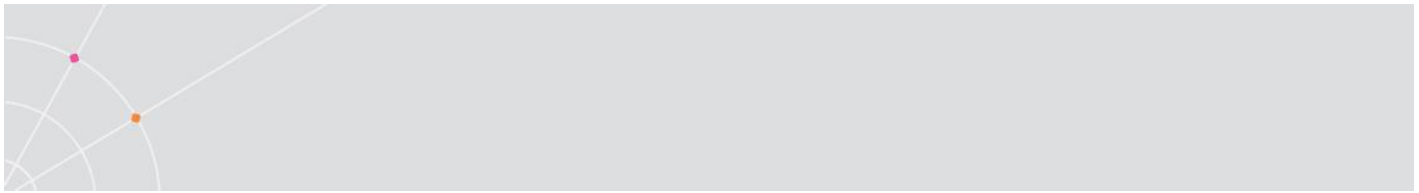
	File Creation, determines whether you want **Append** or **Overwrite** mode.
Print Screen Data Conversion	Converts data to Host or UTF-8 character sets or prints in **Graphics** mode. **None**, does not convert data. NOTE Text mode is designated by selecting Host, UTF-8 character sets or None.
Slave Printer Data Conversion	Converts data to Host or UTF-8 character sets or prints in **Graphics** mode. **None**, does not convert data. NOTE 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 **Tab Stops** 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	**Default**, 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).
	Attribute, colors based on the attributes. For example, you can select different colors for bold, for underline, and for bold/underline.
	ANSI, 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.
	Attribute & ANSI, 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 **Background** color never has the bold attribute

	(therefore it is "dark") while the **Text** (foreground) is always mapped to the color with the Bold (bright, light) attribute.
	Selected, each entity (text, background) can have any of the 8 colors mapped to them.
	Cleared, 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 **Normal**. 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.

4. Directory Services

PowerTerm WebConnect offers the ability to access User, Group and resource information from one of two places, either from within PowerTerm WebConnect's own database, or an external Directory Service (DS). The drawback to storing User and Group information within PowerTerm WebConnect is that it becomes necessary to maintain the external DS data as well as the PowerTerm WebConnect internal database. This entails managing two disparate databases with all the resulting maintenance issues. In order to avoid this, PowerTerm WebConnect is able to fully integrate with an existing LDAP DS such as Microsoft's Active Directory or Novell's eDirectory. No other DSs are supported in this version of PowerTerm WebConnect.

PowerTerm WebConnect is able to authenticate Users by identifying the DS User object and then applying the standard DS User authentication. After authentication, the PowerTerm WebConnect User instance is created.

4.1. Administration Tool Connection Process

PowerTerm WebConnect requires only read access to the Directory Service, except for the ability to change the password for the current user. This is because in the event that a password has expired, it is necessary to replace the expired password with a new password.

The Administration Tool needs to connect to the DS in order to define a new DS for the PowerTerm WebConnect server, or to be able to set the policies of the WebConnect connections. The PowerTerm WebConnect Server can connect to the Directory Service via one of two paths:

- Directly to the Domain Controller or Server where the DS is stored.
- Via the WebConnect server gateway.

The Administration Tool will connect via one of these options depending on the settings chosen in the New Directory Services dialog, as detailed in the Connection to a DS Section below.
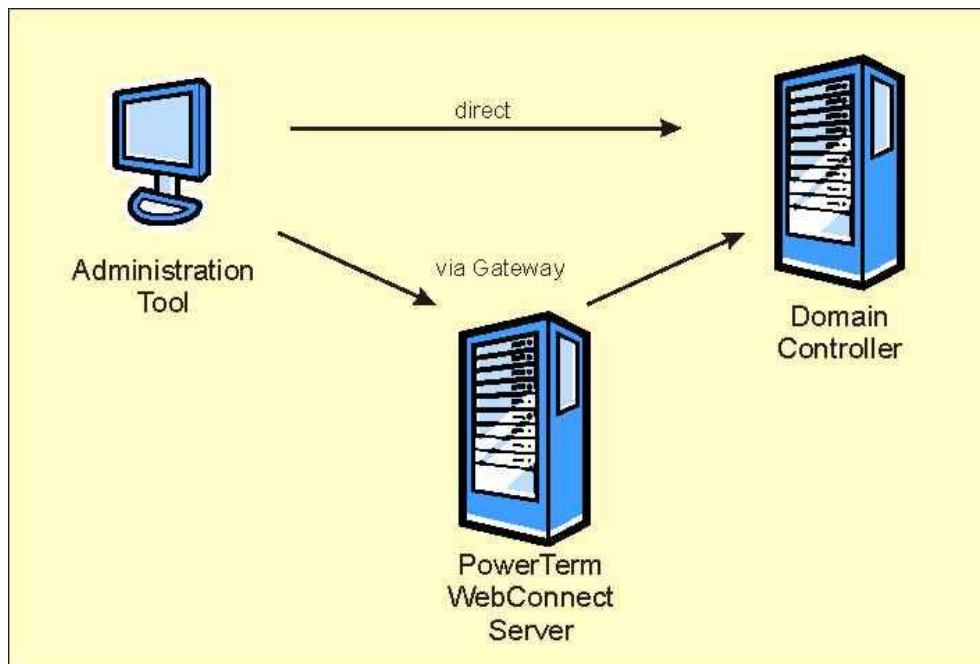
Administration Tool to DS Connection Process

If the computer on which the Administration Tool is running is within the same trusted network as the host of the DS, then it will be possible to connect directly using either an anonymous and/or a secure connection. If the computer on which the Administration Tool is running is outside of the trusted network in which the host of the DS resides, then it will be necessary to access the DS via a gateway. In this case, it is only possible to connect either anonymously or by supplying valid credentials.

Once the connection to the DS database has been configured, the PowerTerm WebConnect Server is able to authenticate Users and to retrieve the Groups of which the Users are members.

4.2. Connection to a Directory Services

By following the following procedure it is possible to configure the PowerTerm WebConnect Server to integrate with an existing Directory Service. Individual items that are related specifically to either Microsoft Active Directory or Novell eDirectory are detailed immediately following this.

The use of SSL provides enhanced security, but does so at the expense of increased traffic overhead and hence possible loss of performance and degradation of the network response times.

To integrate PowerTerm WebConnect with an existing Directory Services:

1. Launch the Administration Tool.

2. Select Server | Directory Services.
   If there is already a default DS identity defined on the WebConnect server computer, this will be discovered and displayed in the list automatically.

3. Clicking New will allow the Administrator to create a new DS. Highlighting one of the existing DSs will allow the administrator to view and update its properties, delete the DS from the list, or test the Directory Service.

4. 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.
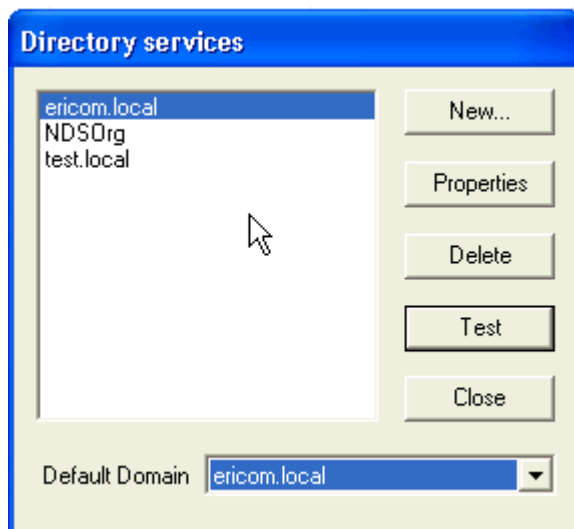
Directory Services Selection

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 assume that the user is trying to log in to the default domain, even when no domain is specified as part of the login.

It is possible to either create a new Directory Service, or to manually designate which Directory Service will be employed.

To create a new Directory Services:

1. Launch the Administration Tool.

2. Select Server | Directory Services.

3. In the Directory Services window click New. The window shown below will be displayed.

New Directory Services Window

4. If an attempt is made to create a new DS with the same name as an existing DS, the following warning will be displayed.
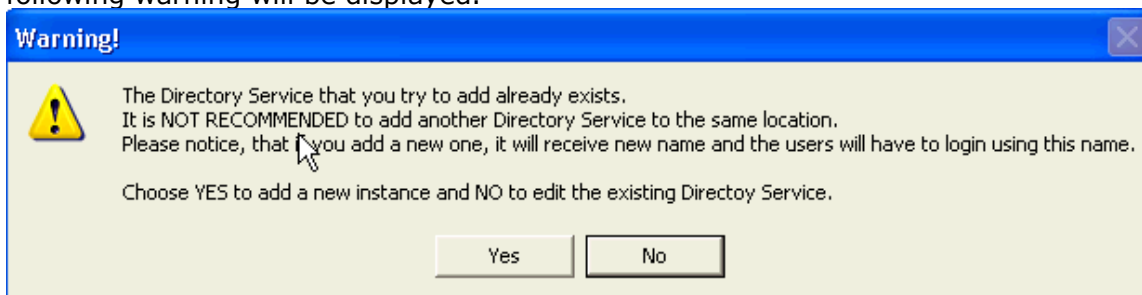
Warning Message when trying to Create a Duplicate DS

If the warning is ignored, PowerTerm WebConnect will create a new DS with the existing name modified by 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 eriocm.local_1, Users will to log in to this domain using a name of the form john@eriocm.local_1.

5. Enter the address as either 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.

6. Select the type of connection to be used from the drop-down list. Selecting "Specify credentials" requires the Administrator to enter a valid User name and Password with which to connect to the Directory Service. Selecting "Windows authentication (Kerberos)" will automatically allow the Administrator to log in to the DS using his current Windows login credentials.

7. Click Connect.
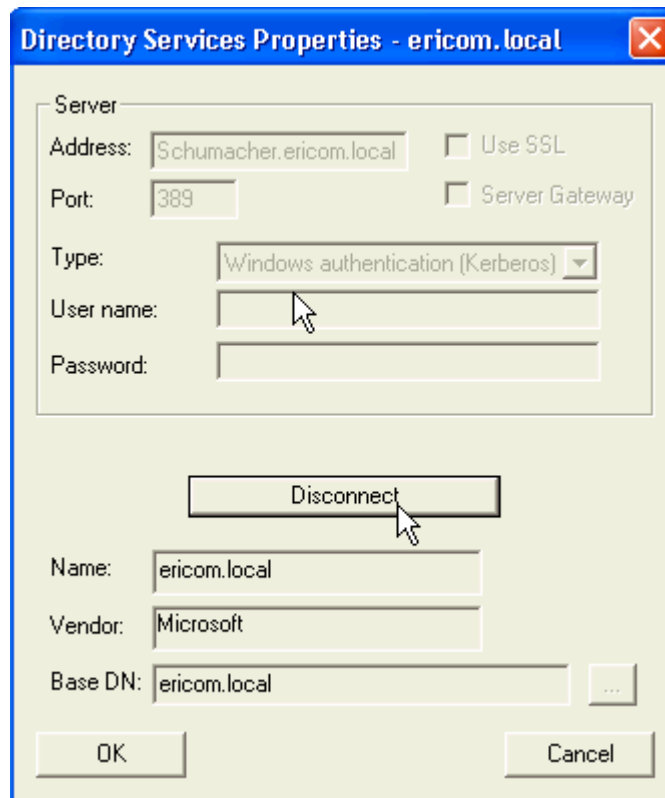
Connection made to Existing DS

8. As shown above, PowerTerm WebConnect will display the Name, Vendor and Base DN (root tree Distinguished Name) of the DS to which the Administrator is currently connected.

> NOTE When in a default configuration, connecting to an eDirectory DS anonymously will allow the Administration Tool to read the necessary objects. When connecting anonymously to a Microsoft Active Directory DS, the Administration Tool will not be allowed by the Active Directory to browse the DS.
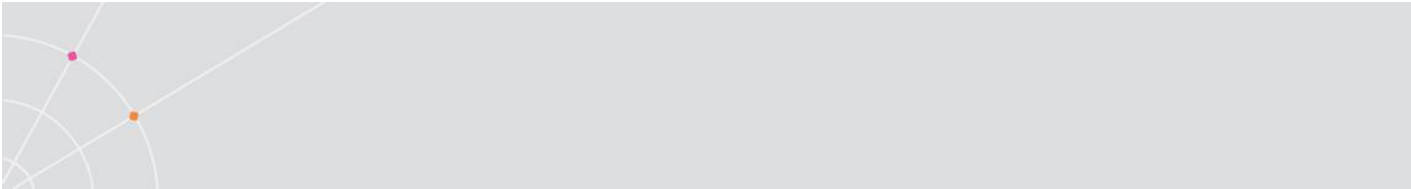
9. Click on the Details of the Base DN button to display the resources stored within the DS.
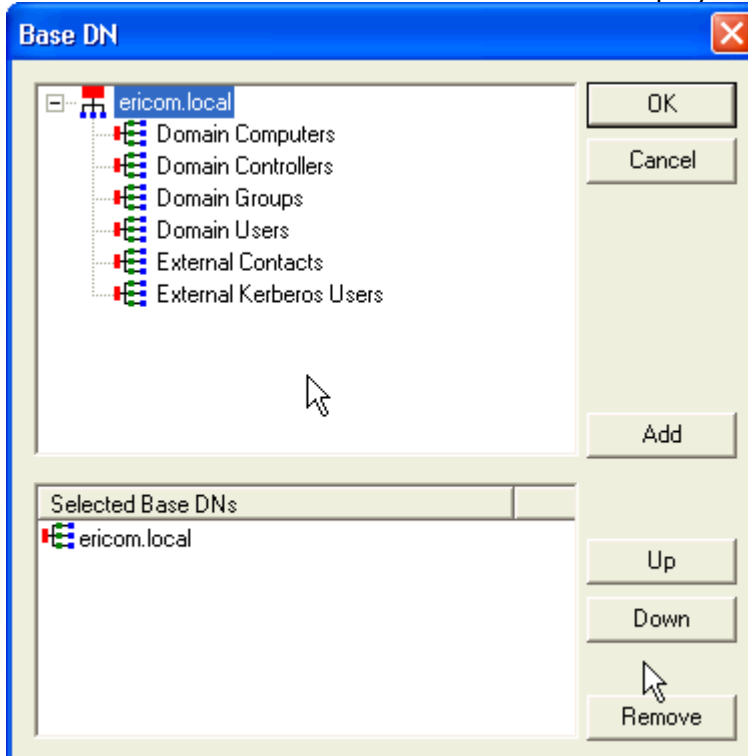
Resources Stored in the Selected DS

By selecting the required Organizational Units (OU), it is possible to tell the WebConnect server in which OU the Users are located. 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 specified OU. The default is to search the entire tree, which is not recommended.

10. Highlight any Organizational Units, Click Add to add the Organizational Units to the Selected Base DNs list. Multiple Organizational Units may be added.
Alternatively, double click on any Organizational Unit to display the branches of the Organizational Units. Highlight any branch to add it to the Selected Base DNs list. Multiple branches may be added. This process may be followed as far down the tree as required.

11. When all required resources have been added to the Selected Base DNs list, arrange the order in which they will be searched by using the Up and Down buttons. Changes in the

order of searching may have a serious impact on the login response times. It is preferable to be as specific as possible when selecting authorized Base DNs.

4.2.1. 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

Connection Options and Ports

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

4.2.2. Publishing Applications

Applications may be published to OUs (Organizational Unites), Groups or Users as described in the Published Application Configuration section, apart from the following new step.
This step allows the publishing of applications to users using LDAP functionality.

To add or remove Objects for the published application:

1. From the PowerTerm WebConnect Administration Tool click Action.

2. Click New.

3. Click Windows Application. Step through the required Application steps until the following window is displayed.
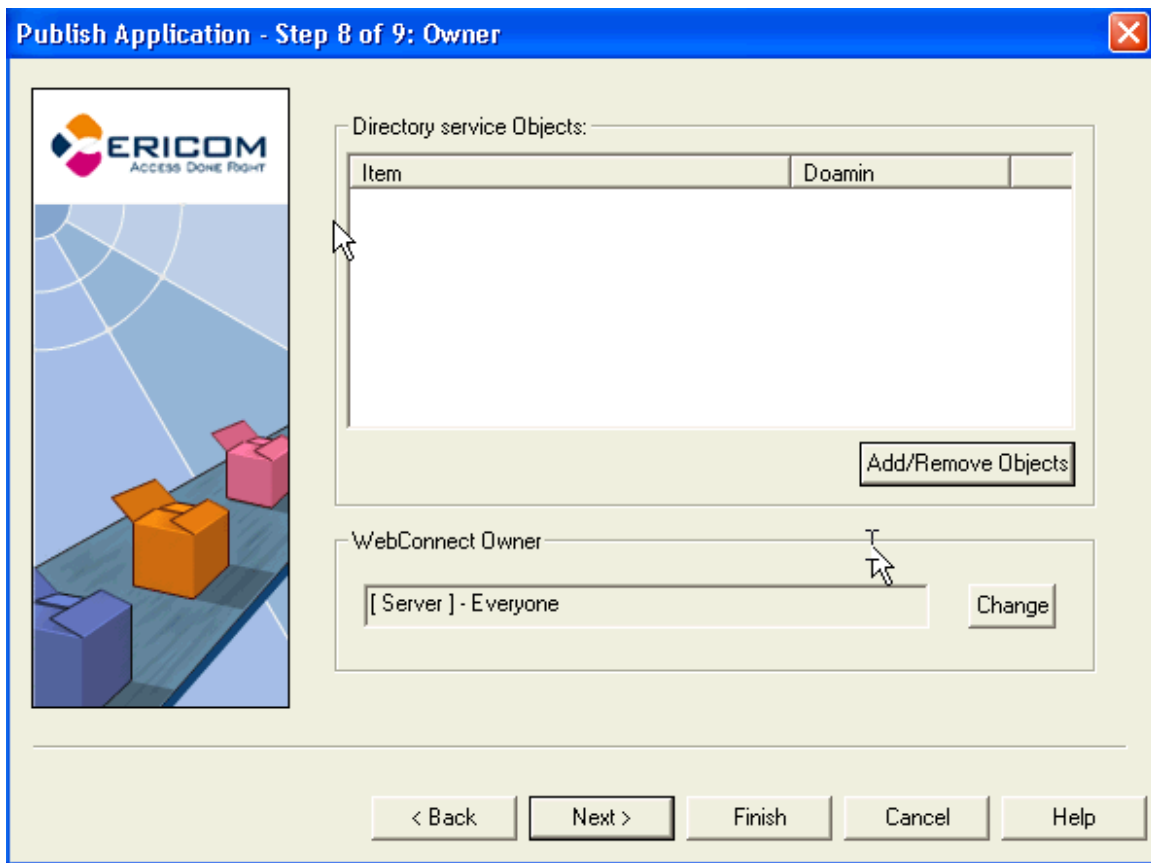
Adding or removing Directory Objects for Published Applications

4. Click Add/Remove Objects. The following window will be displayed.
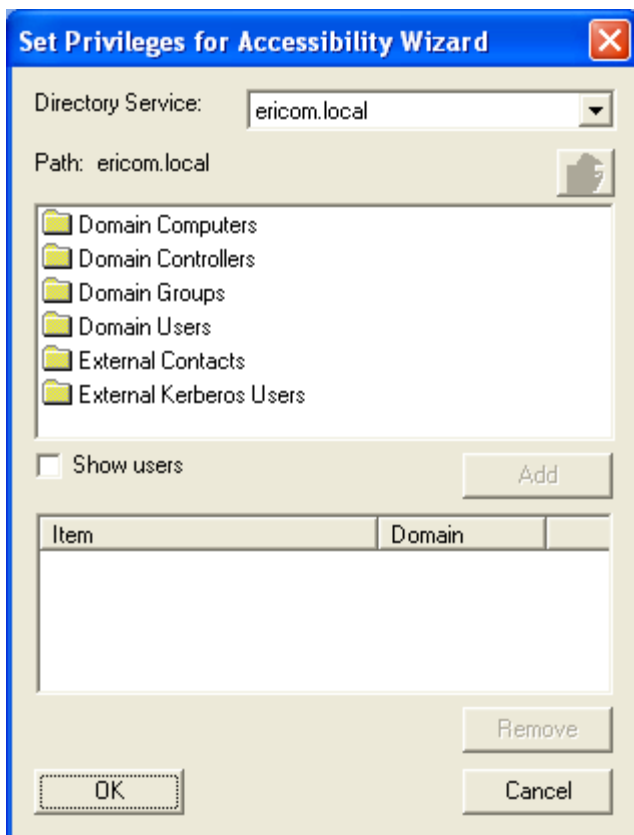
Adding LDAP users, groups or OUs for published applications

5. Select the required Directory Service from the drop-down list. The OU and Group members of the selected DS will be displayed.

6. Select one or more OUs and/or Groups.
    The Administrator should bear in mind that Groups may be members of one or more Groups, whereas OUs may belong to only one OU.

7. Click OK.

> NOTE   Events or changes that occur to published applications within PowerTerm WebConnect, such as, changes in Groups are monitored, and are therefore automatically reflected in the PowerTerm WebConnect Application Zone. Events or changes that occur within the DS are not monitored, and are therefore not reflected automatically in the PowerTerm WebConnect Application Zone.

8. Click Change to modify the PowerTerm WebConnect Owner.

> NOTE   Selecting "[Server] - Everyone" is not secure and should generally not be used.

9. Click Next.

4.2.3. Defining the Novell eDirectory domain base name

Given a user with the following DN:

- cn=user1
- ou=Users
- ou=SaleDepartment
- ou=NDSOrg

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

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

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

4.2.4. Notes

The order of authentication is as follows:

- A check is performed on the client for a Domain to connect to.
- If none is specified, the default is used. If there is no default, the connection will fail.

The naming convention for Active Directory must be of the form `user@domain`. The naming convention for eDirectory must be of the form `user,path.domain`. By default, the root of the tree will be the domain name.

PowerTerm WebConnect allows for the use of Organizational Units, Groups or users for publishing applications.

5. Defining Users and User Groups

NOTE PowerTerm WebConnect allows you to create user and groups in a simple way using Directory Service Integration. However, if for any reason you decide not to use this feature you can still create users and groups in the former PowerTerm WebConnect way.

5.1. Users, Groups, and Connections: Building-Blocks of an Access Policy

The Administration Tool allows you to define an access policy for a host server. The access policy specifies which users can access the host under which conditions.

5.1.1. User Objects and Connection Objects

The basic element of an access policy is the user object, which represents one person (or entity) in the organization. A user object's properties define a user's credentials, the methods by which the user can accesses the system, and his or her access rights. A user object can also define how a specific user's client software should appear and behave.

Another object, called a connection, defines the manner in which users connect to a host server. A connection object specifies the host type and the protocol used to connect to it, and allows you to set communication options specific to that protocol. Depending on the client used for the connection, a connection object can also define the behavior and look-and-feel of the client. For example, for the PowerTerm WebConnect HostView emulation client, connection properties control the behavior of the Power Pad (a floating panel of special definable function buttons) and map keys on the user's keyboard to terminal keys or to script commands. Published applications are represented as connections, containing additional information such as target application and load balancing settings.

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.

5.1.2. Group Objects

The group object represents a group of users with similar access needs (for example, members of a certain department). Group objects allow you to define more complex access policies.

A group contains a number of user objects, and has its own set of properties. When a user object belongs to a group, it will inherit some or all of its properties from the group. Any properties not explicitly defined in the user object are taken from the user's group. Conversely, settings defined at the user level override the settings at the group level.

For example, at the group level you can define that users are allowed to open no more than two host sessions simultaneously (by setting the group's Max. Concurrent Sessions parameter to "2"). Assuming this parameter was not defined explicitly for each user, all the group's members inherit this setting, and are allowed a maximum of two concurrent sessions. If a particular user, such as the group's manager, John, needs to be able to open more sessions simultaneously, then his user object's Max. Concurrent Sessions parameter can be set to "4". Since the user-level setting overrides the group setting, John is allowed more concurrent sessions than his co-workers.

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.

Group Membership

Every user must belong to at least one group. If a user belongs to a number of groups, one of these groups must be set as the user's default group. This is the group from which the user inherits properties. As for other groups, which are not the default, the user can use their connections but does not inherit their properties.

5.1.3. The Server Object – a "Master Group"

Just like users inherit settings from groups, groups inherit settings from a "master group" – the server object. The server object has a dual function: to define server-related settings, and to set the basic defaults for all objects.

If a certain property is not defined at the group level, the group object inherits the default option defined at the server level. By contrast, if the group has an option explicitly defined, it overrides the option defined at the server level. Essentially, settings defined at the server level apply to the entire organization, unless you specify otherwise for a certain group or user.

For example, on the server level you can set that only two concurrent sessions are allowed per user. By default, all groups and users inherit this setting. However, for the

"Technical Support" group (those who have that group defined as their default) are allowed up to six concurrent sessions.

> 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.

In addition, the server object can be set as the owner for specific connections. Such connections become available to all the users.

5.1.4. Summary: Object Interrelationships and Hierarchy
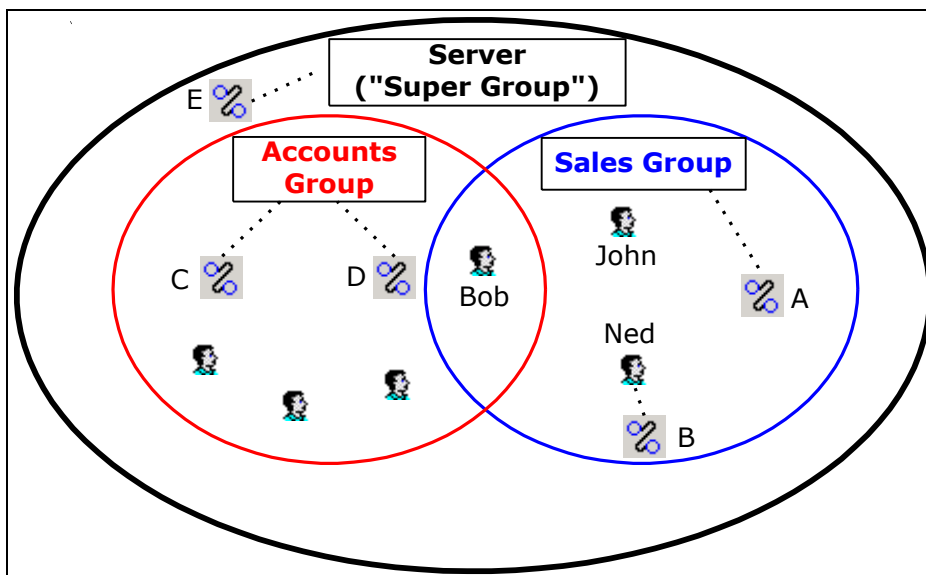
The diagram above shows a simplified PowerTerm WebConnect server with two users belonging to the "Sales" group, three belonging to the "Accounts" group, and one user, Bob, belonging to both. All these users belong to the "Master Group" – the server. The diagram also shows five connections with different 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 connection A, because he belongs to the "Sales" group, as well as to connection E because he belongs to the "Master Group" (the server). John inherits default settings from the "Sales" group (and, in turn, from the server).

- **Ned** is the only user with access to connection B because he owns it. He also has access to connections A and E as a member of the "Sales" group and the server. Ned inherits default settings from the "Sales" group.

- **Bob** belongs to two groups and to the server. Therefore, he has access to all the connections shown (except B, which Ned owns). Bob inherits default settings from his default group, which can be either "Accounts" or "Sales".

Please note that any properties defined explicitly for John, Ned, or Bob override the defaults of their respective groups and the server.

Object Hierarchy

The following diagram shows how properties descend the hierarchy from the server, to the groups, and to the users, while options explicitly defined at a lower level override those at a higher level.
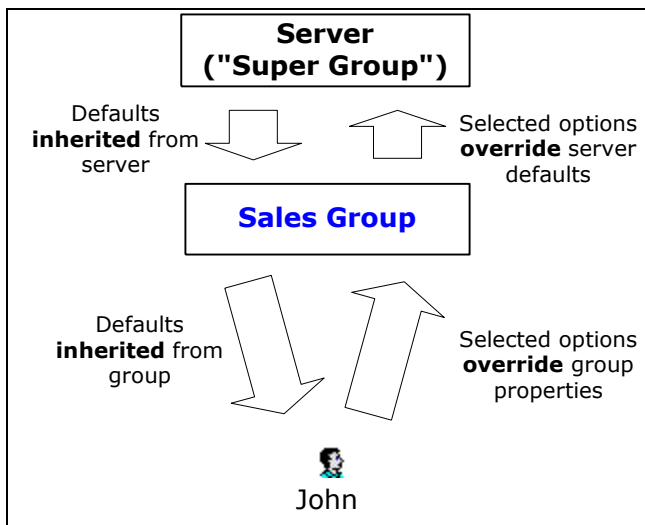
As explained in chapter 1 the Administration Tool's access policy encompasses three main objects types: user, group, and server, (which will also be referred to as the "master group"). The connection object type, which is also vital to an access policy, is discussed in chapter 6. This chapter explains how to make optimal use of the object types.

5.2. Planning Your Access Policy

Before starting to define users and groups, you should consider the following questions:

- Which users in the organization should have access to the Host server?
- Do all the users have similar needs, or are there groups of users with distinct access needs?
- Do different users need different client functionality?

- How will changes in the organization's structure and its personnel affect your access policy?

The following table summarizes the differences between the access rights of the different user profiles.
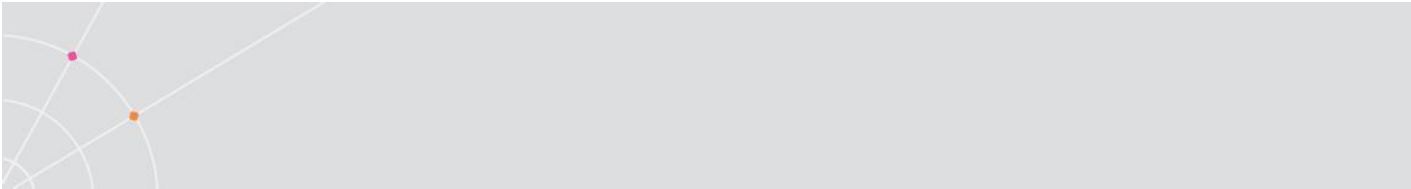
Components/User Rights	User	Supervisor	Administrator
All clients, HostView, RemoteView, PrintView, QuickVNC, etc. to connect to a host	Yes	Yes	Yes
Request support from other Administrators or Supervisors logged on to PowerTerm WebConnect	Yes	Yes	Yes
Provide support to other PowerTerm WebConnect users	No	Yes	Yes
Modify User's profiles by accessing the Administration Tool	No	No	Yes

The following sections explain how these issues relate to the three main building blocks of the access policy – user, group, and server.

5.2.1. Using Groups Effectively

If you have groups of users with distinct needs, you should create several group objects, each with explicit settings that override the server defaults.

But even if different groups in your organization do not presently have distinct needs (for instance, the Accounts and Sales department do not need different client functionality at the moment), it may be a good idea to define them as separate groups

in preparation for the future. In the meantime, these groups can inherit most of their settings from the "master group" (the server object).

Another benefit of designing different groups (even if they do not carry explicit settings) is that they can create a logical division that matches your organization's structure. This makes it easier to organize and find users, particularly if there are many of them. However, if you create too many groups, or arbitrary groups that do not follow a clear convention, it may cause chaos in your user database.

5.2.2. User Object Properties: To Define or Not?

As is discussed later in this chapter, some user properties are "standalone" - defined only at the user level (for example, User Name). However, other properties are "optionally inherited", meaning they can either be left open and inherited from the default group, or defined explicitly for the specific user, overriding the group-level setting.

Before you start to create user objects, you should decide how to use "optionally inherited" properties, leaving them undefined and allow users to inherit from the group, or define them explicitly. Your choice will have serious ramifications later on; the following sections explain the pros and cons of each approach.

Allowing Users to Inherit Properties: Pros and Cons
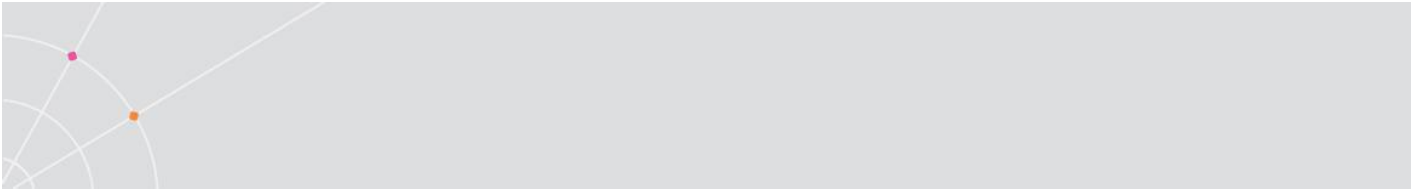
The advantage is that it saves time. If users have no properties explicitly defined, you can simply add them to a group and they assume the properties of the group, so there is no need to define properties user-by-user. Leaving user properties undefined allows you to predictably apply properties to many users at a time, by setting them at the group or server level.

The disadvantage is a loss of flexibility. If you have specific users who need different settings from the others in their group, you must be careful before defining properties explicitly at the group level.

Defining Properties at the User Level: Pros and Cons

The advantage is that you can define specific settings for each user. This can be important since most user groups are fairly heterogeneous, and many users need special treatment.

The disadvantage is a lack of predictability and a higher workload. If you occasionally define properties at the user level (so that some users inherit some of their properties while other properties are fixed and cannot be changed), it is difficult to predict what will happen when you move users from place to place. Imagine moving twenty users from one group to another, and having to track what inherited options will change as a result, and which will not because they are defined explicitly. If, on the other hand, you

consistently define all properties at the user level, you must apply changes to every user individually, and this takes time.

5.2.3. 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.

5.2.4. General Properties at the Group/Server Level

Many options that effect users cannot be defined explicitly in the user object (unlike "optional inherited" properties, which can either be defined explicitly or inherited). These "general properties" are defined as properties of the server object or a group, and are automatically inherited by all member users.

For example, the Max. Intrusion Attempts parameter, which 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 customize this parameter for specific users or groups.

5.2.5. Implementation Workflow

The following procedure is a general guideline, explaining how to define users and groups for the first time.

1	Creating administrator users	Define the attributes and privileges of the Administrator	Chapter 5.3.2
2	Customizing default groups	Review the default groups, supplied with the Administrator,	Chapter 5.3.4
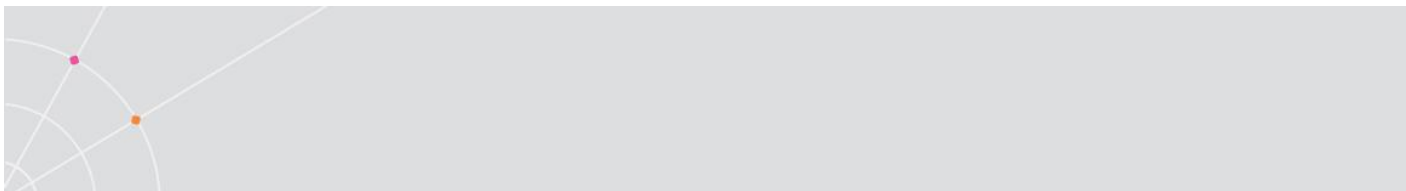
		evaluate their suitability for your access policy, and modify their properties as needed.	
3	Creating new groups	If you require groups other than the basic default groups, create them.	Chapter 5.4
4	Creating users for each group	Collect the credentials (usernames and passwords) for all the users in each group and create user objects for each of them.	Chapter 5.3.4
5	Creating connections	Define the communication parameters that enable the client to connect to the host computer by way of the server.	Chapter 6.1

5.3. Defining Users

Generally speaking, you should define a user object for each person who will access the PowerTerm WebConnect server – both regular users and administrators – or use the "AutoCreated users" facility to generate them automatically. In special cases, several different people can use a single user object. An example is the "Guest user" object, which is supplied by default.

The following sections explain:

- User object properties, which define user credentials, group membership, connections, system permissions, and allowed access methods (chapter 5.3.1).

- Default user objects supplied with the Administration Tool, and how they are used (chapter 5.3.2).

- How to create, modify, delete, and disable users (chapter 5.3.3).

- How to customize a user's client settings (chapter 5.3.5).

- How to monitor group properties and runtime information (chapter 5.4).

5.3.1. User Object Properties (and how they are inherited)

The user object has properties that define user credentials, linked connections, group membership, system permissions, and allowed access methods. These user properties can be defined explicitly using the Add User / User Properties dialog, or inherited from groups or the "master group" – the server object.

To make it easier to understand how user properties are inherited, we have divided them into four types:

- Standalone properties: These are properties that can only be defined at the user level (i.e. using the Add User or User Properties dialog). They cannot be inherited from the group or server. An example is the User Name property, which is always user-specific.

- Shared properties: These are properties that refer to more than one object at a time. When you change them for a user object (using the Add User or User Properties dialog), they change for the other object/s as well, and vice versa. For example, the User's Connections property defines which connections are attached to the user object. When you add a connection here, the Owner property in the connection object changes. If you add a user as the Owner of a connection object (using the Add Connection or Connection Properties dialog), the user's User's Connections property changes.

- Optionally inherited properties: These are properties that can be defined at the user level, but also at the group or server level. If they are not explicitly defined at the user level (using the Add User or User Properties dialog), 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 "master group" – the server object. An example is Max. Concurrent Sessions, which defines the maximum number of client sessions the user is allowed to open.

- General properties: These are always inherited from the user's group and/or from the server, regardless of what you define in the user object. Some of these properties can be defined in the user object, but the user-level setting does not override the properties set at a higher level.
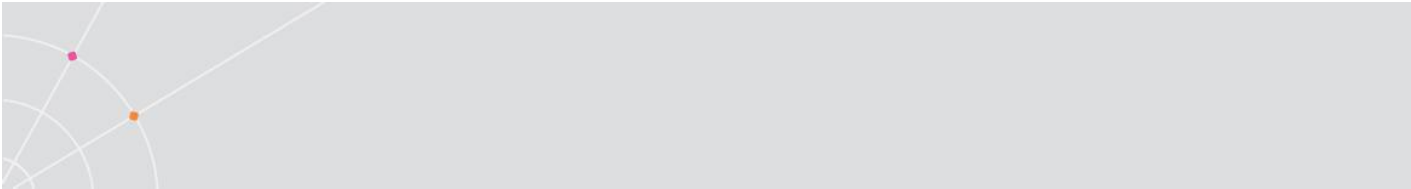
The following section explains the Add User/User Properties dialog, which is used to explicitly define user properties. The following sections list and detail standalone, shared, optionally inherited, and general user properties.

Using the Add User / User Properties Dialog

The User Properties dialog (called the Add User dialog when you are creating a new user) has several main components:

- User properties fields: These take up much of the dialog, and allow you to define a new user object's properties, or view and modify the properties of an existing user. The following sections demonstrate which of these are standalone, inherited, or shared properties, and provides an explanation for each of them.

- Environment variables table: This table allows you to create and edit free-text variables that have numerous uses, including customization of emulation client

appearance and behavior (see chapter 8.2). Environment variables you add here are defined on the user level.

- Settings button: Launches the Settings dialog, which allows you to customize emulation client appearance and behavior. Client settings you modify using the dialog are defined on the user level.

- Memo button: Opens a text file to enable you to type a memo conveniently and save it.

- Sessions button: Shows information for client sessions opened by this user.

- Up and down arrows: Clicking these arrows switches to the previous (up) or next (down) user, as sorted in the Users pane. You will be prompted to save any changes you have made.

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

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

Standalone Properties

Standalone properties are properties that can only be defined at the user level (using the Add User or User Properties dialog). They cannot be inherited from the group or server. In other words, they are user-specific.

Property	Description
User Name	The unique name of the user.
Alias	An alternative name or ID for the user that is not necessarily unique.
ActiveDiretory Path	The Active Directory Path identifies users for PowerTerm WebConnect. Click the adjacent button to browse for the correct path.
Use Network Password	Specifies that the PowerTerm WebConnect server authenticates the user with the network. When the checkbox is cleared, the Password button is enabled. Click it to specify the PowerTerm WebConnect password.
Password	The user's password. Ignored if

	Network Password is used instead.
Free User	Enables the user to specify the connection properties. This allows the user to connect to any accessible host.
Allow Concurrent Machines	Specifies that the user is allowed to log on simultaneously from multiple computers.
Rights	Selects whose rights will be accorded to the user being created. Select one of the following options:
	Administrator, allows the individual to use the Administration Tool.
	Client, does not allow the individual to use the Administration Tool.
	Supervisor, an intermediate role. The user cannot use the Administration Tool. However, the user received notifications on intruders and working-set exceeding size. Also, this user gets support requests from clients, as a Support Team member.
Access Limit Mode	Specifies the rule according to which the user is allowed to access the PowerTerm WebConnect server. Select one of the following options:
	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 file to enable you to
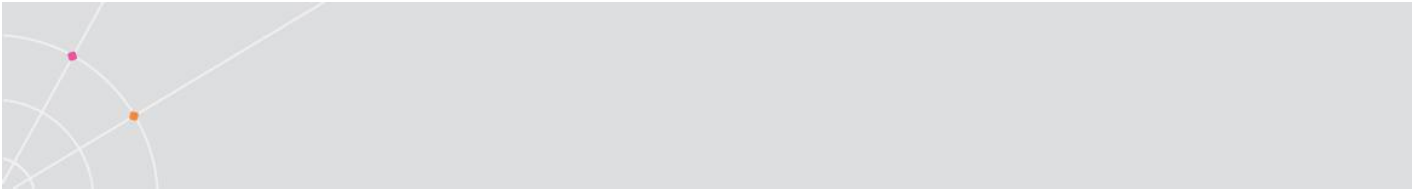
	type and save free-form information about the user.

Shared Properties

Shared properties refer to more than one object at a time. When you change them for a user object (using the Add User or User Properties dialog), they change for the other object/s as well, and vice versa. When you change these properties in other objects, they change for the respective user object.

Property	Description	Property shared with…
User's Groups	Select a group from the Available Groups box and click the right-arrow to make the user a member of the group. Use the multiple right-arrows to add all the groups. Double click a group in the User's Groups box to make it the user's default group.	Groups. Every group you add here has this user added under Group's Users. The opposite is also true: If you add this user to a group (using the Group Properties dialog), the group is added here.
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. Use the multiple right-arrows to affiliate all the unaffiliated connections to this user. The user can select one of the connections show here (or one of the connections inherited from groups and the server) when logging	Connections. For every connection you add here, the user is added as the Owner in the connection object. The opposite is also true: If you set this user as a connection's Owner (using the Connection Properties dialog), the connection appears added here.

	in.	

Optionally-Inherited Properties

Optionally-inherited properties can be defined at the user level, but also at the group or server level. If they are not explicitly defined at the user level (i.e. using the Add User or User Properties dialog), 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 "master group" – the server object.

Property	Description	Inheritance
Settings	This button opens a dialog that allows you to customize client settings for this user (see chapter 8)	If you do not define any client settings using this button, all client settings are inherited from the default group.
Max. Concurrent Sessions	Specifies the maximum number of concurrent sessions that this user may have. 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's value from the default group. If the default group also has '0' defined, the value is inherited from the server object's Default Sessions property.
Max. LPD Queues	Specifies the maximum number of LPD queues that this user will be allowed to have at any	Enter '0' to inherit this property's value from the default group. If the default group also

	particular time. Enter '0' to revert to the default group's setting (or the server's setting).	has '0' defined, the value is inherited from the server object's Default LPD Queues property.
Highest Reconnect Mode	Specifies the rule according to which the user is allowed to reconnect to the PowerTerm WebConnect server (see chapter 15). Select one of the following options: None, specifies that no reconnect occurs. Default, specifies that the value is received from its associated group. OnDemand, specifies that reconnect is only performed via the Gateway. Wireless, specifies that reconnect is performed via the Gateway.	Select Default to inherit this property's value from the default group.
Environment Variables	This table allows you to create and edit free-text variables that have numerous uses, including customization of emulation client appearance and behavior (see chapter 8.2).	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 explicitly define them here, they are inherited from the group. Environment variables that are not defined
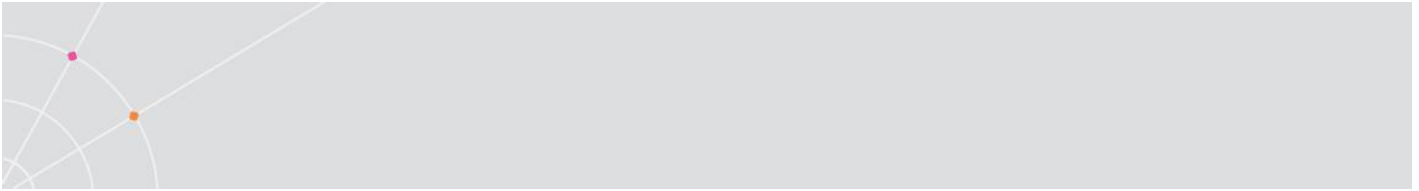
		here but are defined for the user's default group, function as general properties – they are always inherited (see next section).

General Properties

General properties are always inherited from the user's groups and from the server, regardless of what you define in the user object. Some of these properties cannot be defined in the user object. Others can be defined explicitly, but the user-level setting does not override the properties set at a higher level – rather, it is added to the setting at a higher level.

Some of the general properties can be configured in the User dialog whereas other general properties cannot be defined per-user, and so they do not appear in the dialog.

Property	Description	Inheritance
User's Connections	Select a connection from the Available Connections box and use the right-arrow to make the user the owner of the connection. Use the multiple right-arrows to affiliate all the unaffiliated connections to this user. The user can select one of the connections shown here (or one of the connections inherited from groups and the server) when logging in.	In addition to the connections you define here, the super object inherits connections from all the groups it belongs to, and from the server. Therefore, the user always has access to all the connections owned by his/her groups and the server.
Enabled	Specifies whether to make the user active. Only active users can	If the default group is disabled (the Enable checkbox in the Group

	connect to the server.	Properties dialog is not selected), the user object inherits this setting and becomes disabled as well. This happens even if the Enabled checkbox is selected here.
		However, if the user is disabled, it remains disabled even if the default group is enabled.
Allow Access From	Specifies the machines from which the user is allowed to access PowerTerm WebConnect. NOTE Field is only visible when the value for Access Limit Mode is either "User" or "Both".	In addition to the connection sources you define here, the user object inherits computers and addresses from all the groups it belongs to. So the user can always connect from all the addresses and computers defined under Allow Access From in his/her groups (in addition to the sources defined here).
Environment Variables	Specifies variable names and associated values. These PowerTerm WebConnect Environment Variables can be accessed from the login scripts (using the w2h-var PSL command). The dynamic device names for IBM emulations can also use these	Environment variables that are not defined here for the user's default group and on the server function as general properties. They are always inherited. Therefore, a user object always acquires environment variables defined for its default group, as well as those defined for

	variables, referring to them as %X"var-name".	the server object. However, 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 here explicitly, they are inherited from the group (see previous section).
Client Inactivity Timeout* (server object)	Specifies the inactivity timeout for all clients.	Always inherited from server object.
Max. Sessions* (server object)	Specifies the maximum number of PowerTerm sessions that can be opened simultaneously.	Always inherited from server object. The user's Max. Concurrent Session parameter must always be lower than the Max. Sessions defined on the server.
Max. LPD Queues* (server object)	Stipulates maximum number of LPD queues that this user will be allowed to have at any particular time.	Always inherited from server object. The user's Max. LPD Queues parameter must always be lower than the Max. LPD Queues defined on the server.
Max Intrusion Attempts* (server object)	Stipulates maximum number of unsuccessful login attempts the user can attempt to the PowerTerm WebConnect Server.	Always inherited from server object.
Intruders Disable Timeout* (server	Stipulates the amount of time the PowerTerm	Always inherited from server object.
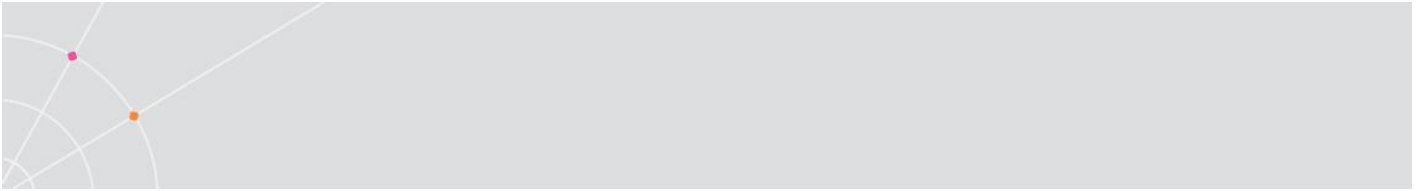
object)	WebConnect Server refuses to login a valid user after detecting an intruder.	
Background Bitmap File	Stipulates the background bitmap on the screen.	Always inherited from server object. If the user runs the HostView client, this image is used as the background.

* Does not appear in the User Properties/Add User dialog, as it cannot be defined per-user. You can define this property using the Server Configuration dialog.

5.3.2. Using Default User Objects

Several default user objects are supplied with the Administration Tool. The following sections explain what each of these can be used for.

<Generic Customer>

Used by the Support VNC in generic support mode.

Try the following hypertext links in the Clients' URLs.htm: Call Administrator support.

Call the Tech Support for assistance.

The attributes of this user cannot be modified.

<Portal>

Used by the PowerTerm WebConnect portal component.

<Software Installer>

Used by the Agent to install the clients PrintView, HostView, and WebView.

Try the following hypertext links in the Clients' URLs.htm:

Install the PrintView component.

Install the HostView component.

Install the WebView component.

This user's attributes cannot be modified.

Administrator

Used to login to the Administration Tool for the first time since no password is requested.

We strongly recommend that you immediately create another administrator account, with password and fewer privileges.

By default: Has no password

Access limitations: no concurrent machines, LOCALHOST (the server's console) only.

Default AutoCreated User Template

Used by PowerTerm WebConnect for Windows to automatically create user entities for any user authenticated by the network (NTLM).

Example

This user is implemented in both the Example_VT and Example_AS400 connections. These connections are used in the WebView examples.

This user's password is `example`.

Guest

Used to allow temporary users. A slightly restricted user in that the user is unable to request Tech-support or Administrator support.

By default: Has no password

5.3.3. Creating, Modifying, Deleting, and Disabling Users

Once you create a user object, you can make changes to all its properties (with the exception of Allow Access From, which can only be set when you create an object).

You can also delete or disable a user object. Both these actions have the effect of preventing the user from accessing the server again. If you intend to use a user object again in the future, disable it instead of deleting it. When you need it again, you can enable it again.

NOTE If the user's default group is disabled (see chapter 5.3.3), 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 create a user:

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

To modify user properties:

1. Double-click the desired user or right-click on the desired user and select Properties.

2. Modify the necessary properties.

3. Click OK.

To delete a user:

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

2. Click OK.

To disable a user:

1. Select the desired user and right-click Properties or select Action | Properties.

2. Clear the Enabled checkbox.

3. Click OK.

To enable a user again after disabling it:

1. Select the desired user and right-click Properties or select Action | Properties.

2. Select the Enabled checkbox.

3. Click OK.

> NOTE   This will only work if the user's default group is also enabled (see chapter 5.4.2).
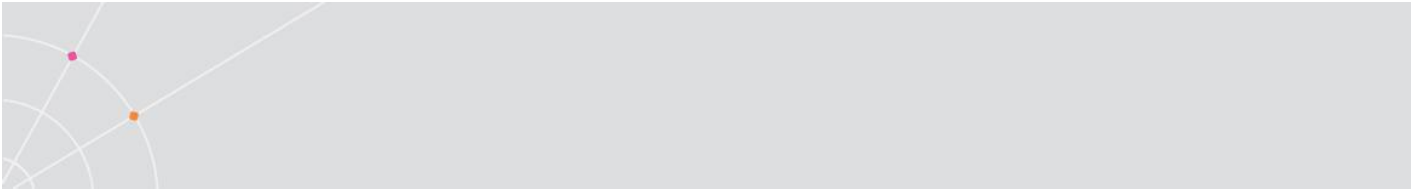
5.3.4. Adding a User to a Group and Setting its Default Group

Every user must belong to at least one group. Users inherit general properties, most significantly connections, from all the groups to which they belong. Users optionally inherit properties from their default group, unless they have these properties explicitly defined. For more details on general properties and optionally inherited properties, see the relevant sections in chapter 5.3.1.

> 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 5.5.1).

To affiliate Users with Groups:

In the User Properties dialog

1. Select the desired user and right-click Properties or select Action | Properties. The User Properties dialog appears.

2. Select the desired group that the user will be affiliated with and click the right-arrow.

3. Click OK.

In the Group Properties dialog

1. Select the desired group and right-click Properties or select Action | Properties. The Group Properties dialog appears.

2. 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.

3. The desired member(s) appear in the Group User's list.

4. Click OK.

To remove Users from Groups:

In the User Properties dialog

1. Select the desired user and right-click Properties or select Action | Properties.

2. Select the desired group from which the user will be disaffiliated, and click the left-arrow.

3. Click OK.

In the Group Properties dialog

1. Select the desired member to be excluded from this group from the Group's Users list.

2. Click the left-arrow. The desired member appears in the Available Users list.

3. Click OK.

To set a default group for a user:

1. Select the desired user and right-click Properties or select Action | Properties. The User Properties dialog appears.

2. Double-click on the group that you want to be the default group. An arrow appears adjacent to the selected group signifying default group.

NOTE   Double-click to clear the default designation.

5.3.5. Customizing the User's Client Settings

Defined terminal and communication settings for a user are saved in a setup file. These settings can be modified at any subsequent time.

To change the user's client settings:

1. Select the desired user and right-click Properties or select Action | Properties.

2. Click the Settings button. The Settings dialog is displayed.

3. Make the necessary modifications.

4. Click OK to close the Settings dialog.

5. Click OK. The new modifications take effect.

> NOTE If you do not set client settings at the user level (using the above procedure),
> they are inherited from the user's default group. If they are not defined there, the
> default settings of the server are used.

5.3.6. Viewing User Sessions, Properties, and Status

You can choose to view on your system the general information of all the:

- Sessions

- Sessions of a user

- Sessions of a group

This general information includes User ID, associated Group, operating system, security and I/O information.

To view all current client sessions:

Select View | Client Sessions or select the desired user and click .

To view current status for multiple users:

Place the cursor anywhere in the Users pane and right-click Columns | Runtime information.

5.3.7. Testing a User

The Administration Tool allows you to connect as a user, and test the access options, client settings and available connections.

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.
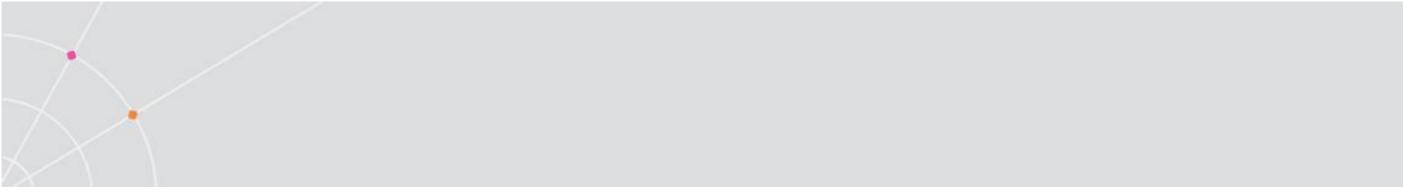
To test the user's capabilities:

1. Select the desired user and right-click Test. The Login dialog appears.

2. Type in the Password, if required.

3. Select Reconnect Mode, if required.

4. Click Login. The PowerTerm emulation appears and connects to the desired host.

5.4. Defining Groups

In general, you should define a group object for each group of users that have similar access needs. You can also use groups to create a logical division of your users, or to prepare for future access needs.

The following sections explain:
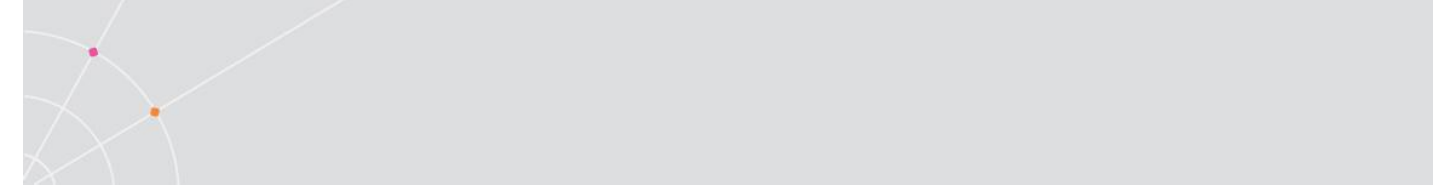
- Group object properties, which define group membership, connections, and allowed access methods for users who do not have them explicitly defined (chapter 5.4.1).

- Default group objects supplied with the Administration Tool, and how they are used (chapter 5.4.3).

- How to create, modify, delete, and disable group objects (chapter 5.4.2).

- How to customize client settings, for group members who do not have them explicitly defined (chapter 5.4).

- How to monitor group properties and runtime information (chapter 5.4).

5.4.1. Group Object Properties (and how they are inherited)

The group object has properties that define group membership, linked connections and allowed access methods for users. These properties can be defined explicitly using the Add Group / Group Properties dialog, or inherited from the "master group" – the server object.

To better understand how groups inherit properties from the server and from other objects, we have divided them into three types:

- Standalone properties: These are properties that are defined at the group level (using the Add Group or Group Properties dialog), and cannot be inherited from the "master group" – the server. An example is the Group Name property, which is always group-specific.

- Shared properties: These are properties that refer to more than one object at a time. When you change them for a group object (using the Add Group or Group Properties dialog), the properties change for the other object/s as well, and vice versa. For example, the Group's Connections property defines which connections

are attached to the group object. When you add a connection, the Owner property in the connection object changes. If you add a group as the Owner of a connection object (using the Add Connection or Connection Properties dialog), the whole group's Group's Connections property changes.

- Optionally inherited properties: These are properties that can be defined at the group level, as well as 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.

In principle, all of a group's properties are passed on to users, unless they are explicitly defined in the individual user objects. For more details on how users inherit options from groups, and directly from the server, see chapter 5.3.1.

The following section explains the Add Group / Group Properties dialog, which is used to explicitly define group properties. The following sections list and detail shared and optionally-inherited group properties.

Using the Add Group / Group Properties Dialog

The Group Properties dialog (called the Add Group dialog when creating a new group) has several main components:

- Group properties fields: These fields take up much of the dialog, and allow you to define a new group object's properties, or view and modify the properties of an existing group. The following sections illustrate which of these are shared and optionally-inherited, and explains them.

- Environment variables table: This table allows you to create and edit free-text variables that have numerous uses, including customization of emulation client appearance and behavior (see chapter 8.2). Environment variables that are added here are defined on the group level.

- Settings button: Launches the Settings dialog, which allows you to customize emulation client appearance and behavior (see chapter 8.1). Client settings modified here are defined on the group level, and are inherited by users who do not have client settings explicitly defined.

- Memo button: Opens a text file to enable you to conveniently type a memo and save it.

- Sessions button: Shows information for client sessions opened by this group's users.

- Up and down arrows: Clicking these arrow switches to the previous (up) or next (down) group, as sorted in the Groups pane. You will be prompted to save changes if you have made any.

> NOTE   The arrows are not displayed in the Add Group dialog when you create a new group.

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

Standalone Properties

Standalone properties are properties that are defined at the group level (using the Add Group or Group Properties dialog), and cannot be inherited from the server. In other words, they are user-specific.

Property	Description
Group Name	Stipulates the name of the group.
Alias	Stipulates the name of the group that is familiar to the members of the organization.
Enabled	Specifies whether to make the group active.
Highest Reconnect Mode	Specifies the rule according to which the user is allowed to automatically reconnect to the PowerTerm WebConnect server, which has undergone unintentional communication interruptions. This is only applicable when the Highest Reconnect Mode of the User is not explicitly specified (<Default> is

	used).
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 which can be separated by a semi colon.
Access Limit Mode	Specifies the rule according to which the user is allowed to access the PowerTerm WebConnect server.
	Unlimited, access from any computer.
	User, access from a computer specified in Allow Access From.
	Group, access from a computer specified in a User's group.
	Both, access according to both the User and Group rules.
Memo	Opens a text file to enter a memo.

Shared Properties

Shared properties refer to more than one object at a time. When you change them for a group object (using the Add Group or Group Properties dialog), they change for the other object/s as well, and vice versa. When you change these properties in other objects, they change for the respective group object.

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. Every user you add here has this group added under User's Groups in the user object. The opposite is also true: If you use the User Properties dialog to add a user to this group, the user will be added here.

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. For every connection you add here, the group is added as the Owner in the connection object. The opposite is also true: If you set this group as a connection's Owner (using the Connection Properties dialog), the connection is added here.

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 that allows you to customize client settings for this group's users (see chapter 8).	If you do not define any client settings using this button, all client settings are 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	Enter '0' to inherit this property value from the server object's Default Sessions property.
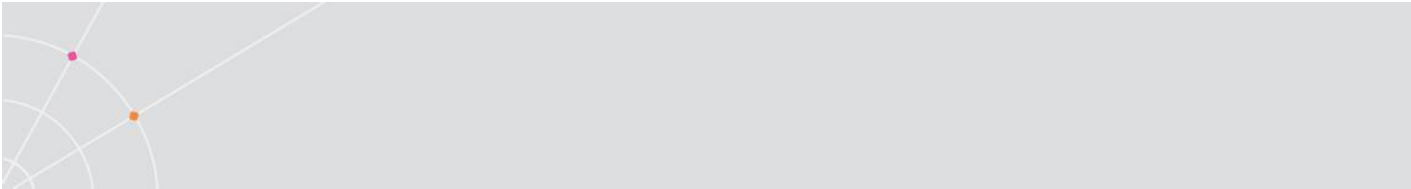
	concurrent connections) in the User's default group. If this value is also '0', then the program uses the default value in the MaxUserQuota field located in the [Server] section of the PtServer.ini file. Other values will override the default value.	
Max. LPD Queues	Stipulates maximum number of LPD queues 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, including customization of emulation client appearance and behavior (see chapter 8.2). 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.

5.4.2. Creating, Modifying, Deleting, and Disabling Groups

Even after you have created a group object, you can still make changes to all its properties.

You can also delete or disable a group object. Both these actions have the effect of preventing all the users who have the group as default, from accessing the server, until another default group is assigned to them. If you intend to use a group object again in

the future, it is preferable to disable rather than delete it. If users that belong to the disabled group need access to a host, you can enable that group again.

NOTE   If a group is disabled, all its users are effectively disabled. However, if a user is specifically disabled, the user remains disabled even if the group is enabled.

To create a new group from scratch:

1. Select Action | New | Group. The New Group dialog appears.

2. Fill out all of the necessary fields.

3. Click OK. The new group has been created and appears in the Group pane.

To create a new group based on an existing group:

1. Select a group that you want to use as your model and right-click Copy. The Copy Group 'groupname' dialog appears.

2. Type in a new group name.

3. Click OK. The new group has been created while its Group Properties dialog appears.

4. Make the necessary modifications.

5. Click OK. The new group appears with its own unique properties in the Group pane.

To modify properties for an existing group:

1. Select a group to which you want to modify its properties and right-click Properties. The Group Properties dialog appears.

2. Make the necessary modifications.

3. Click OK. The new group appears with its modifications.

To delete a group:

1. Select a group that you want to delete and right-click Delete. A confirmation notice is displayed.

2. Click OK. The selected group is deleted.

To disable a group:

1. Select a group that you want to disable and right-click Properties. The Group Properties dialog appears.

2. Clear the Enable checkbox.

3. Click OK. The selected group is disabled.

> NOTE   This has the effect of disabling all the users who have this group set as the default group (see chapter 5.4.3).

To enable a group again after disabling it:

1. Select the disabled group and right-click Properties. The Group Properties dialog appears.

2. Select the Enable checkbox.

3. Click OK. The selected group is enabled.

5.4.3. Using Default Group Objects

Several default group objects are predefined in the PowerTerm WebConnect server. These groups are supplied strictly as an example. You are free to change their names or create additional groups as you wish, according to the particular needs of your organization.

The default groups have increasingly more privileges as you go down the list (Novice Users<Advanced Users<Expert Users<Super Users).

5.4.4. Customizing Client Settings for Group Users

When you set client settings for the group, the settings are used for all the group's users, unless they have client settings explicitly defined. You can set a user's client settings explicitly using the user object's Settings dialog.
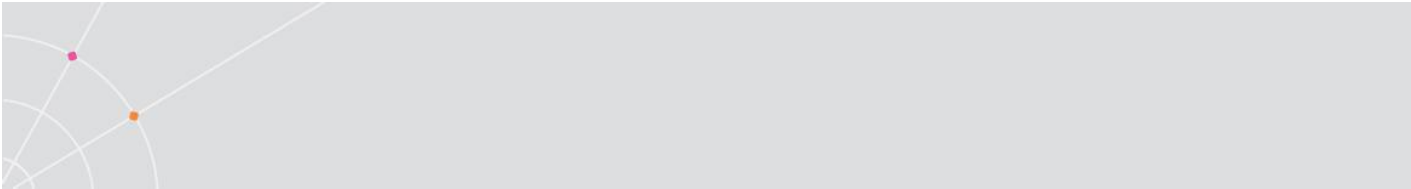
To change client settings for the group object:

1. Right-click Properties on the desired group. The Group Properties dialog is displayed.

2. Click the Settings button.

3. Modify the client settings, as required.

4. Click Save / Save All. The Settings of group 'groupname' window is displayed.

> NOTE   If you do not specify client settings at the group level (using the above procedure), the group inherits the system defaults.

5.4.5. Viewing Group Sessions, Properties, and Status

You can choose to view the general information, properties and status of a particular group's sessions on your system.

This general information includes User ID, associated Group, operating system, security and I/O information.

To view the sessions currently open by a group's users:

1. Right-click Properties on the desired group. The Group Properties dialog is displayed.

2. Click the Sessions button.

OR

Right-click Sessions on the desired group. The Sessions widow is displayed.

To view properties for multiple groups:

Right-click Definition Information in the Groups pane.

To view current status for multiple users:

Right-click Runtime Information in the Groups pane.

5.5. Defining the "Master group" – the Server

The server object functions as a "master group" from which groups and users inherit properties, unless these properties are explicitly defined at the group and user levels. From another perspective, the server object's settings are the system defaults, which apply to all users unless you specify otherwise.

5.5.1. 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
Default Reconnect	Specifies the rule	Optionally-inherited

Mode	according to which the user is allowed to reconnect to the PowerTerm WebConnect server. It is applicable only when both the User's and Group's reconnect mode value is Default.	
Max. Sessions	Specifies the maximum number of concurrent sessions that a user can open	General
Default Sessions	Specifies the default number of concurrent sessions that a user can open.	Optionally-inherited. Groups with Max. Concurrent Sessions set to '0', inherit this value.
Max LPD Queues	Specifies the maximum number of registered LPD queues that a user can define.	General
Default LPD Queues	Specifies the default LPD quota, used when '0' is specified at the user and Group level.	Optionally-inherited. Groups with Max. LPD Queues set to '0', inherit this value.
Administrator Auto Refresh Freq.	Specifies the interval in which the Administration Tool's AutoRefresh 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 locked out for a	General

	specific 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	Specifies the default group for all the users.	Optionally-inherited. Users who do not have a default group selected acquire this group as their default group.
Background Bitmap File	Sets a background bitmap for clients that support this feature.	General
Server's Connections	Specifies the connections to be used by the server.	General. All users can access the server's connections. If Server is stipulated as the connection's Owner (in the Connection Properties dialog), then here it will be reflected as a Server's Connection.
Environmental Variables	Specifies variable names and associated values. These PowerTerm WebConnect 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. Environment variables that are defined in a group or user object are not inherited.

5.5.2. Customizing Default Client Settings

If settings are not set for a user or one's default group, then the settings of the server will be applied by default.

To change the default client settings:

Select Server | Default Settings.

> NOTE   If you set client settings at the group or user level, they override these settings for those groups or users.

5.5.3. Receiving a File from the Server

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

To receive a file from the server:

1. Select Files | Get File. The Get File dialog appears.
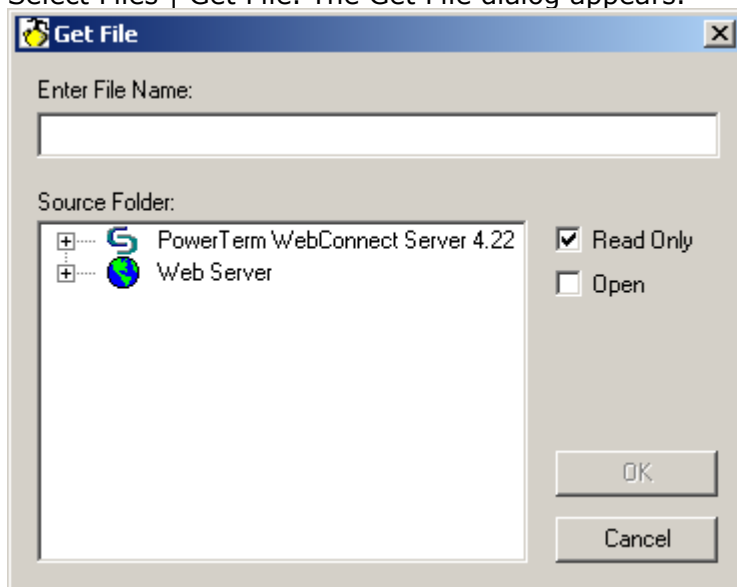
2. Browse the Folders for the desired file.

3. Check Read Only if you want the local copy to have the Read Only attribute.

4. Check Open if you want the local copy to be opened by its associated application when it's received.

5. Click OK. The file is copied from the server.

Copied files are placed into a temporary folder under your Application Data folder in the Ericom/ptadmin subdirectory. If you do not check the Open option, you will be offered to open Windows Explorer on that folder.

5.5.4. Sending Files to the Server

Enables easy transferring of files from your computer (the computer on which the Administration Tool is running) to the WebConnect server.

To send files to the server:

1. Select Files | Put Files. The standard Select Files to Put on Server dialog appears.
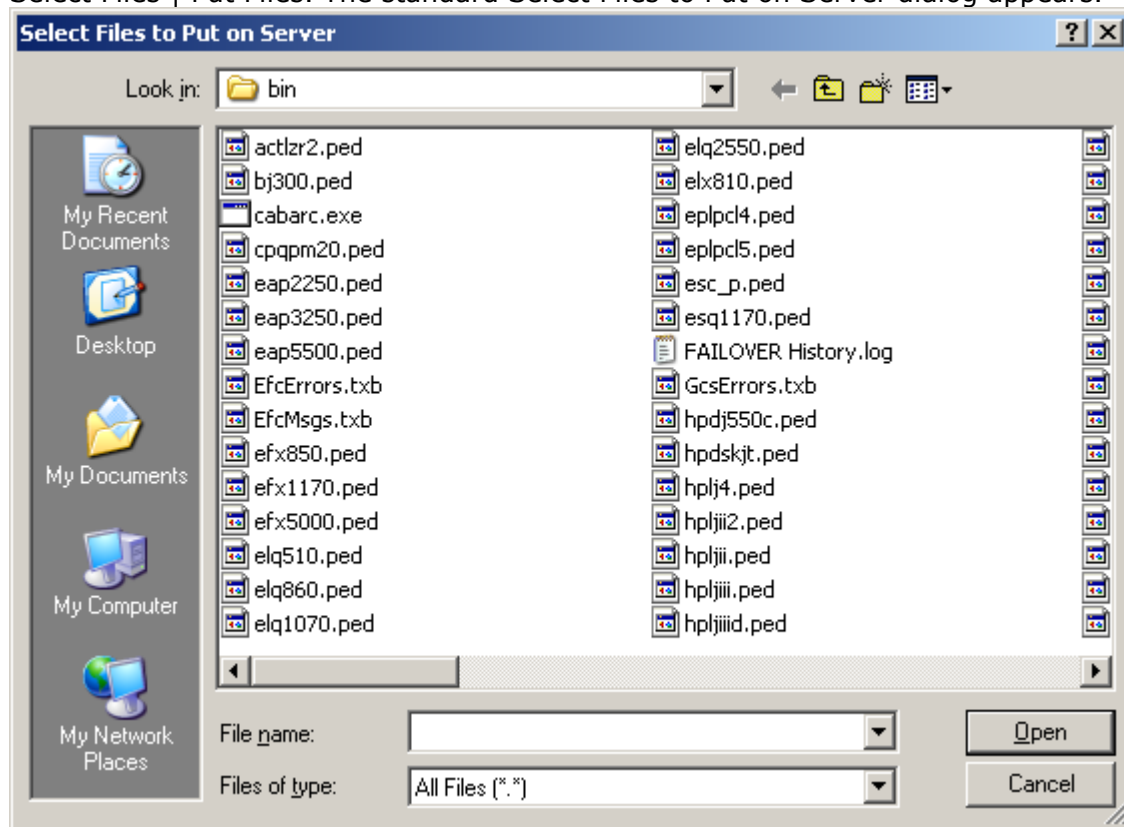
2. Select one or more files and click Open. The Put Files dialog appears.
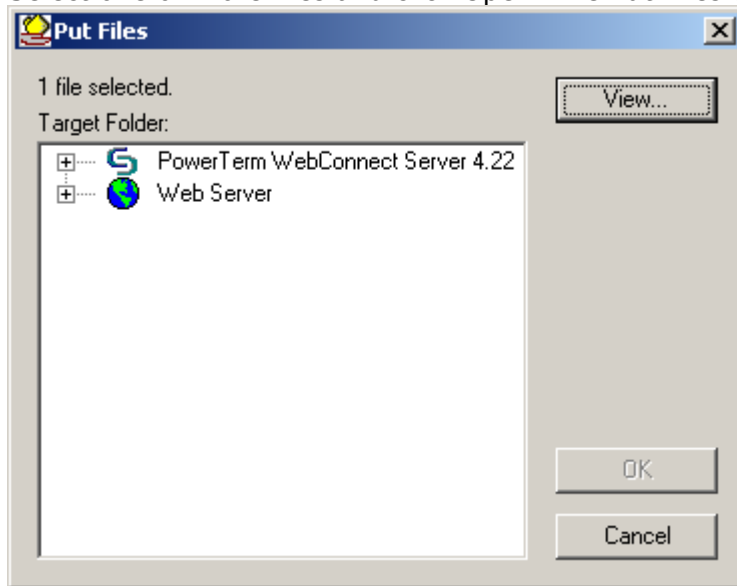
3. Select the target folder on the server for the file(s) destination.
4. Click OK. The files are transferred to the server.

6. Defining Connections

Connection is the manner in which users can run a remote application or connect to a host server (much like "Dial-Up Networking" in Windows, which allows you to connect to your ISP with certain predefined settings).

A host connection specifies the host type and the protocol used to connect to it, and allows you to set communication options specific to that protocol. Depending on the client used for the connection, a connection object can also define the behavior and look-and-feel of the client. For example, for the PowerTerm WebConnect HostView emulation client, connection properties control the behavior of the Power Pad (a floating panel of special definable function buttons) and map keys on the user's keyboard to terminal keys or to script commands.

Some examples of default connection objects are supplied with the PowerTerm WebConnect server:

- Example_VT: This represents a VT420-7 Terminal type operating over a Telnet connection.

- Example_As400: This represents an IBM 5250 Terminal type operating over a TN5250 connection.

- Localhost

Affiliating Connections to Other Objects
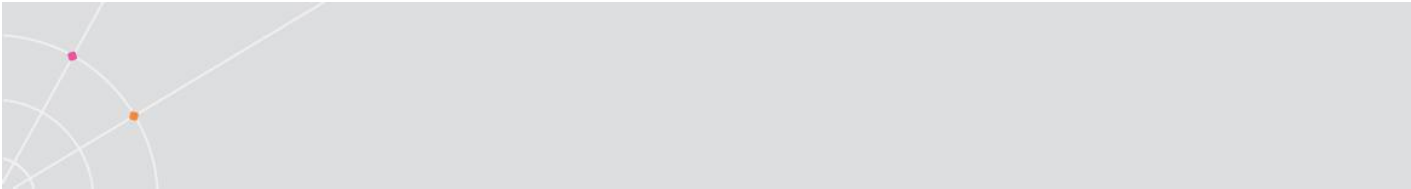
In order to be used, a connection must be affiliated to another object. This object becomes the connection's owner. A connection can only be owned by one object at a time, so a connection intended for multiple users should be affiliated to a group, which contains those users. If you create a connection for one specific user, you can affiliate the connection to that user's object. No other users will be able to use it.

> NOTE   A connection can be affiliated with the "master group", i.e. the entire server. In such a case, all the users will be able to use the connection.

A connection can also be owned by another connection, which becomes its parent connection. This means that when the parent connection is executed, the child connection is launched automatically. Child connections do not inherit settings from the parent connection.

Application Publishing

PowerTerm WebConnect enables an integrated solution for both legacy systems and access to remote applications on Terminal Servers. It publishes remote applications and content for access by any authorized user or group and providing users with easy access

to their applications. These are viewed in True Seamless Windows™, where the remote applications are fully integrated into the local desktop, and so local and remote application look and behave identically.

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

NOTE   The Applicaton Zone shortcut format is **<OrganizationName> PowerTerm Application Zone by Ericom**. If there are more then 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 PtServer.ini **OrganizationName** variable.

The published application can be a legacy application, document or URL.

PowerTerm WebConnect Application Zone and Application Portal allows for:

- Request administrator help via PowerTerm WebConnect QuickVNC

- Download large software components expediently

- Technical support including non-PowerTerm WebConnect assistance needs.

- Run PowerTerm WebConnect PrintView client

- Run PowerTerm Secure FTP client

- Run PowerTerm AS/400 Data File Transfer

6.1. Defining Host Connections

In order to allow PowerTerm WebConnect users to connect to a specific host, you must define one or more connection objects that target that host.

6.1.1. Connection Object Properties

The Connection Properties dialog allows you to change the connection options for an existing connection object, or to create a new connection object (in such a case it is called the Add Connection dialog). It also allows you to edit various settings that control the client's appearance and behavior. Unlike the User, Group and Server entities the connection object has only the following types of properties:

Standalone Properties

Standalone properties are properties that are only defined at the connection level (using the Connection Properties dialog), and cannot be inherited from the server. In other words, they are connection-specific.

Using the Add Connection/Connection Properties Dialog

- Connection properties fields: These fields allow you to define a new connection object's properties, or view and modify the properties of an existing connection object.

- Settings button: Displays the Emulation Settings dialog, which allows you to customize emulation client appearance and behavior (see chapter 8.2).

- Details button: Only visible for RDP connections. Allows you to customize the PowerTerm WebConnect RemoteView client's appearance and behavior. For example, it lets you choose between window and Seamless modes.

- Key Mapping button: Enables you to map the emulation Keyboard (see chapter 8.1.3).

- Power Pad button: Allows you to define Power Pad and Function buttons displayed by the emulation client (see chapter 8.1.4 and 8.1.5).

- Login Script: Opens a text window to edit scripts to be run after communication is established by an emulation client. To learn how to edit a PSL scripts, see the PowerTerm PSL Reference.

- Memo button: Opens a text file that enables you to type and save free-form information about the connection.

- Publishing button:

- Help button: Displays the online help file.

- Up and down arrows: Clicking these arrows switches to the previous (up) or next (down) group, as sorted in the Groups pane. You will be prompted to save any changes, if made.

> NOTE   The arrows are not displayed in the Add Connection dialog when you create a new connection.

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

6.1.2. Creating, Modifying, Deleting, and Disabling Host Connections

Once you create a connection object, you can make changes to all its properties.

You can also delete or disable a connection. Both these actions have the effect of preventing the user from accessing the server using this connection. If you intend to use a connection object again in the future, disable it instead of deleting it. When you need it again, you can enable it.

> NOTE   If a parent connection is disabled, its child connection will effectively be disabled as well because users cannot access it directly. (A child connection is a connection that has another connection as its owner. See the introduction above.)

To create a connection from scratch:

1. Select Action | New | Host Connection. The New Connection dialog appears.

2. Fill in all of the necessary fields.

3. Click OK. The new connection has been created and appears in the Connection pane.

To create a connection based on an existing one:

1. Select a Connection, which you want to use as your model and right-click Copy. The Copy Connection 'connectionname' dialog appears.

2. Type in a new Connection Name.

3. Click OK. The new connection has been created while its Connection Properties dialog appears.

4. Make the necessary modifications.

5. Click OK. The new connection appears with its own unique properties in the Connection pane.

NOTE   A copied connection is initially disabled. Only after the connection has been modified it will be made available.

To modify connection properties:

1. Select a Connection that you want to modify and right-click Properties. The Connection Properties dialog appears.

2. Make the necessary modifications.

3. Click OK. The connection's properties are modified.

To delete a connection:

1. Select a Connection that you want to delete and right-click Delete. A confirmation message appears.

2. Click OK. The connection is deleted.

To disable a connection:

1. Select a Connection that you want to disable and right-click Properties. The Connection Properties dialog appears.

2. Clear the Enabled checkbox.

3. Click OK. The connection is disabled.

To enable a connection again after disabling it:

1. Select a Connection that you want to enable and right-click Properties. The Connection Properties dialog appears.

2. Select the Enabled checkbox.

3. Click OK. The connection is enabled.

> NOTE   If the connection is a child connection (i.e. its owner is another connection), enabling will only take affect if the parent connection is also enabled.

6.1.3. Customizing the Host Connection Settings

Defined connection and communication settings for a user are saved in a setup file. These can be modified at any time.

To change the connection settings:

1. Select the desired connection and right-click Properties or select Action | Properties. The Connection Properties dialog is displayed.

2. Make the necessary modifications.

3. Click OK. The new modifications take effect.

6.1.4. Viewing Host Connection Properties and Status

You can choose to view the general information, properties and status of a particular connection on your system.

This general information includes Target, Network, Terminal Type, Terminal Model, Comm Type and Security.

To view an active connection:

Right-click Properties on the desired connection, then click the Sessions button.

OR

Select the desired connection and select Action | Properties.

The Connection Properties dialog is displayed.

To view the definition information for all the connections:

Right-click Definition Information in the Groups pane.

To view current status for all the connections:

Right-click Runtime Information in the Connection pane.

6.1.5. Testing Host Connections

The Administration Tool allows you to test the settings of a connection by using it to access the host yourself.

While you can view all the connection's settings using the Connections pane, it is recommended that you test the connection yourself, either immediately after creating a connection object, after making changes to a connection, or in response to a user's request or complaint.

To test a connection:

1. Select a connection in the Connections pane and right-click Test. The Login dialog appears.

2. Provide the necessary Password and click OK. The desired host access client will be launched.

NOTE   Testing a connection that has a login script will also invoke that script. As a result, you will be able to view and validate the automatic interaction between the client and the host.

6.2. Published Application Configuration
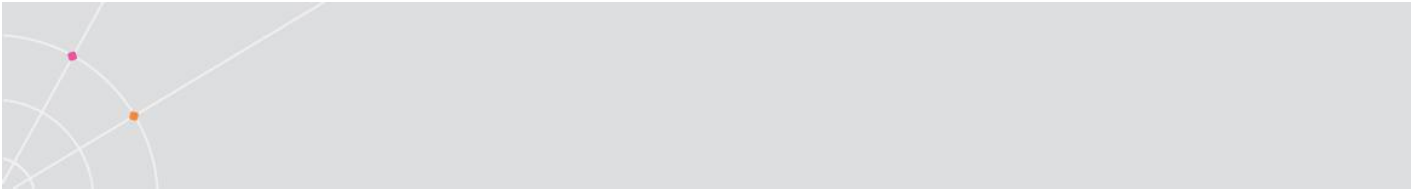
You can easily publish applications with the PowerTerm WebConnect Application Publishing Wizard. This wizard will guide you step by step through the configuration procedure as explained further down. The parameters you enter will automatically be saved in the wizard for the next time you will publish an application.

NOTE   If you prefer not to save last entered data in the wizard, set the Environment Variable **ADMIN_SavePublishSetting** to **0**. (Read more about Environment Variables in chapter 8.2.)

The PowerTerm WebConnect Application Publishing wizard requires Ericom Remote Browser to be installed over the designated Terminal Server/local host before publishing an application. This Remote Browser is a service over the remote machine passing the browsed files display names, icons, and link parameter which is the base of the Published Application connection. When publishing a local application the Administration Tool will download and execute a local browser which will be terminated once the Administrator exits the publishing wizard.

Application Publishing and the Load Balancer

PowerTerm WebConnect Application Publishing can be configured so that the selected applications may run on any Terminal Server. Alternatively, the administrator can select

which servers participate from a list that displays all the Terminal Servers known to the PowerTerm Load Balancer.

In the first case, i.e. using all available servers connected to the Load Balancer, the addition of a new server will automatically be used by the Load Balancer to find the selected applications as well.

NOTE You can copy and delete connections, including connections that are linked to PowerTerm Load Balancer, even if PowerTerm Load Balancer is not available (i.e. the PowerTerm Load Balancer is down or locked). However, in that case, the PowerTerm Load Balancer configuration file will not be updated. This does not affect the copied/deleted connection but it does collect unnecessary data in the PowerTerm Load Balancer configuration file which can cause future discrepancies.

While the PowerTerm Load Balancer server is not available, the user will not be able to update connections that were created with PowerTerm Load Balancer. However, copy and delete options are enabled.

NOTE When an administrator ("the first") connects to Publishing Application Wizard, PowerTerm WebConnect checks if there is a connection to PowerTerm Load Balancer Server. Any other administrator ("the second", "the third", etc.) that wants to use Publishing Application Wizard, will get the same status of PowerTerm Load Balancer Server as the first administrator got, as long as any administrator is still in the Published Application Wizard.

If PowerTerm Load Balancer is not attached, the administrator must explicitly provide the address of the server and the port to use. By default the port number is 3389 (RDP port).

To publish a Windows application:

1. Select **Action | New | Windows Application**. The **Application Publisher Step 1** dialog appears.

2. Determine **What to Publish**, where to publish it from and click **Next**. The **Application Publisher Step 2** dialog appears.

3. Determine the application that you want to publish. Either browse or designate any legal value from the Start button's Run dialog i.e. `C:\Windows\notepad.exe`. Upon selecting the browse button, you will be prompted to confirm the **Terminal Server's IP** address and **Port number**.

4. Override, if necessary the **Working Directory** (the preferred folder from where to run the application.).

NOTE This field does not necessarily have content.
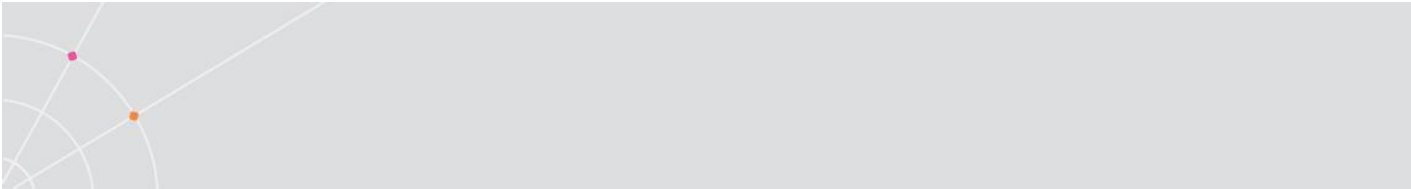
5. Provide **Parameters** if necessary.
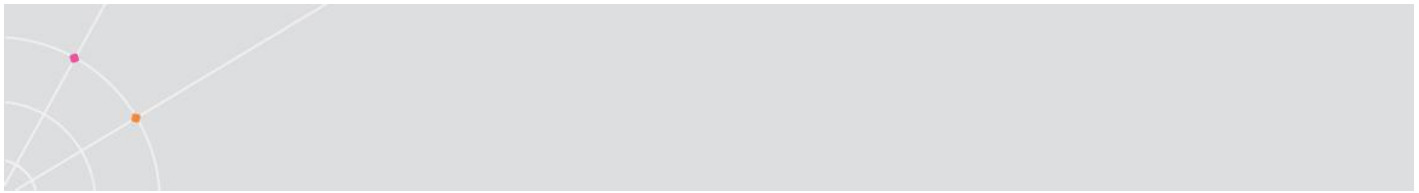
6. Type the **Display Name** which will appear in the list of **Connections** and click **Next**. The **Application Publisher Step 3** dialog appears.

7. Determine the shortcut location of published application in **Publish to**.

8. Click **Choose Icon**. The **Change Icon** dialog appears.

9. Select the desired icon and click **OK**. The icon appears adjacent to the Choose Icon button. You can also browse to a different folder if you prefer another icon selection.

10. Click **Next**. The **Application Publisher Step 4** dialog appears.

11. Determine the **Color Quality** of your published application.

12. Determine the mode in which you want to run the published application and click **Next**. The **Application Publisher Step 5** dialog appears.

13. Choose the connection speed in order to achieve maximal optimization.
This will automatically determine the optimization settings which you may override by selecting one of the 3 settings. If necessary, modify these settings.

14. Determine whether you prefer the window to be dragged with or without the content and click **Next**. The **Application Publisher Step 6** dialog appears.

15. Determine the **Remote Computer Sound**.

16. Determine which local devices you want to automatically connect to when logged on to the remote computer and click **Next**. The **Application Publisher Step 7** dialog appears.

17. If you have **PowerTerm Load Balancer** installed:
Use all Servers (default) will enable the application to run on any Terminal Server. Alternatively, you can select from a list which servers will be included in the Load Balancer Terminal Server pool from a list that displays all the Terminal Servers known to the Load Balancer.
Selecting **Use all Servers** will add the application to Load Balancer with no server specified. If you add a new server, it will be included in the Load Balancer pool of available servers. If **Specify the Servers** is selected, only selected servers will be included in the pool.
Selecting **Show only servers with this application** will clear both lists and will display only the available servers where the application is installed.

If you do not have PowerTerm Load Balancer installed:
Stipulate the **Server Address** and **Port Number** through which the Application Publishing will take place.

If you selected to publish from a **Virtual Desktop**:
Select **Pool** to use for this application.

18. Click **Next**. The **Application Publisher Step 8** dialog appears.

19. Select those **Owner(s)** (users) which will be able to view the published application and click **Next**. The **Application Publisher Step 9** dialog appears.

NOTE   Selecting **Show Users** will display all the current WebConnect Users.

20. Click **Advanced Settings** to modify any of the **Credentials**, **Domain**, **Network Name**, and **Environment Variables** or enable/disable this application and click **OK**.

21. Click **Finish**. The published application appears in the **Connection List**.

NOTE   Right-click **Properties** or double click on the published application to modify any of the settings which you previously defined.

To publish multiple Windows applications:

1. Select **Action | New | Multiple Windows Applications**. The **Choose Terminal Server for Browsing** dialog appears.

2. Provide the **Server Address** and **Port Number** of the Terminal Server which will be used for browsing and click **OK**. The **Application Publisher Step 1** dialog appears.

3. Select those applications found in the programs folder of the designated target that you want to publish and click **Next**. The **Application Publisher Step 2** dialog appears.

4. Determine the destination of your publishing and click **Next**. The **Application Publisher Step 3** dialog appears.

5. Determine the **Color Quality** of your published application.

6. Determine the mode in which you want to run the published application and click **Next**. The **Application Publisher Step 4** dialog appears.

7. Choose the connection speed in order to achieve maximal optimization. This will automatically determine the optimization settings which you may override by selecting one of the 3 settings. If necessary, modify these settings.

8. Determine whether you prefer the window to be dragged with or without its content and click **Next**. The **Application Publisher Step 5** dialog appears.

9. Determine the **Remote Computer Sound**.

10. Determine which local devices you want to automatically connect to when logged on to the remote computer and click **Next**. The **Application Publisher Step 6** dialog appears.

11. If you have **PowerTerm Load Balancer** installed:
    Use all Servers (default) will enable the application to run on any Terminal Server. Alternatively, you can select from a list which servers will be included in the Load Balancer Terminal Server pool from a list that displays all the Terminal Servers known

to the Load Balancer.

Selecting **Use all Servers** will add the application to Load Balancer with no server specified. If you add a new server, it will be included in the Load Balancer pool of available servers. If **Specify the Servers** is selected, only selected servers will be included in the pool.

Selecting **Show only servers with this application** will clear both lists and will display only the available servers where the application is installed.

If you do not have PowerTerm Load Balancer installed:
Stipulate the **Server Address** and **Port Number** through which the Application Publishing will take place.

12. Click **Next**. The **Application Publisher Step 7** dialog appears.

13. Select those **Owner(s)** (users which will be able to view the published application) and click **Next**. The **Application Publisher Step 8** dialog appears.

NOTE Selecting Show Users will display all the current WebConnect Users.

14. Click **Advanced Settings** to modify any of the **Credentials**, **Domain**, **Network Name**, and **Environment Variables** or enable/disable this application and click **OK**.

15. Click **Finish**. The published application appears in the **Connection List**.

NOTE Right-click **Properties** or double click on the published application to modify any of the settings which you previously defined.

To publish an application for a Remote Desktop:

1. Select **Action | New | Remote Desktop**. The **Application Publisher Step 1** dialog appears.

2. Type the **Display Name** which will appear in the list of **Connections** and click **Next**. The **Application Publisher Step 2** dialog appears.

3. Determine the shortcut location.

4. Click **Choose Icon** if desired. The **Change Icon** dialog appears.

5. Select the desired icon and click **OK**. The icon appears adjacent to the **Choose Icon** button. You can also browse to a different folder if you prefer another icon selection.

6. Click **Next**. The **Application Publisher Step 3** dialog appears.

7. Determine **Screen Size** and the **Color Quality** of your published application.

8. Select, if desirable, **Show Connection Bar in Full Screen Mode**.

9. Click **Next**. The **Application Publisher Step 4** dialog appears.
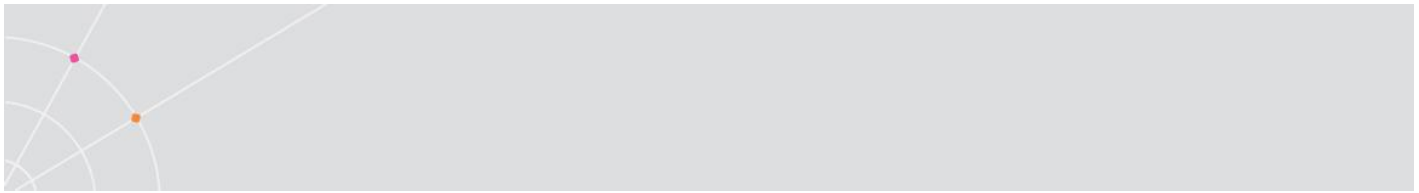
10. Select the connection speed in order to achieve maximal optimization. This will automatically determine the optimization settings which you may override by selecting one of the 3 settings. If necessary, modify these settings.

11. Determine whether you prefer the window to be dragged with or without its content.

12. Click **Next**. The **Application Publisher Step 5** dialog appears.

13. Determine the **Remote Computer Sound**, **Where to Apply Window Key Combinations** and which local devices you want to automatically connect to when logged on to the remote computer.

14. Click **Next**. The **Application Publisher Step 6** dialog appears.

15. If you have **PowerTerm Load Balancer** installed:
    Use all Servers (default) will enable the application to run on any Terminal Server. Alternatively, you can select from a list which servers will be included in the Load Balancer Terminal Server pool from a list that displays all the Terminal Servers known to the Load Balancer.
    Selecting **Use all Servers** will add the application to Load Balancer with no server specified. If you add a new server, it will be included in the Load Balancer pool of available servers. If **Specify the Servers** is selected, only selected servers will be included in the pool.
    Selecting **Show only servers with this application** will clear both lists and will display only the available servers where the application is installed.

    If you do not have PowerTerm Load Balancer installed:
    Stipulate the **Server Address** and **Port Number** through which the Application Publishing will take place.

    If you selected to publish from a **Virtual Desktop**:
    Select **Pool** to use for this application.

16. Click **Next**. The **Application Publisher Step 7** dialog appears.

17. Select the **Owner(s)** (users) which will be able to view the published application) and click **Next**. The **Application Publisher Step 8** dialog appears.

NOTE   Selecting **Show Users** will display all the current WebConnect Users.

18. Click **Advanced Settings** to modify any of the **Credentials**, **Domain, Network Name**, and **Environment Variables** or enable/disable this application and click **OK**.

19. Click **Finish**. The published application appears in the **Connection List**.

NOTE   Right-click **Properties** or double click on the published application to modify any of the settings which you previously defined.

Viewing Application Publishing Properties

You can choose to view the general information, properties and status of a particular Application Publishing on your system.

This general information includes Display Name, type of publication, from where it is published and the source.

To view an active connection:
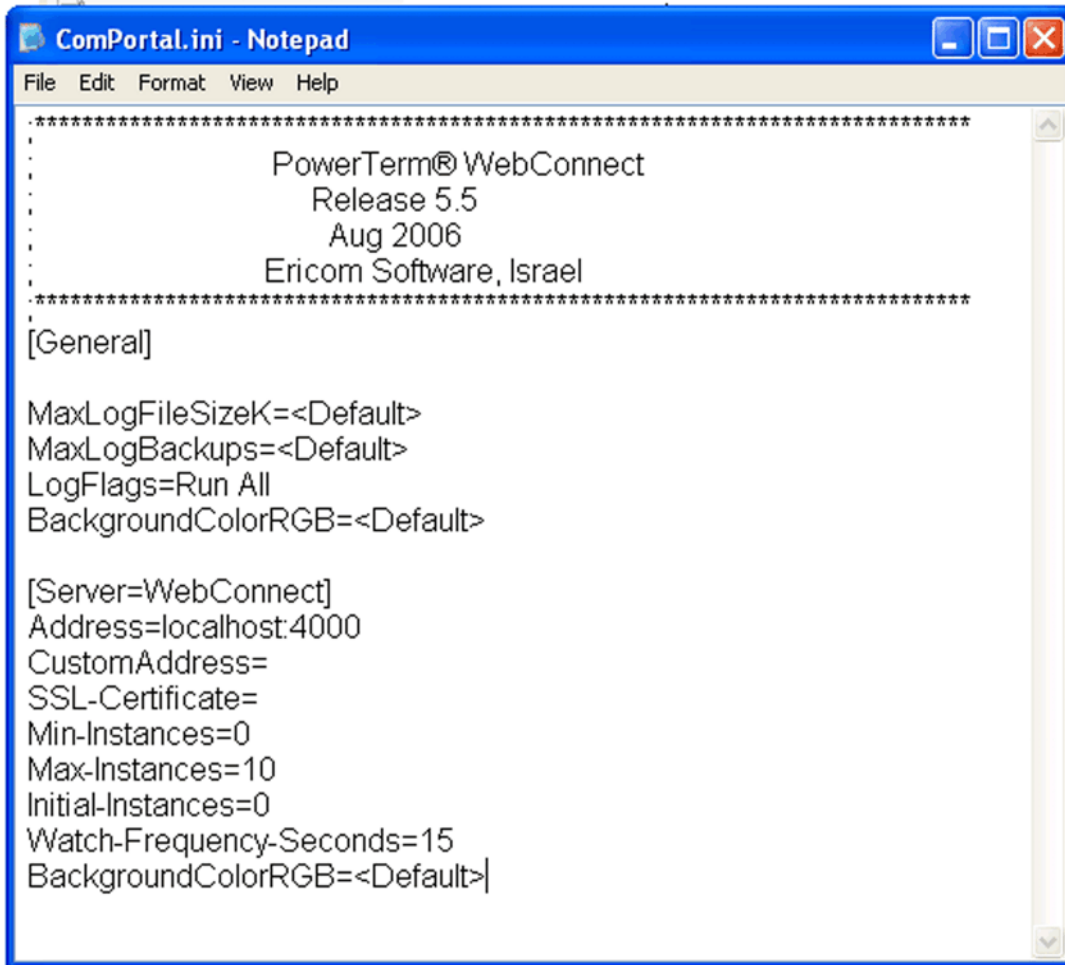
Double-click the desired connection in the Connections view. The Application Properties dialog is displayed.

6.3. PowerTerm WebConnect Application Portal

The WebConnect Application Portal provides a Web based User Interface for published applications from within standard browsers running on Windows and Linux. Published applications can be launched directly from within the browser by means of an ActiveX control or Java applets. (The appropriate method is automatically selected based on the client operating system and browser type.) The PowerTerm WebConnect Application Portal requires Microsoft's Internet Information Server (IIS) version 5 or higher and can be deployed on the same computer as the PowerTerm WebConnect Server or on a separate server.

6.3.1. Application Portal Configuration

As part of the Application Portal installation process, a COM (ActiveX) object called 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 object and additional configuration files, such as, **ComPortal.ini** are installed in the `\WebConnect5.6\ComPortal\` directory on the Web Server. In most cases, the WebConnect Application Portal will function correctly with the default parameters specified in the ComPortal.ini file, as shown below.
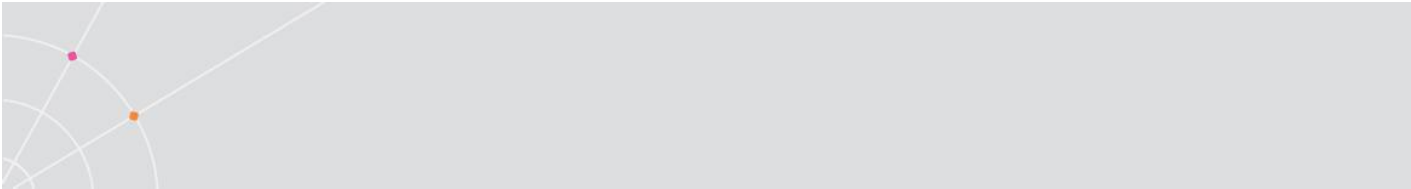
```
ComPortal.ini - Notepad

File  Edit  Format  View  Help

;*********************************************************************
;
;                    PowerTerm® WebConnect
;                        Release 5.5
;                         Aug 2006
;                    Ericom Software, Israel
;*********************************************************************
;
[General]

MaxLogFileSizeK=<Default>
MaxLogBackups=<Default>
LogFlags=Run All
BackgroundColorRGB=<Default>


[Server=WebConnect]
Address=localhost:4000
CustomAddress=
SSL-Certificate=
Min-Instances=0
Max-Instances=10
Initial-Instances=0
Watch-Frequency-Seconds=15
BackgroundColorRGB=<Default>|
```

ComPortal.ini configuration file defining a single WebConnect Server

ComPortal.ini parameters

The PowerTerm WebConnect Application Portal reads the configuration parameters specified in ComPortal.ini during its initialization. The ComPortal.ini file can be edited using a standard text editor, such as, Notepad. However, any changes made to the parameters will not take effect until the ComPortal object is reloaded by the Web Server.

NOTE   Whenever any of the CompPortal.ini parameters are modified, you need to reset the IIS Server by running the IISReset command for the changes to take effect.

The administrator can modify the values of the configuration parameters in order to optimize performance of the PowerTerm WebConnect Server and the Web Server. For example, ComPortal can generate a log file to assist in identifying and correcting problems. Configuration parameters in ComPortal.ini determine which operations will be logged as well as the maximum disk space consumed by the log file. 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—Options are:

- **Run**—general software workflow flags. These options dictate which of the initialization and maintenance events will be reported, such as, whether or not the default WebConnect record will be stored, allocating the pool name, allocating the client pool name, creating the pool watch thread and starting client pools.

   All of the following are services provided by the WebConnect Portal client:
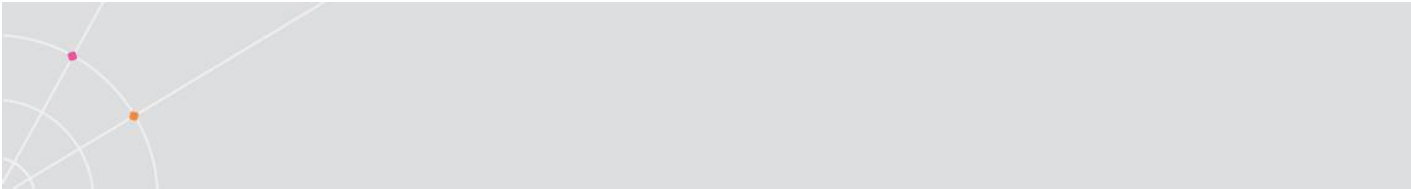
- **Authenticate**.
- **GetConnectionsList**.
- **GetLoginTicket**.
- **AddLoginVariable**.
- **GetServerAddress**.
- **GetPreferenceValue**.
- **SetPreferenceValue**.
- **GetConnectionIcon**.
- **All**—place holder to log all the above services and is equivalent to specifying **Authenticate GetConnectionsList GetLoginTicket** and so on.

   Default is **Run All**.

[Server= ...]—table record

The Server=… section is a single "record" of the Servers table. Each record specifies the properties of a connection to a specific PowerTerm WebConnect server.

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.

It is important to understand that the Portal sessions are stateless and provide services in a "modal" way—each session that is processing a service is busy until the service is completed. This means that 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 generally improve availability, but will also increase the load on the PowerTerm WebConnect Server and also the Web Server.

Address—the address or host name and port of the PowerTerm WebConnect Server to which ComPortal will connect.

> Default is localhost:4000.

CustomAddress—address and TCP port of the PowerTerm WebConnect Server in relation to the Web browser (client). If not specified, then the default IP address of the PowerTerm WebConnect Server will be used. For example, if the value of Address is "localhost" it will be replaced by the server's default IP address.

If the organization has external clients connecting to an internal PowerTerm WebConnect server via Application Portal, then in the sysadmin needs to add the PowerTerm WebConnect Server IP. For example CustomAddress=192.168.71.166

SSL-Certificate—location of the PowerTerm WebConnect Server's SSL certificate, if any. Where available, this certificate will be used to authenticate communication between the Web Server and the PowerTerm WebConnect Server.

> Default is empty which indicates that there is no SSL certificate and server authentication will not take place.

Initial-Instances—number of sessions that will be connected to the PowerTerm WebConnect Server at the time of initialization.
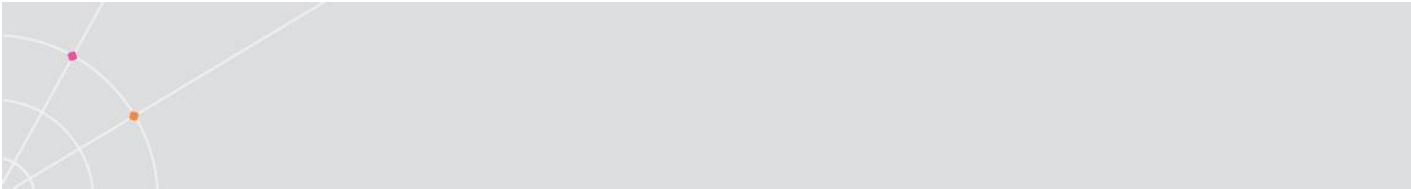
> Default is 0.

Min-Instances—minimum number of sessions that will be generated and which will be 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 to see that there are at least Min-Instances number of sessions connected to the WebConnect server. If for any reason, the number of sessions in the pool is less than Min-Instances, the pool manager will create additional pool sessions.

Default is 15.

There may be more than one [Server=…] record section in order to define more than one PowerTerm WebConnect Servers, depending on the site scenario. Each such record corresponds to a session pool.

6.3.2. The "< Portal >" Special User

At installation of the PowerTerm WebConnect Servers a special user called "< Portal >" is automatically created. This user entity is used for the communication between the Web Server and the PowerTerm WebConnect Server, regardless of the user actually logged into the Application Portal. The "< Portal >" user has special attributes and should not be used to directly log in to PowerTerm WebConnect.
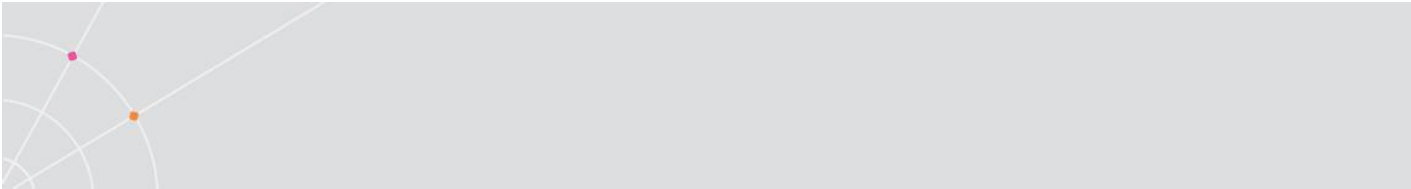
NOTE The "< Portal >" user properties should not be modified nor should the user be deleted.

If this user is deleted either by using the AdminTool or by setting the [Server]UsePortalUser entry to False in the PtServer.ini file, all PowerTerm WebConnect portal clients that are logged on will 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 [Server] UsePortalUser must be set to True.
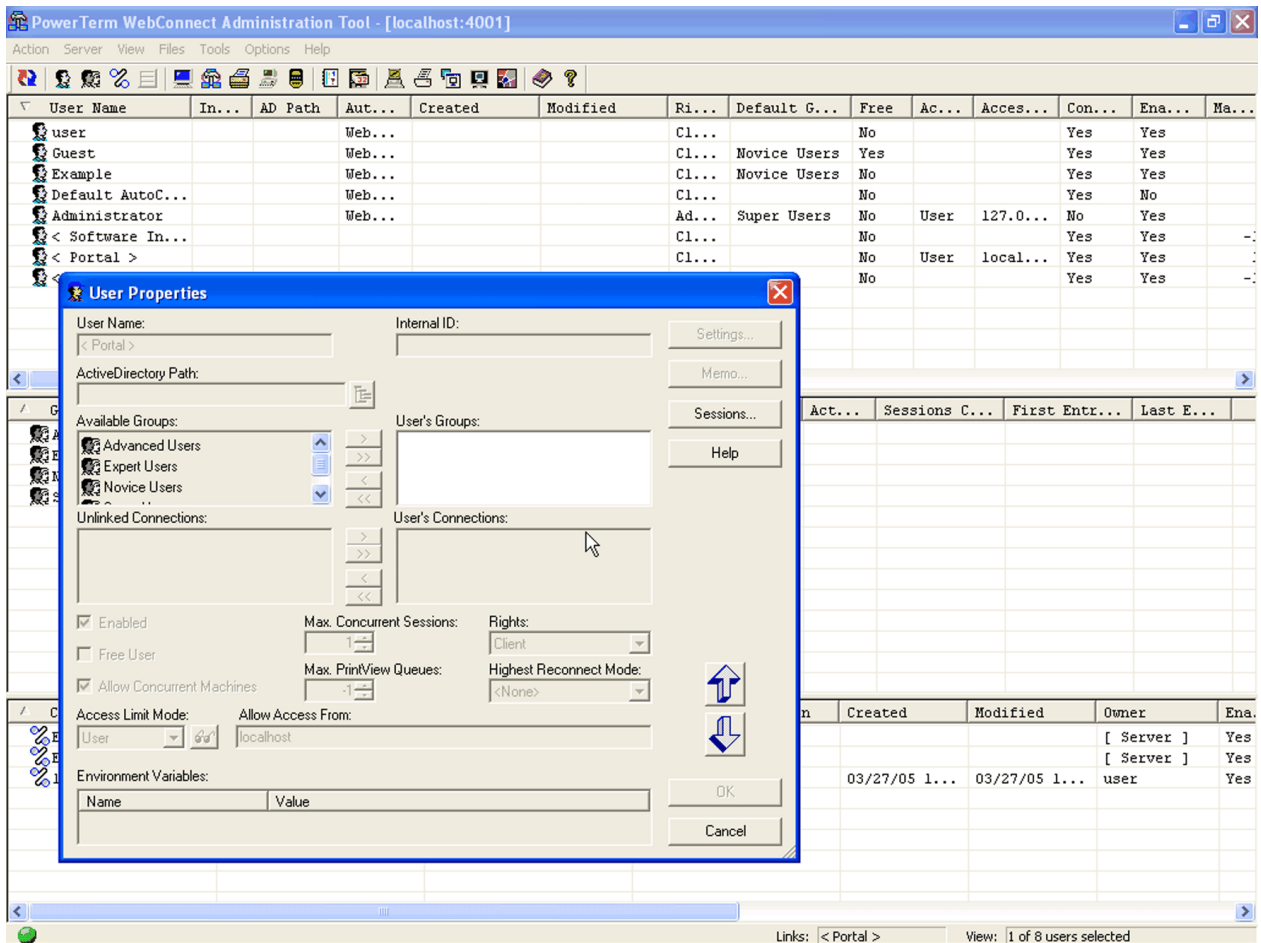
Administration Tool showing the Properties of the dedicated <Portal> user

By default, the "<Portal>" user is a member of the Everyone group in the security settings. If the "<Portal>" user is not a member of the Everyone group, the ComPortal.LOG log file will not be created. These log files are often crucial for diagnosing communication and configuration problems.

Installing the Application Portal on the same computer as the PowerTerm WebConnect Server

The default WebConnect Server installation procedure installs the Application Portal on the same computer as the PowerTerm WebConnect Server. In such a case there is no need to modify any of the ComPortal.ini parameters and the communications should function without the administrator having to make any other parameter modifications. As shown above, the default parameters of the ComPortal.ini point to localhost, as this is where the PowerTerm WebConnect Server resides in this case.

Installing the Application Portal on a computer other than the PowerTerm WebConnect Server

If the Application Portal is installed on one or more computers other than the computer hosting the PowerTerm WebConnect Server, the following parameter in the PtServer.ini file [Portal] section must be modified accordingly:

- Machines—must be either the IP address(es) or the name(s) of the IIS server(s). By default this is set to localhost. If multiple Web servers need to be specified, their names or IP addresses must be separated by semicolons (;).

- IPaddress

It is also possible to add additional [Server] record sections within the ComPortal.ini file that define other servers so that multiple PowerTerm WebConnect Servers will be available. Such a scenario is shown below.

```
********************************************************************************
:
:                    PowerTerm® WebConnect
:                          Release 5.5
:                           Aug 2006
:                      Ericom Software, Israel
:
********************************************************************************
:
[General]

MaxLogFileSizeK=<Default>
MaxLogBackups=<Default>
LogFlags=Run All
BackgroundColorRGB=<Default>

[Server=WebConnect_1]
Address=localhost:4000
CustomAddress=
SSL-Certificate=
Min-Instances=0
Max-Instances=10
Initial-Instances=0
Watch-Frequency-Seconds=15
BackgroundColorRGB=<Default>

[Server=WebConnect_2]
Address=192.168.0.1:4000
CustomAddress=192.168.0.135
SSL-Certificate=
Min-Instances=5
Max-Instances=20
Initial-Instances=8
Watch-Frequency-Seconds=10
BackgroundColorRGB=<Default>
```

ComPortal.ini file defining multiple WebConnect Servers

6.3.3. Troubleshooting

It is necessary to isolate where the operation has failed when a user is not able to login to the Application Portal,.

To check whether the failure is caused by the PowerTerm WebConnect Server or the IIS Server:

- Examine the PtServer.ini file found in the "WebConnect 5.6\database" directory for correct settings, in particular the [Server Connection Points Table] section.

- Examine the ComPortal.ini file found in the WebConnect 5.6\ComPortal\ directory for correct settings, in particular the Server name and IP address.

- Restart the IIS Server by running the IISreset command.

To isolate the point of failure:

1. Select View | Intruders from the Administration Tool to view failed logon attempts.

2. Examine the ComPortal.LOG file found in the WebConnect 5.6\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 unduly long elapsed times should be suspected of malfunctioning. See the LOG file samples below.

LOG file samples

6.3.3.1.1   Cannot find WebConnect Server

This error is caused by the ComPortal.ini parameters pointing to an incorrect WebConnect Server address. An extract of the LOG file showing this error displayed below.

```
**************************************************************************
C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.LOG

Started at   : 06/09/25 09:21:14
Terminated at: 06/09/25 09:22:24
Elapsed time :  0:01:10

DLL unloaded.

Software:
   Execute: C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.dll
   Version: 5.6 - Main Release
   Built  : 5.6.0.4000-rel.14317

Context:
   Account: DEMO2003\IUSR_ERICOM-MM10SFS8
   Machine: \DEMO2003
   IP addr: 126.0.1.173
   OS ver.: Windows 2003 Server (Service Pack 1) - Enterprise, Terminal Server
```

```
    OrgName: Ericom Software Ltd.

Process:
    PID    : 2776
    Thread : 820

LOG Recycle Count:
**************************************************************************
06/09/25 09:21:14.243 |      820 | Attaching to C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                              |      Version: 5.6.0.4000
                              |      Built  : 06/02/28 19:05:58
06/09/25 09:21:14.259 |      820 | Loading C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll
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 requested type
was found
06/09/25 09:21:28.409 |      f28 | *** ERROR *** [1095]
                              | Cannot create PortalClient:
                              | NO_DATA error encountered calling 'gethostbyname' (#11004)
                              | The requested name is valid, but no data of the requested type
was found
06/09/25 09:21:28.409 |      820 | *** ERROR *** [S21]
                              | in service Authenticate (CLIENT_POOL_EMPTY)::
                              | Pool empty
06/09/25 09:21:28.424 |      f28 | Portal client for demo20031:4000 terminated.
                              |      Status: UNDEFINED
06/09/25 09:21:28.424 |      820 | Service 'Authenticate' completed.
                              | Elapsed time: 2.490 seconds
                              | Total Count : 1
                              | Average time: 2.490 seconds
06/09/25 09:22:24.089 |      334 | DLL unloaded.
06/09/25 09:22:24.120 |      334 | Detaching from C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                              |      Version: 5.6.0.4000
                              |      Built  : 06/02/28 19:05:58
06/09/25 09:22:24.120 |      334 | C:/WINDOWS/system32/WS2_32.dll released
                              |      Version: 5.2.3790.1830
                              |      Built  : 05/03/24 17:26:40
06/09/25 09:22:24.136 |      334 | C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll released
                              |      Version: 0.9.7.10
                              |      Built  : 06/01/15 14:49:48
```

6.3.3.1.2   Machine is not in 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>". An
extract of the LOG file showing this is displayed below.

```
**************************************************************************
C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.LOG
```

```
Started at    : 06/09/25 09:25:09
Terminated at: 06/09/25 09:25:25
Elapsed time :  0:00:16

DLL unloaded.

Software:
   Execute: C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.dll
   Version: 5.6 - Main Release
   Built  : 5.6.0.4000-rel.14317

Context:
   Account: DEMO2003\IUSR_ERICOM-MM10SFS8
   Machine: \DEMO2003
   IP addr: 126.0.1.173
   OS ver.: Windows 2003 Server (Service Pack 1) - Enterprise, Terminal Server
   OrgName: Ericom Software Ltd.

Process:
   PID    : 1136
   Thread : d74

LOG Recycle Count:
***************************************************************************
06/09/25 09:25:09.165 |      d74 | Attaching to C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                             |     Version: 5.6.0.4000
                             |     Built  : 06/02/28 19:05:58
06/09/25 09:25:09.181 |      d74 | Loading C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll
06/09/25 09:25:09.181 |      d74 | 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 09:25:14.695 |      d74 | Service 'Authenticate' started.
06/09/25 09:25:14.695 |      880 | Connecting to server 'demo2003', port 4000...
06/09/25 09:25:14.695 |      880 | Connection to server 'demo2003' established
06/09/25 09:25:14.695 |      880 | Starting the pre-identification handshake...
06/09/25 09:25:16.429 |      880 | Sending the login request...
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.
                             | Server: demo2003:4000
06/09/25 09:25:16.476 |      880 | MessageBox :
                             |    Sevr: WARNING
                             |    Capt: w3wp - Login Rejected
                             |    Text: The access of user '< PORTAL >' to  is denied.
                             | Please contact your system administrator.
                             |
                             | Server: demo2003:4000
                             | Time:   2006/09/25 09:25:16
06/09/25 09:25:16.492 |      880 | Cleaning up...
06/09/25 09:25:16.492 |      d74 | *** ERROR *** [S21]
                             | in service Authenticate (CLIENT_POOL_EMPTY)::
                             | Pool empty
06/09/25 09:25:16.492 |      880 | Portal client for demo2003:4000 terminated.
                             |     Status: REJECTED
06/09/25 09:25:16.492 |      d74 | Service 'Authenticate' completed.
                             | Elapsed time: 1.797 seconds
                             | Total Count : 1
```
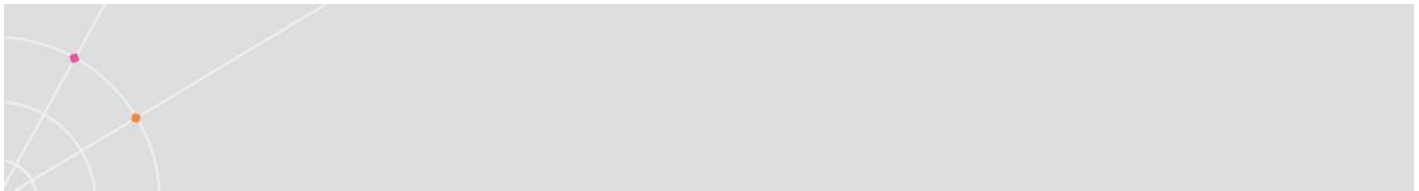
```
                                         |  Average time: 1.797 seconds
06/09/25 09:25:25.334 |        3e4 | DLL unloaded.
06/09/25 09:25:25.334 |        3e4 | Detaching from C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                                         |      Version: 5.6.0.4000
                                         |      Built  : 06/02/28 19:05:58
06/09/25 09:25:25.334 |        3e4 | C:/WINDOWS/system32/WS2_32.dll released
                                         |      Version: 5.2.3790.1830
                                         |      Built  : 05/03/24 17:26:40
06/09/25 09:25:25.365 |        3e4 | C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll released
                                         |      Version: 0.9.7.10
                                         |      Built  : 06/01/15 14:49:48
```

6.3.3.1.3   User <Portal> does not exist

This error is caused when the key UsePortalUsers in the PtServer.ini file is false. There
will be an entry in the intruder Record showing "Unknown user <Portal>". An extract of
the LOG file showing this error is displayed below.

```
************************************************************************
C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.LOG

Started at   : 06/09/25 09:30:02
Terminated at: 06/09/25 09:30:21
Elapsed time :  0:00:19

DLL unloaded.

Software:
   Execute: C:/Program Files/Ericom Software/WebConnect 5.6/ComPortal/ComPortal.dll
   Version: 5.6 - Main Release
   Built  : 5.6.0.4000-rel.14317

Context:
   Account: DEMO2003\IUSR_ERICOM-MM10SFS8
   Machine: \DEMO2003
   IP addr: 126.0.1.173
   OS ver.: Windows 2003 Server (Service Pack 1) - Enterprise, Terminal Server
   OrgName: Ericom Software Ltd.

Process:
   PID    : 1840
   Thread : b68

LOG Recycle Count:
************************************************************************
06/09/25 09:30:02.770 |        b68 | Attaching to C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                                         |      Version: 5.6.0.4000
                                         |      Built  : 06/02/28 19:05:58
06/09/25 09:30:02.785 |        b68 | Loading C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll
06/09/25 09:30:02.801 |        b68 | 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 09:30:02.817 |        b68 | Service 'Authenticate' started.
06/09/25 09:30:02.817 |        790 | Connecting to server 'demo2003', port 4000...
06/09/25 09:30:02.832 |        790 | Connection to server 'demo2003' established
06/09/25 09:30:02.832 |        790 | Starting the pre-identification handshake...
```
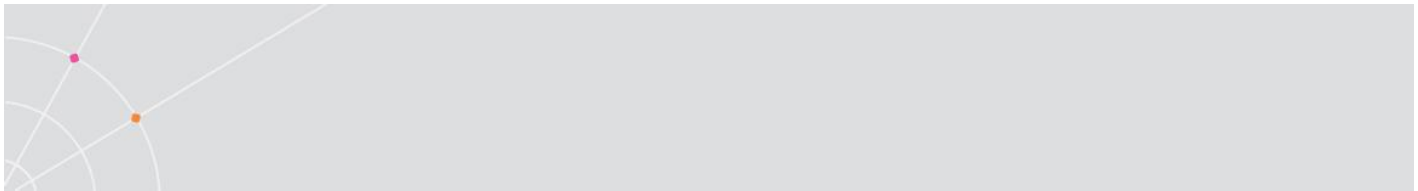
```
06/09/25 09:30:04.381 |        790 | Sending the login request...
06/09/25 09:30:04.397 |        790 | The login request was sent
06/09/25 09:30:04.397 |        790 | Login rejected:
                                  | State : 4
                                  | Reason: The user '< PORTAL >' is not defined.
                                  | Server: demo2003:4000
06/09/25 09:30:04.397 |        790 | MessageBox :
                                  |    Sevr: WARNING
                                  |    Capt: w3wp - Login Rejected
                                  |    Text: The user '< PORTAL >' is not defined.
                                  |
                                  | Server: demo2003:4000
                                  | Time:   2006/09/25 09:30:04
06/09/25 09:30:04.397 |        790 | Cleaning up...
06/09/25 09:30:04.397 |        b68 | *** ERROR *** [S21]
                                  | in service Authenticate (CLIENT_POOL_EMPTY)::
                                  | Pool empty
06/09/25 09:30:04.412 |        790 | Portal client for demo2003:4000 terminated.
                                  |     Status: REJECTED
06/09/25 09:30:04.412 |        b68 | Service 'Authenticate' completed.
                                  | Elapsed time: 1.595 seconds
                                  | Total Count : 1
                                  | Average time: 1.595 seconds
06/09/25 09:30:21.227 |        700 | DLL unloaded.
06/09/25 09:30:21.227 |        700 | Detaching from C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/ComPortal.dll
                                  |     Version: 5.6.0.4000
                                  |     Built  : 06/02/28 19:05:58
06/09/25 09:30:21.227 |        700 | C:/WINDOWS/system32/WS2_32.dll released
                                  |     Version: 5.2.3790.1830
                                  |     Built  : 05/03/24 17:26:40
06/09/25 09:30:21.243 |        700 | C:/Program Files/Ericom Software/WebConnect
5.6/ComPortal/openssl.dll released
                                  |     Version: 0.9.7.10
                                  |     Built  : 06/01/15 14:49:48
```
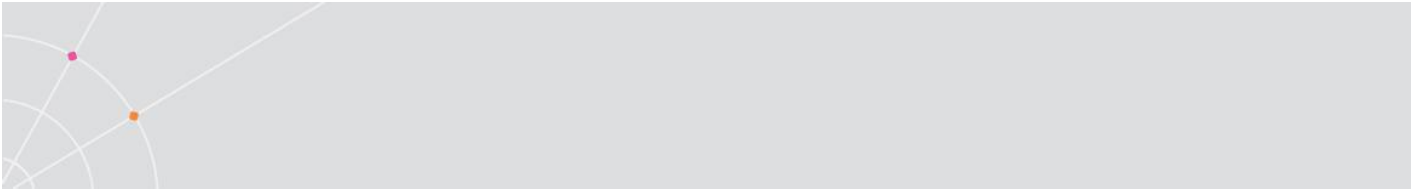
7. Monitoring Settings, Status, and History

A PowerTerm WebConnect Administrator can get the complete overview of the users, groups, and connections in the entire system. All the current settings are visible and, if necessary, the administrator can modify the properties for all or any of these entities. For example, you can view the status information to determine if any user or groups is exceeding its bandwidth threshold, thus creating a problem for the rest of the system users.

7.1. Information Tables: Focusing on What You Need

The Client Sessions, Administrative Sessions, LPD Queues, and Intruders windows, as well as the Users, Groups, and Connections panes, all use the same tabular structure.

Each table row represents an object, queue, or session, while each column represents a property or a piece of runtime information about the item. In the main information panes, new rows are added when you create new objects. In other windows, new rows are added when new queues are generated or sessions established.

In all these windows, there are numerous columns, and you may want to customize which columns are shown, in order to focus on the information you need.

7.1.1. Changing Column Width and Order

You can manually change the width of specific columns, or automatically expand a column to view its title or contents. You can also drag-and-drop column titles to change the order in which columns appear.

> NOTE You can view column titles and the full text of column contents without expanding a column. Position your mouse over a column title, or a certain line's text, to see a tool-tip with the full text.

To manually change a column width:

Click and drag the desired border heading to required width.

To automatically expand a column:

Right-click the desired column title.

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

To change the position of a column:

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

7.1.2. Adding and Removing Columns

Some information tables contain numerous of columns. You can choose to remove specific columns, or filter columns by type, so the table only shows properties and settings, or current status information.

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

To filter columns so only properties and settings are shown:

Right-click an object and select **Columns | Definition Information** (**Communication Information** in the **Connections** table).

To filter columns so only current status information is shown:

Right-click an object and select **Columns | Runtime Information**.

To view all columns (including those you have removed or filtered out):

Right-click an object and select **Columns | Set Default Size**.

7.1.3. Sorting the Tables

You can sort the tables by clicking a column (field). The column you click will become the primary sorting field. When you click 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.

7.1.4. Refreshing the Information Tables

You can set the information tables to update at fixed intervals, or refresh them manually.

To refresh all the information tables manually:

Select View | Refresh I/O Information or click   .
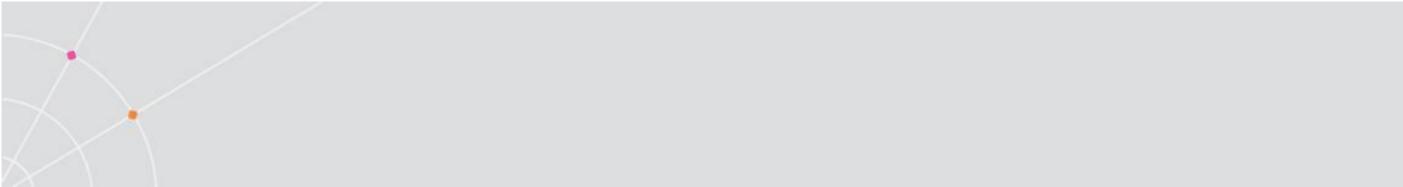
To set the automatic refresh interval:

1. Select Server | Configuration.

2. Designate the time interval in which refresh will be done automatically in Administrator Auto Refresh Freq.

NOTE   For servers that contain many objects, enabling automatic refresh may effect the performance of both the server and the Administration Tool, causing significant network traffic. In such cases it is recommended to increase the automatic refresh interval, or turn off the automatic refresh capability altogether.

To synchronize the WebConnect Server and the Active Directory:

Select Server | Refresh ActiveDirectory Information.

7.2. Monitoring Users' Online Activity

The Administration Tool provides extensive information about user status and activities. This information is organized in two ways:

- By connection source: You can view status reports for computers, PowerTerm WebConnect users, or PowerTerm WebConnect groups.

- By sessions: You can view information about client sessions originated by a specific user, users belonging to a certain group, or all users.

7.2.1. Status Information for Computers, Users, and Groups

Two information panes and one window show status reports organized by connection source: the Users pane, filtered by Runtime Information; the Groups pane, filtered by Runtime Information; and the Machines window.

All of these use the standard PowerTerm WebConnect tabular format.

Runtime Information Fields

The Users pane, Groups pane, and Machines window, each show runtime information for a different class of connection source. The following table lists and explains all the runtime information fields, and indicates which of them are shown in each window (a √ indicates that the window shows the field).

Keep in mind that fields shown 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.
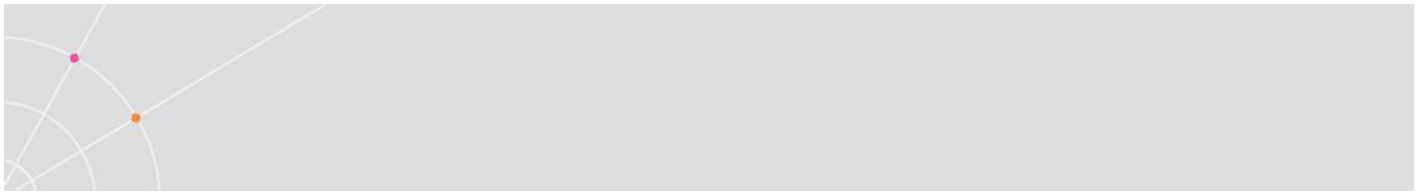
Column	Description	Users Pane	Groups Pane	Machines Pane
IP Address	The IP address of the remote client.	-	-	√
Sessions Count	The total number of sessions that are currently being used by the group.	√	√	√
First Entrance	The date and time of the login of the user.	√	-	-
Last Entrance	The date and time 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	√	-	-
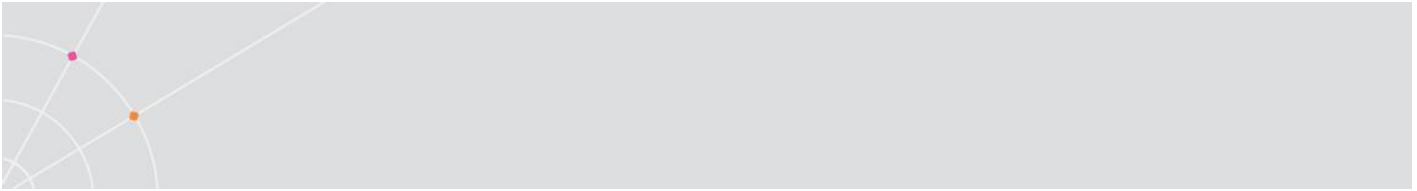
	traffic that were received from the client.			
Output Messages	The total of application packets that were sent to the client.	√	-	-
Input Messages	The total of application packet that were received from the client.	√	-	-
Active Users Count	The total number of the group's users that are currently active.	-	√	-

7.2.2. Online Activity by Sessions

You can also view runtime information organized by client sessions. In the Client Sessions table, a new entry is created each time a user connects to the host, regardless of the number of active sessions that the user already has.

You can view a table showing all the sessions opened by a specific user, all the users in a specific group, or all the users in the system. The fields in session information tables are divided into two groups: static fields that identify the session and I/O Information fields that show constantly updated information about the session (until it ends).

These tables use the standard PowerTerm WebConnect tabular format.

To view sessions opened by a specific user:

Right-click Sessions on the desired user. The session window for that user opens.

OR

1. Select the user and right-click Properties. The User Properties dialog is displayed.

2. Click the Sessions button.

To view sessions opened by all the users in a specific group:

Right-click Sessions on the desired group. The session window for that group opens.

OR

1. Select the group and right-click Properties. The Group Properties dialog is displayed.

2. Click the Sessions button.

To view sessions opened by all users:

Select View | Client Sessions or click . The Sessions window opens.

To filter session tables so only static definition information is shown:

Right-click Identification Information in the Sessions window.

To filter session tables so only live input/output information is shown:

Right-click I/O Information in the Sessions window.

7.3. Viewing Administrative Sessions

The Administrative Sessions window allows you to view 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.

The table uses the standard PowerTerm WebConnect tabular format.

To open the Administration Sessions Window:

Select Views | Administrative Sessions or click .

7.4. Viewing Intruders

The Intruders window shows suspected attempts at breaching security. Every entry in the table represents an instance where a user either:

- Attempted to connect using HTTP protocol, 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 his **Allow Concurrent Machines** parameter is switched off.

After several suspected intrusion attempts, users are blocked temporarily. The number of attempts and the time period of blocking are defined in the Intruders area of the Server Configuration dialog (see chapter 2.6.2).

In addition to showing suspected intrusion attempts, the Intruders window allows you to remove restrictions on users. If the system's users are repeatedly picked up and singled out as intruders, and you believe the action performed is innocent, you can prevent this individual from being picked up as an intruder in the future

To open the Intruders view:

Select View | Intruders or click . The All Intruders view appears.

To remove a user restriction:

Right-click the desired user entry in the table and select **Allow**.

7.5. Viewing Properties for Multiple Users, Groups, and Connections

You can view the current settings for a large number of system objects in a tabular format. The Users pane, Groups pane, and Connections pane (which together take up most of the Administration Tool's main window), allows you to view properties for all the users, groups, and connections in the system, respectively.

These three panes use the standard PowerTerm WebConnect tabular format.

To show the Users pane if it is not currently showing, or to enlarge it:

Select View | Users.

To show the Groups pane if it is not currently showing, or to enlarge it:

Select View | Groups.

To show the Connections pane if it is not currently showing, or to enlarge it:

Select View | Connections.

7.6. Viewing Status for PrintView (LPD) Queues

The PrintView Client allows transparent printing (i.e. passes all characters, including escape sequences that arrive at the port directly to the printer without translation) from the host server to a printer, which may be at a location remote from the host. The host sends print jobs from certain queues to the PrintView Client, running on a PC that has access to a conveniently located printer. The PrintView Client, which may be in another network or even in another geographic location, prints the job on the local printer.

For this process to work, PrintView queues corresponding to the host's queues must be defined on the PrintView Client, and then registered with the PowerTerm WebConnect server. The PrintView Queues window shows definition and runtime information on all the print queues registered with the server.

For more detailed information on the PrintView Client and its queues and jobs, see the PrintView Client User Guide in PDF format or the PrintView Client's online help.

To open the PrintView Queues Window:

Select View | PrintView Queues.

7.7. Viewing Server Statistics and Logs

PowerTerm WebConnect Administration Tool allows you to view status information on the server, and open the logs for the PowerTerm WebConnect server and the starter service.

7.7.1. Real-time Statistics

The Deployment and Performance Statistics dialog, displays real-time information for the PowerTerm WebConnect server. These statistics are similar to the ones that appear in the Performance tab of the Windows Task Manager.
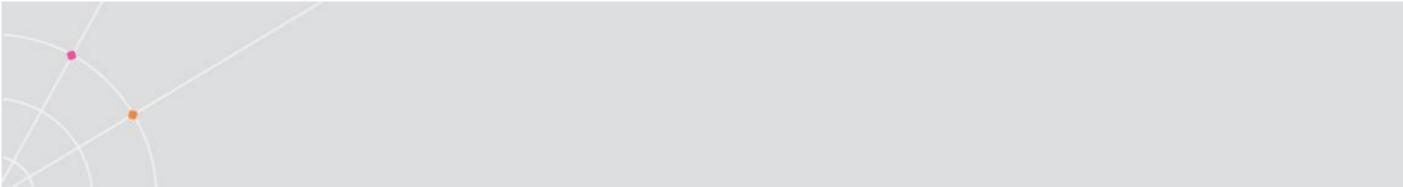
To open the Deployment and Performance Statistics dialog:

Select Server | Deployment and Performance Statistics.

7.7.2. Event Viewer

The Administration Tool provides a shortcut to the Windows Management Console Event Viewer, where you can view all Windows system events, including events generated by the PowerTerm WebConnect server.

To open Event Viewer:

Select Tools | Event Viewer.

7.7.3. System Logs

The log files are circular text files. The last log message is followed by a line filled in by the "~" character. If the maximum allowed file size is reached, then the last line is filled in by the "^" character, indicating that any new log messages will be written at the start of the file overwriting any previously written log messages.

Each execution of the PowerTerm WebConnect server or starter opens two new (standard) log files, PtServer.LOG and PtStarter.LOG. PowerTerm WebConnect maintains backup versions of these log files. They are named exename.LOG.bck-00N.

- PtServer.LOG This is the log file of the PowerTerm WebConnect server.

- PtStarter.LOG This is the log file of the PowerTerm WebConnect starter.

There are also log files for

- Failover History, records the Failover state transition of PowerTerm WebConnect servers working in Failover mode (see chapter 12).

- Audit Trail

- Error log, an Excel CSV document. Each error signaled in the Standard log goes also here.

- System Information log, 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).

To view the log file for the PowerTerm WebConnect Server:

Select Files | LOG files | PtServer.LOG.

To view the log file for the PowerTerm WebConnect Starter Service:

Select Files | LOG files | PtStarter.LOG

To view the Failover log:

Select Files | LOG files | FAILOVER History.LOG.

7.7.4. Audit Trail

The Audit Trail is a chronological record of the PowerTerm WebConnect system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized. The output is a record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

AuditTrail_Options uses a standard command line format, where the following values and flags are supported:

* /LAYOUT=	Establishes the layout mode, one of MINIMAL (default) or FULL.
	When /LAYOUT=FULL is used, all the relevant columns are filled in.
* One of /TITLE, /NOTITLE or /TITLE=…	Enables/disables/specifies the usage of the column titles row.
	/TITLE The default column titles will be used (default).
	/NOTITLES Column titles will not be used.
	/TITLE=… The supplied list of column titles will be used. The very first character will be used as separator. The column titles must be specified in their regular order.
* One of /READ_ONLY or /READ_WRITE	Establishes the write permission mode of the file when it will be closed at midnight. Default: /READ_ONLY
* /DIR=	Specifies the folder of the audit trail output, other than the default. By

	default the PtAT.dll creates files in the folder <database>/Audit Trail.
	The value specified by /DIR= <option> may contain the logical folders <database> and <exe>.
* /FILETITLE=	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:
	<YEAR> Year with century, as decimal number.
	<YEAR2> Year without century, as decimal number (00-99).
	<MONTH> Month as decimal number (01-12).
	<MONTHNAME> Abbreviated month name.
	<MONTHNAMEFULL> Full month name.
	<WEEKDAY> Abbreviated weekday name.
	<WEEKDAYFULL> Full weekday name.<DAY> Day of month as decimal number (01-31).
	<COMPUTER> PowerTerm WebConnect server's computer name.
* /EXT=	Specifies the file extension of the audit trail output, other than the default. By default the PtAT.dll creates files of CSV type.
* One of /DAILY, /WEEKLY or /MONTHLY	Establishes the file replacement (renewal) mode.
	/DAILY The file will be replaced at midnight (default).
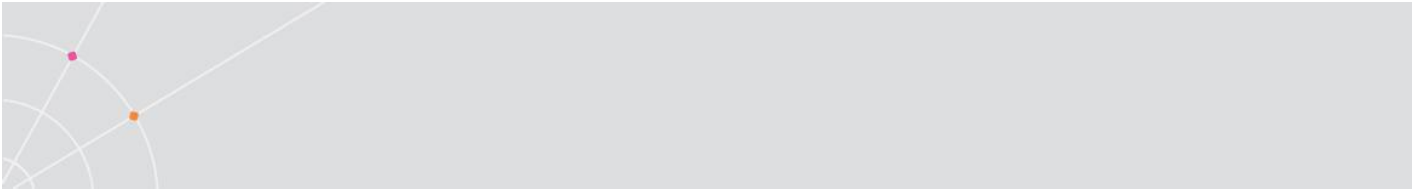
	/WEEKLY The file will be replaced on Mondays at midnight.
	/MONTHLY The file will be replaced at midnight on the 1st of the month.

To view the audit trail:

Select Files | LOG files | Audit Trail. An Excel file containing the current audit trail information is displayed.

8. Customizing Clients

PowerTerm WebConnect provides a wide variety of tools and options to customize the look and behavior of its clients. Use the Administration Tool to control and modify these options.

8.1. Customizing Emulation Clients

By modifying various properties of the connection and user objects, you can control the appearance and functionality of the emulation clients: PowerTerm WebConnect HostView for Windows and Linux, PowerTerm WebConnect WebView and the Java Client.

8.1.1. Terminal Setup

PowerTerm WebConnect enables you to configure your terminal emulation to work with your desired preferences. You can configure the Settings on multiple levels where the levels are organized as a hierarchy going from Connection settings (the least user specific), through the Group settings, to the User settings (most user specific). You can also configure default settings on the Server level.

To configure settings at the user level:

1. Double-click the desired User. The User Properties dialog is displayed.

2. Click the Settings button. The Terminal Setup dialog is displayed.

3. Enter your preferences in the different Property tabs and click Save.

To configure settings at the group level:

1. Double-click the desired Group. The Group Properties dialog is displayed.

2. Click the Settings button. The Terminal Setup dialog is displayed.

3. Enter your preferences in the different Property tabs and click Save.

To configure settings at the connection level:

1. Double-click the desired Connection. The Connection Properties dialog is displayed.

2. Click the Settings button. The Terminal Setup dialog is displayed.

3. Enter your preferences in the different Property tabs and click Save.
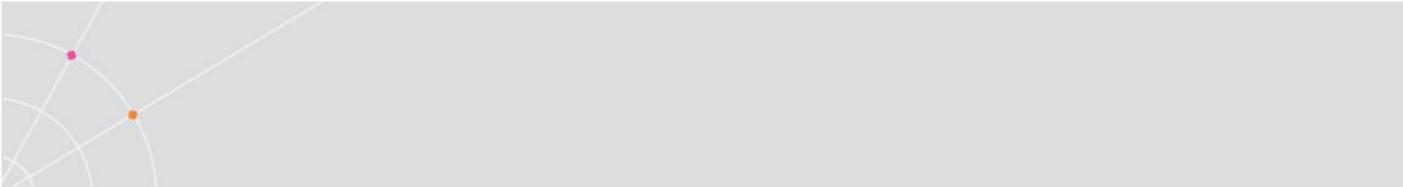
To configure settings at the server level:

1. Select Server | Default Settings. The Terminal Setup dialog is displayed.

2. Enter your preferences in the different Property tabs and click Save.

8.1.2. Background Bitmap

You can specify a bitmap of your choice as the background of your emulation screen until the user connects to the host.

To set a background bitmap:

1. Select Files | Put Background Bitmap. The Select Background Bitmap File dialog appears.

2. Locate the appropriate folder and bitmap file.

3. Select it and click Open. The bitmap appears as your background until you connect to the host.

8.1.3. Keyboard Mapping
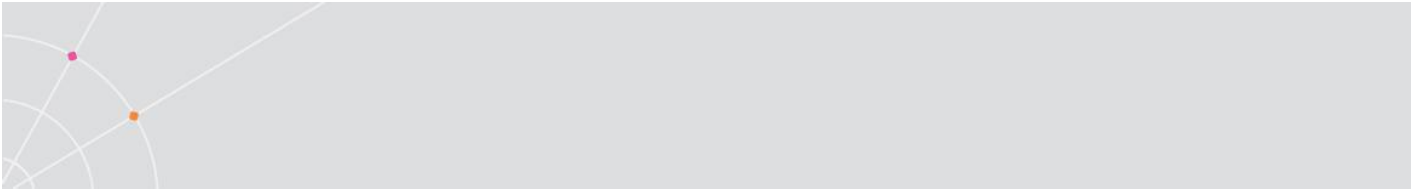
PowerTerm emulation clients enable you to map PC keys to host keys in order to emulate the host terminal keyboard. You can also move the functionality of a mapped PC key to another PC key. The keyboard mapping definitions are stored in a file with the same name as the current terminal setup file, with the extension .ptk. For example, the default keyboard mapping definitions are stored in a file called ptdef.ptk.

To view (open) the keyboard mapping:

1. Select the emulation for which you want to map the keys.

2. Right-click Properties. The Connection Properties dialog appears.

3. Click the Key Mapping button. The Keyboard Mapping dialog appears.

4. Slide the mouse over the different keys. The bottom line of the dialog shows you the corresponding PC and terminal keys. For example, if you point to the "t" key of the VT keyboard, you see that the corresponding PC key is "T".

To map a PC key to a host key:

1. Open the Keyboard Mapping dialog.

2. Drag a key from the upper terminal keyboard to a PC key on the lower keyboard.

3. Click the <Shift> or <Control> keys on the terminal keyboard to display additional key functions. For example, if you click the <Shift> key, the alphabet keys on the terminal keyboard are displayed in upper case. You can then map (drag) these keys to your PC keyboard keys.

To copy a PC key to another PC key:

1. Open the Keyboard Mapping dialog.

2. Hold the <Ctrl> key while dragging the PC key whose function you want to copy to the required PC key. Both keys now have the same functionality.

To assign a script command to a PC key:

1. Open the Keyboard Mapping dialog.

2. Right-click a key on the PC keyboard to which you want to assign a command and select Enter Script Commands. The PC Button dialog appears.

3. Enter the script (PSL) command description and click OK. The PC key has now been assigned a script command.

To replace a PC key with another PC key:

1. Open the Keyboard Mapping dialog.

2. Drag the desired PC key onto the PC key that it will replace. The functionality of the PC key has been replaced.

3. Drag the replacing key back to its original position to restore the values.

To map combinations of keys that include Alt, Ctrl, and Shift:

1. Open the Keyboard Mapping dialog.

2. Click the <Alt>, <Ctrl>, or <Shift> key (or any combination) on your PC keyboard. You are able to map keys by following the procedures described previously.

3. Click <Alt>, <Ctrl>, or <Shift> key (or any combination), to view the mapped key.

To cancel a keyboard key definition:

1. Open the Keyboard Mapping dialog.

2. Drag the PC key definition that you want to cancel, in the Keyboard Mapping dialog, to the wastebasket icon. This restores the default function of the PC key.

To restore the default keyboard mapping of all mapped keys:

1. Open the Keyboard Mapping dialog.

2. Click the Default button.

8.1.4. Power Pad

The Power Pad is a floating keypad for which its buttons can be programmed to execute customized PSL scripts. The buttons are by default named F1, F2, F3, and so on, with a few default function names, such as Clear, Enter, and Insert. The number of displayed buttons and their names can be changed.

The Power Pad can be defined at the server's general level or at the connection level.

To open the Power Pad & Function Buttons at Server's General Level:

Select Server | Default Power Pad. The Power Pad & Function Buttons dialog appears.

To open the Power Pad & Function Buttons at Connection Level:

1. Select the emulation for which you want to map the Power Pad.

2. Right-click Properties. The Connection Properties dialog appears.

3. Click the Power Pad button. The Power Pad & Function Buttons dialog appears.

To program the Power Pad:

1. Double-click the row/column line for the button you want to program. The Power Pad Button dialog appears.

2. Enter its Description and Script Command.

NOTE   If you want to conceal the PSL command, add an asterisk to the beginning of the command.

3. Click OK.

To preview the Power Pad:

Click .

To reset the Power Pad:

1. Click the Clean Power Pad button. A confirmation message is displayed.

2. Click Yes.

To adjust the number of buttons in the Power Pad:

Select the number of rows and/or columns that you desire from the dropdown boxes.

NOTE   You can display a maximum of 10 rows and 10 columns in the Power Pad, whereas the defaults are 9 rows and 4 columns.

8.1.5. Function Buttons

Along the bottom of the PowerTerm emulation window are Function buttons by default named F1, F2, F3, etc. These can be renamed and programmed to execute customized scripts. Send the programmed command to the host by clicking the desired Function button. The Function button parameters are saved automatically in the terminal setup file.

The Function buttons can be defined at the server's general level or at the connection level.

To open the Power Pad & Function Buttons at Server's General Level:

Select Server | Default Power Pad. The Power Pad & Function Buttons dialog appears.

To open the Power Pad & Function Buttons at Connection Level:

1. Select the emulation for which you want to map the Function buttons.

2. Right-click Properties. The Connection Properties dialog appears.

3. Click the Power Pad button. The Power Pad & Function Buttons dialog appears.

To program the Function buttons:

1. Double-click the row/column line for the button you want to program. The Function Button dialog appears.

2. Enter its Description and Script Command.

NOTE   If you want to conceal the PSL command, add an asterisk at the beginning of the command.

3. Click OK.

To preview the Function buttons:

Click .

To reset the Function buttons:

1. Click the Clean Functions button. A confirmation messages is displayed.

2. Click Yes.

To adjust the number of Function buttons:

Select the number of columns that you desire from the dropdown box.

> NOTE You can display a maximum 24 columns of Function buttons, whereas the default is 12.

8.2. Using Environment Variables

Use the Environment Variables table, available in various Property dialogs, to create environment variables that effect the behavior of specific objects.
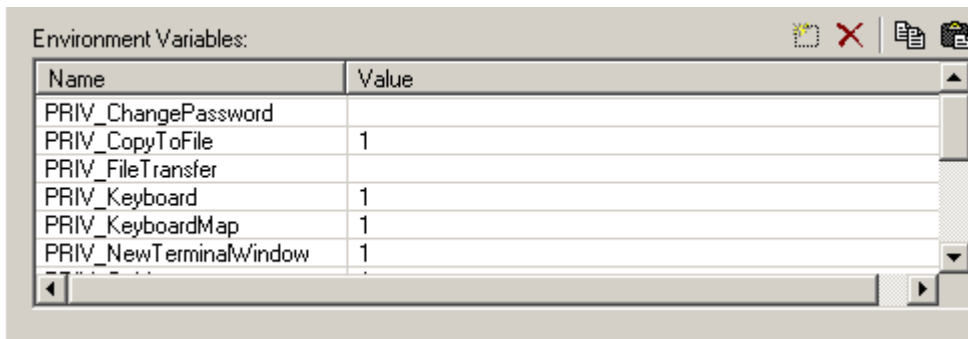
8.2.1. Default Environment Variables

The following table explains the main environment variables that are defined by default.

> NOTE An empty value indicates that the initial value of the variables is set to none.

Variable name	Values	Description
AGENT_AllowMultiple	1 = on Default: 1 Upgrade: empty	Privilege to run multiple agents for the same user (but different IPs).

AGENT_ExitCleanMode	DoNothing	Specifies what to clean when exiting the Agent.
	CleanCredentials	
	CleanApplications	
	CleanAll = Cleans credentials and all the created shortcuts.	
	Disable = The user cannot exit the agent.	
	Default: empty = Cleans credentials and applications.	
AGENT_SysTray	Regular	
	HoldUp	
	Hide	
	Default: empty = The command line value will be used.	
DOWNLOADS_Disable	Updates = Only the updates are disabled (missing files are downloaded).	Specifies download permissions.
	NewFiles = Only the missing files are disabled (updates are allowed).	
	All = The download functionality is fully disabled.	
	Any other value = Download fully enabled.	

	Default value: empty	
LPD_AutoReloginAnyway	1 or TRUE = The PrintView client tries to re-login even if there are queues that support direct accesss also. Default: empty	Only relevant if LPD_AutoReloginFrequen cySeconds value >0.
LPD_AutoReloginFrequen cySeconds	Range 10 – 300 0 (zero) to disable Default: 30	Specifies the frequency of the re-login attempts when the login to PowerTerm WebConnect server was lost or closed because of an internal error.
LPD_SocketReadTimeout Seconds	5 Default: 30	The timeout of reading from the socket while processing a job.
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/WebView clients.
PRIV_Keyboard	1 Default: empty	Enables the user to open and/or save the keyboard mapping of the
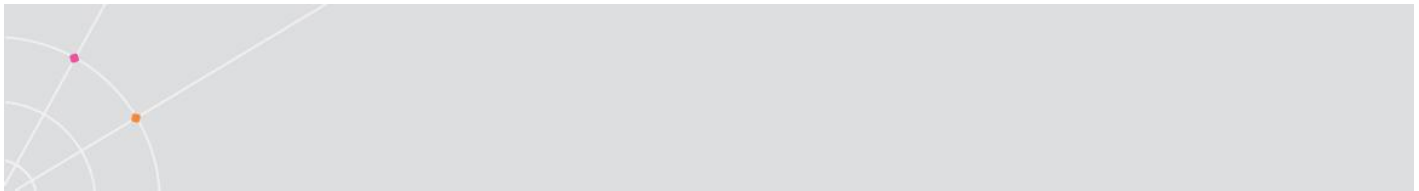
		emulator clients.
PRIV_KeyboardMap	1 Default: empty	Enables the user to view and/or modify the keyboard mapping of the emulator clients.
PRIV_Online	1 Default: empty	Enables the user to switch the emulator client off/on line.
PRIV_PowerPad	1 Default: empty	Enables the user to modify, open and/or save the Power pad and Function buttons of the emulator clients.
PRIV_RunDFT	Default: empty	Enables the user to run Ericom's DFT utility.
PRIV_RunFTP	Default: empty	Enables the user to run Ericom's FTP utility.
PRIV_RunLPD	Default: 1	Enables the user to run PowerTerm WebConnect PrintView client.
PRIV_RunQuicFTP	Default: 1	Enables the user to run PowerTerm WebConnect QuickFTP client.
PRIV_RunRDP	Default: 1	Enables the user to run PowerTerm WebConnect RemoteView client.
PRIV_RunSupport	Default: 1 Upgrade: 1	Enables the user to run PowerTerm WebConnect SupportView client.
PRIV_RunVNC	Default: 1	Enables the user to run PowerTerm WebConnect QuickVNC client.
PRIV_Script	Default: empty	Enables the user to run PSL commands and scripts, to edit and to record them.
PRIV_SendImage_BitsPe	0, 4, 8, and 16	The maximum resolution
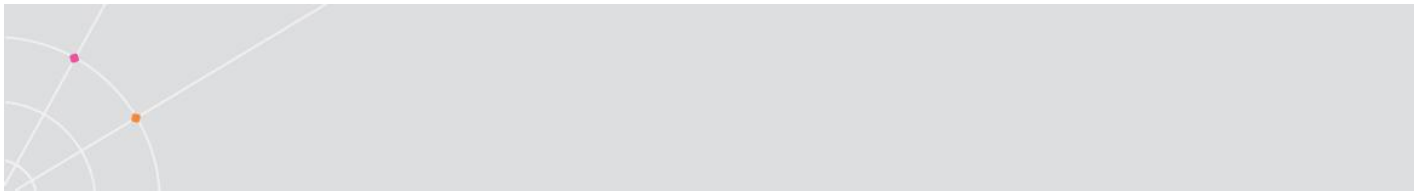
rPixel	Default: 4	of the Desktop bitmap image to be attached to a message. 0 (zero) means than no image can be attached.
PRIV_SendImage_MaxSizeK	Default: 32	The maximum size (in kB) of the compressed Desktop bitmap image. 0 (zero) means than no size limitation is applied.
PRIV_SendMessage	0 = off 1 = single messaging target 2 = multiple messaging targets Default: emtpy	Enables the user to use the messaging facility of PowerTerm WebConnect.
PRIV_Setup	Default: empty	Enables the user to modify and/or save the setup of the emulator clients.
PRIV_TerminalCanCreateShortcut	Default: empty	For sessions running on a Terminal Server. Only evaluated if PRIV_CreateShortcut is enabled.
PRIV_Trace	(empty)	Enables the user to use the trace facility of the emulator clients.
PRIV_UniversalPrinting	Default: empty Upgrade: empty	Enables the user to use the Universal Printing feature of the RDP client.
PRIV-NewTerminalWindow	1	Enables the user to open a new emulator client.
RDP_DisablePrintScreenKey	1 = on Default: 0 Upgrade: empty	Disables the PrintScreen function in RemoteView sessions.

RDP_DisableSessionSharing	1 = on Default: 0 Upgrade: empty	Disables the Session Sharing of RemoteView sessions.
RDP_DisableUniversalPrinting	Default: 1 Upgrade: 1	Disables the Universal Printing feature of RDP client.
RDP_PreTsAgentExe	Default: empty Upgrade: empty	Name of file to run before running the TSAgent.
RDP_RedirectSchemes	Default: empty Upgrade: empty	Specifies what protocols to redirect, like http, https, etc.
RDP_RedirectExclude	Default: empty Upgrade: empty	Specifies what URLs not to redirect.
Support_ERICOM	Default: support@ericom.com	Specifies the To e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailBcc	Default: empty	Specifies the Bcc 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 Body e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailCc	Default: empty	Specifies the Cc e-mail parameter to be used by the SendEmailToSupport facility of the

		Administration Tool.
Support_MailSubject	Default: empty	Specifies the Subject e-mail parameter to be used by the SendEmailToSupport facility of the Administration Tool.
Support_MailTo	Default: support@ericom.com	Specifies the To e-mail parameter to be used by the SendEmailToSupport facility of the HostView/WebView clients.
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	Specifies the terminal language (code page set) for the HostView/WebView client.
TriceratUniversalPrinting Version	Default: empty Upgrade: empty	Enables the user to use the version of triCerat plug-in client. Used for multiple triCerat plug-in clients support.
USE_CLIENT_HostView		Replaces USE_CLIENT_activex and USE_CLIENT_exe
USE_CLIENT_Java		Allows use of Java emulators.

USE_CLIENT_WebView		Replaces USE_CLIENT_ocx
W2H_LoginDisabledReason	Default: empty	If not empty, any new emulator client will be logged off immediately, displaying the specified text.
W2H_SupportAccepted		The text sent to the client requesting support when the request is accepted.
W2H_SupportRejectedBy User		The text sent to the client requesting support when the request is rejected explicitly by the support.
W2H_SupportRejectedOn Timeout		The text sent to the client requesting support when the request is rejected due to the timeout being exceeded.

8.2.2. Creating and Modifying Variables

Creating New Environment Variables

There are two ways to create Environment Variables: Create a new one from scratch, or copy an existing one and modify its name and values.

To create a new Environment Variable:

1. Double-click or right-click Properties on the desired User or Group. The Properties dialog appears. You can also select Server | Configuration to create Environment Variables on the server level.

2. Click [ ]. The Define Environment Variable dialog appears.

3. Type the new environment variable's Name.

4. Determine the new environment variable's Value.

5. Determine whether the new environment variable should be Encrypted.

6. Click OK. The new environment variable appears in the list.

To copy and modify a new Environment Variable:

1. Double-click or right-click Properties on the desired User or Group. The Properties dialog appears.

2. Select the desired Environment Variable and click .

3. Use and to navigate to the particular user or group entity to where you want to copy the variable.

4. Click . A copy of the original appears in the Environment Variables table.

5. Double-click on the newly copied variable and make any necessary modifications.

6. Click OK.

> NOTE   You can also copy and paste variables between different user and group Properties dialog. However, only one dialog can be open at a time.

Modifying Existing Environment Variables

You can modify an existing Environment Variable either from the main Environment Variable window or from the Environment Variable table in the Properties dialog.

To open the Environment Variables Window:

Select View | Environment Variables.

To modify an Environment Variable:

1. Double-click the variable that you want to modify. The Define Environment Variable dialog appears with the selected variable's details. If you modify from the main Environmental Variable window, then it will be superimposed upon its relevant properties dialog.

2. Make the necessary modifications. The modifications are visible in the Environment Variables table of the Property dialog.

3. Click OK again if you modify from the main Environmental Variable window.

8.3. Advanced Client Customization and Command Line Parameters

Further advanced customizations can be done manually in the different default files found in the Files menu.

WARNING This should only be done by an experienced Administrator.

To make further advanced customizations:

1. Select Files | Defaults.
2. Select the appropriate file. The desired file opens in Notepad.

8.3.1. Common Client Command Line Parameters

Below is a list of common command-line parameters and flags that can be provided to most PowerTerm WebConnect clients, including the Administration Tool. These parameters control the behavior of the clients, specifically in their interaction with the WebConnect server. All the parameter names are non-case sensitive.

SSL-usage

/NOSSL= specifies if the connection to the server is not to be secured by SSL.

/SSL= (*) specifies if the connection to the server is to be secured by SSL.

/SSLCERTFILE[=[*]] explicitly specifies the SSL certificate filename.

/SSLCERTPATH[=[*]] specifies the path for the SSL certificate.

show-login-dialog-mode

/C2S_DLG(*) displays the Connection-to-Server dialog.

/NO_C2S_DLG does not display the Connection-to-Server dialog.

Reconnect-mode

/RM_NONE (*) will not reconnect an interrupted session.

/RM_ON DEMAND will reconnect only sessions connected through the PowerTerm WebConnect server's gateway.

/RM_WIRELESS will reconnect any session automatically. All wireless sessions use the PowerTerm WebConnect server's gateway.

/RM_INTERACTIVE enables the client to select the mode during login.

Self-update

/NOSELFUPDATE when activated the client does not verify whether a newer version appears on the WebConnect server.

(*) Earmarks the default value.

[*] If the designated file is not found, then the program will create it.

NOTE   The FTP client and the AS/400 DFT client do not support these command-line parameters because they connect directly to the host, without direct interaction with the WebConnect server. PowerTerm WebConnect WebView also does not support these parameters because it is an in-process COM Control and not a stand-alone executable.

8.3.2. Customizing the HostView Command Line Parameters

The following parameters can be used to customize the component either from the Command Line or via HTML:

Required

The server's address and port number in the following format:

<address>:port or address:port

for example: <webserver>:4001, webserver:4001

If the port number is omitted, the default (4000) is used.
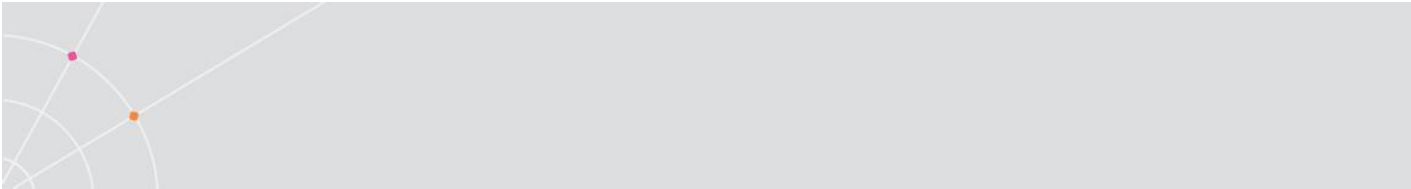
Optional

/USER= specifies the value for the User Name field. Placing an asterisk in front of the user name causes it to login immediately without displaying the login dialog.

/SID= specifies the value for the Session ID field.

/CONNECTION= specifies the predefined connection name.

NOTE   When you start PowerTerm WebConnect HostView with a specified **Connection** command line parameter you 'dedicate' it. This means that the **New Terminal Session** icon and menu item are removed from the GUI and there is no **Connection List** displayed.

Component Specific

shortcut-location

`/DESKTOP(*)` places a shortcut to the connection in use to the desktop.

`/STARTUP` places a shortcut to the connection in use to the Windows Startup menu.

`/BOTH` places a shortcut to the connection in use both to the desktop and to the Windows Startup menu.

language-id

/EN = English (*)

/FR = French

/DE = German

/IT = Italian

/ES = Spanish

/CZ = Czech

/? = as specified in the Regional Settings

8.3.3. Customizing HostView via the HTML

The Agent receives the parameters from the HTML and is customized accordingly. In turn, the Agent passes the /EXTRA_PARAMS to the HostView client.

Specify the parameters according to the appropriate platform. See the different examples below:

Activate using the Windows Downloader

```
<PARAM NAME="Parameters" VALUE="<WebServer> /NOSELFUPDATE /USER=*example
/PASS=example /RUN=HostView /EXTRA_PARAMS=/CONNECTION=Example_VT">
```

In this parameter string, <WebServer> is a macro that is translated by the Windows Downloader into the hostname of the Web server which provided the HTML. For details see chapter 11.

Activate using the Java Downloader

Modify the value of Java Script variable parameters in the corresponding html file.

For Windows clients edit the file **web/windows/HostView_J.html**. For example, to launch PowerTerm WebConnect HostView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect Server as user 'example' with password 'example' and to run a connection defined in PowerTerm WebConnect database as 'Example_VT':

```
//---------------------------------------------------
// Head Actions
//---------------------------------------------------
var component = "HostView";
```

// update here

parameters =

" /NOSELFUPDATE /SHORTCUT=BOTH /AUTOLOGIN=NO /RUN=HostView " +

" /USER=*example /PASS=example " +

" EXTRA_PARAMS=/CONNECTION=Example_VT ";

// end of update

```
// Identify browser
…
```

For Linux clients copy the file **web/linux/ix86/Agent_J.html** to **web/linux/ix86/HostView_J.html** and edit it. For example, to launch PowerTerm WebConnect HostView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect server as user 'example' with password example' and to run a connection defined in PowerTerm WebConnect database as 'Example_VT':

```
//---------------------------------------------------
// Head Actions
//---------------------------------------------------
```

// update here

parameters =

"/NOSELFUPDATE /SHORTCUT=BOTH /AUTOLOGIN=NO " +

"/RUN=HostView /USER=*example /PASS=example " +

" EXTRA_PARAMS=/CONNECTION=Example_VT ";

```
var component = "HostView";

// end of update

// Identify browser

…
```

8.3.4. Customizing the RemoteView Command Line Parameters

The following parameters can be used to customize the component either from the Command Line or via HTML:

Required

The server's address and port number in the following format:

<address>:port or address:port

for example: <webserver>:4001, webserver:4001

If the port number is omitted, the default (4000) is used.

Optional

/USER= specifies the value for the User Name field. Placing an asterisk in front of the user name causes it to login in immediately without displaying the login dialog.

/SID= specifies the value for the Session ID field.

/CONNECTION= specifies the predefined connection name.

8.3.5. Customizing RemoteView via the HTML

The Agent receives the parameters from the HTML, and is customized accordingly. In turn the Agent passes the /EXTRA_PARAMS to the RemoteView client.

Specify the parameters according to the appropriate platform. See the different examples below:

For example you want to run RemoteView client, which logs onto a WebConnect Server with a specific username and password and runs a specific connection.

Activate using the Windows Downloader

<PARAM NAME="Parameters" VALUE="<WebServer> /NOSELFUPDATE
/USER=*example /PASS=example /RUN=RemoteView
/EXTRA_PARAMS=/CONNECTION=MyTerminalServer">

In this parameter string, <WebServer> is a macro that is translated by the Windows Downloader into the hostname of the Web server which provided the HTML. For details see chapter 11.

Activate using the Java Downloader

Modify the value of the Java Script variable **parameters** in the corresponding html file.

For Windows clients edit the file **web/windows/RemoteView_J.html**. For example, to launch PowerTerm WebConnect RemoteView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect server as user 'example' with password 'example' and to run a connection defined in PowerTerm WebConnect database as 'MyTerminalServer':

```
//---------------------------------------------------
// Head Actions
//---------------------------------------------------
var component = "RemoteView";
// update here
parameters =
" /NOSELFUPDATE /RUN=RemoteView " +
" /USER=*example /PASS=example " +
" EXTRA_PARAMS=/CONNECTION=MyTerminalServer";
// end of update
// Identify browser
…
```

For Linux clients copy file **web/linux/ix86/Agent_J.html** to **web/linux/ix86/RemoteView_J.html** and edit it. For example, to launch PowerTerm WebConnect RemoteView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect server as user 'example' with password example' and to run a connection defined in PowerTerm WebConnect database as 'MyTerminalServer':

```
//-----------------------------------------------
// Head Actions
//-----------------------------------------------
// update here
parameters =
"/NOSELFUPDATE /RUN=HostView "   +
" /USER=*example /PASS=example " +
" EXTRA_PARAMS=/CONNECTION=MyTerminalServer ";
var component = "RemoteView";
// end of update
// Identify browser
```

…

8.3.6. Customizing the PrintView Command Line Parameters

The following parameters can be used to customize the component either from the Command Line or via the HTML:

Component Specific

shortcut-location

/DESKTOP(*) places a shortcut to the connection in use, to the desktop.

/STARTUP places a shortcut to the connection in use, to the Windows Startup menu.
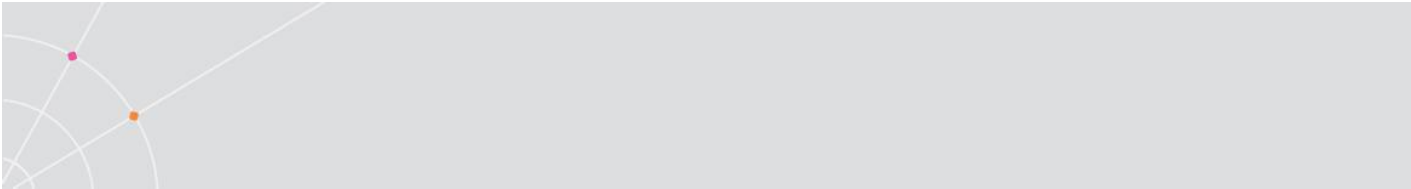
/BOTH places a shortcut to the connection in use, both to the desktop and to the Windows Startup menu.

/LPD_PORT=port-number

A valid TCP/IP port number to listen for LPD/LPR commands. (Default: 515)

/EXT_NAMES=external-names

A list of up to 9 external names, separated by spaces. They can be referred dynamically in the queue names by the symbol %N, where N is a 1 based index in the external names list. Example: if /EXT_NAMES="A B C" then the queue name Queue_%2 will be dynamically evaluated as Queu_B because B is the second (2) item in the external names list.

(*) Earmarks the default value

[*] If the designated file is not found, then the program will create it.

8.3.7. Customizing PrintView via the HTML

The Agent receives the parameters from the HTML, and is customized accordingly. In turn the Agent passes the /EXTRA_PARAMS to the PrintView client.

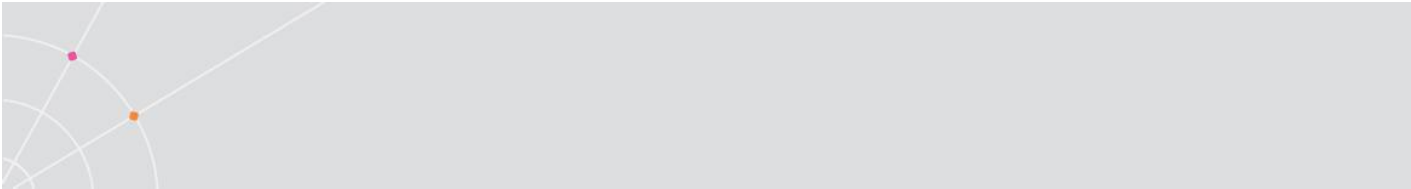Specify the parameters according to the appropriate platform. See the different examples below:

For example, you want to run PrintView client, which listens on Port 1000, and logs into a WebConnect Server with a specific username and password.

Activate using the Windows Downloader

```
<PARAM NAME="Parameters" VALUE="<WebServer> /NOSELFUPDATE
/USER=*example /PASS=example /RUN=PrintView
/EXTRA_PARAMS=/LPD_PORT=1000">
```

In this parameter string, <WebServer> is a macro that is translated by the Windows Downloader into the hostname of the Web server which provided the HTML. For details see chapter 11.

Activate using the Java Downloader

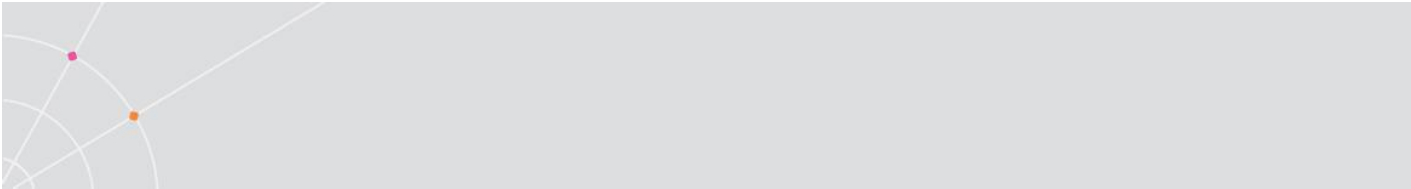Modify the value of Java Script variable **parameters** in the corresponding html file.

For Windows clients edit the file **web/windows/PrintView_J.html**. For example, to launch PowerTerm WebConnect PrintView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect server as user 'example' with password 'example' and listens on Port 1000:

```
//-------------------------------------------------
// Head Actions
//-------------------------------------------------
var component = "PrintView";
// update here
parameters =
```

```
" /NOSELFUPDATE /RUN=RemoteView " +

" /USER=*example /PASS=example " +

" EXTRA_PARAMS=/LPD_PORT=1000";

// end of update
// Identify browser

…
```

8.3.8. Customizing the Application Zone Command Line Parameters

You can customize the Application Zone to activate autologin, run a client or call for assistance.

By default the **Application login** dialog displays a checkbox for saving the credentials (the username, domain and password). This checkbox is cleared by default. However, if the user checks it, a credentials file will automatically be created in the ERICOM folder (usually in Windows `C:\Documents and Settings\<user>\Local settings\Application Data\Ericom\`). The credentials are saved in an encrypted format that is user and machine specific. Saving the credentials will allow for automatic login to the Application Zone in case there was a non-clean closure of it. Exiting the Application Zone correctly will erase the credentials unless the server configuration has been changed with **AGENT_ExitCleanMode**.

If the credentials are incorrect, the login dialog will be displayed with the current values pre-entered, and the checkbox checked. When the user clicks **Connect** and the logon to PowerTerm WebConnect succeeds, the new values will be saved to the credentials file instead of the previous outdated values. In this case, if the user clears the checkbox, the credentials file is deleted.

Right-clicking on the Agent icon in the system tray provides an option to clear the credentials file. This option is titled: "Clear Credentials". When selected this causes the password contained in the credentials file to be erased.

The following parameters can be used to customize the Application Zone either from the Command Line or via HTML:

/AUTOLOGIN=	YES – If the credential file exists, the login dialog will not be displayed at all. Otherwise the Login dialog will be displayed, but the **Save Credentials** check box will not be shown.
	NO - No autologin
	INTERACTIVE - If the credentials file exists and the

	user changed the credentials when the check box is still ON, the user will be asked whether to save the updated credential information.
	FIRST INTERACTIVE – Default. If the credential file exists, the Login dialog will not be displayed at all. Otherwise the Login dialog will be displayed and the Save Credentials check box will be shown (cleared).
	Empty, missing or invalid value - Will be treated as FIRST INTERACTIVE
/RUN= client-id	Run a certain client upon activating the Application Zone where client-id is one of
	HostView - Browser-based emulation, classic look
	PrintView - Print Server Solution over LPD protocol
	QuickVNC - Remote Desktop Connection using VNC protocol
	RemoteView - Server-based Computing using extended RDP protocol
	QuickFTP – Secure FTP client
	FTP - Secure FTP client stand-alone tool
	DFT - AS/400 (iSeries) Data File Transfer stand-alone
/EXTRA_PARAMS=	Additional command line parameters to be passed to the client being activated by the Application Zone.
/CALL_ADMIN	Requests the PowerTerm WebConnect administrator's assistance upon activating the Application Zone.
/CALL_SUPPORT	Requests the PowerTerm WebConnect tech-support's assistance upon activating the Application Zone.

(*) Earmarks the default value

[*] If the designated file is not found, then the program will create it.

8.3.9. Customizing QuickVNC Command Line Parameters

The following parameters can be used to customize the component either from the Command Line or via the HTML:

Required

The server's address and port number in the following format:

<address>:port or address:port

for example: <webserver>:4001, webserver:4001

If the port number is omitted, the default (4000) is used.

Optional

/USER= specifies the value for the User Name field. Placing an asterisk in front of the user name causes it to login immediately without displaying the login dialog.

/SID= specifies the value for the Session ID field.

/CONNECTION= specifies the predefined connection name.

8.3.10. Customizing QuickVNC via the HTML

The Agent receives the parameters from the HTML and is customized accordingly. In turn, the Agent passes the "extra-params" to the QuickVNC component.

Specify the parameters according to the appropriate platform. See the different examples below:
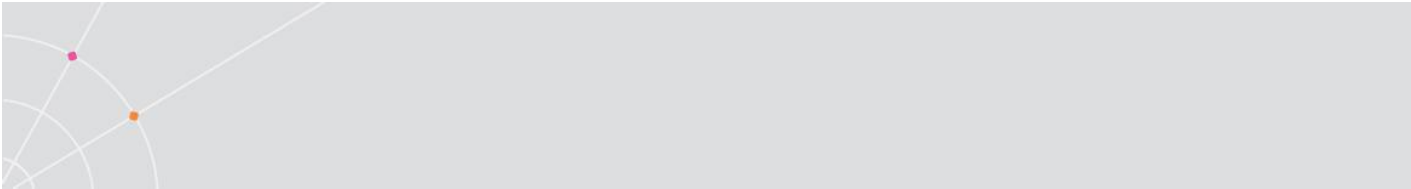
For example, you want to run QuickVNC client, which logs in to a WebConnect Server with a specific username and password and runs a specific connection.

Activate using Windows Downloader

```
<PARAM NAME="Parameters" VALUE="<WebServer> /NOSELFUPDATE
/USER=*example /PASS=example /RUN=QuickVNC
/EXTRA_PARAMS=/CONNECTION=connection">
```

Activate using Java Downloader

Modify the value of Java Script variable **parameters**'in the corresponding html file.

For Windows clients edit the file **web/windows/QuickVNC_J.html**. For example, to launch PowerTerm WebConnect PrintView client from ClientURLs.html using the Java Downloader to connect to a PowerTerm WebConnect server as user 'example' with password 'example' and run a 'VNCConnection' connection:

```
//--------------------------------------------------

// Head Actions

//--------------------------------------------------

var component = "QuickVNC";

// update here

parameters =

" /NOSELFUPDATE /RUN=RemoteView " +

" /USER=*example /PASS=example " +

" EXTRA_PARAMS=/CONNECTION=VNCConnection";

// end of update

// Identify browser

…
```

8.3.11. Modifying the Initial GUI Language in the Java Client

To modify the initial GUI language:

Open NoSSLClient.html or SecureClient.html and search for the following string:

var sParamLanguage = '<param name="lang" value="">';

In the value tag, insert another language from the list of supported languages: Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Norwegian, Polish, Portuguese, Spanish, Swedish and Turkish.

For example:

var sParamLanguage = '<param name="lang" value="German ">';

The HTML starts the PowerTerm WebConnect Client applet's GUI text in German.

NOTE On Netscape Communicator the Java client only supports English.

8.3.12. Modifying the Timezone Offset from Greenwich in the Java Client

It is necessary to set the time zone so that the proper times appear in the Printer Jobs list.

To modify the Timezone Offset:

Open NoSSLClient.html and/or SecureClient.html and search for the following string:

var sParamTimeZone = '<param name="zone" value="2">';

In the value tag write offset (in hours) of your time zone.

For example:

var sParamTimeZone = '<param name="zone" value="-5">';

The HTML starts the PowerTerm WebConnect Client applet with the −5 time zone (corresponding to United States Eastern Standard Time zone).

8.3.13. Disabling Menu Items in the Java Client

To disable menu items:

Open NoSSLClient.html and/or SecureClient.html and search for string:

```
var sParamDisableMenuItems = '<param name="disable_menu" value="">';
```

In the value tag, type sequence of numbers mapping the menu items to be disabled, separated by a comma.

Removable menu items and their numeral value:

1	New Terminal Window
2	Print Properties
3	Print Job List
4	Edit
5	Paste from Clipboard
6	Select Screen
7	Clear Screen
8	Reverse Screen
9	Send
10	Terminal Setup
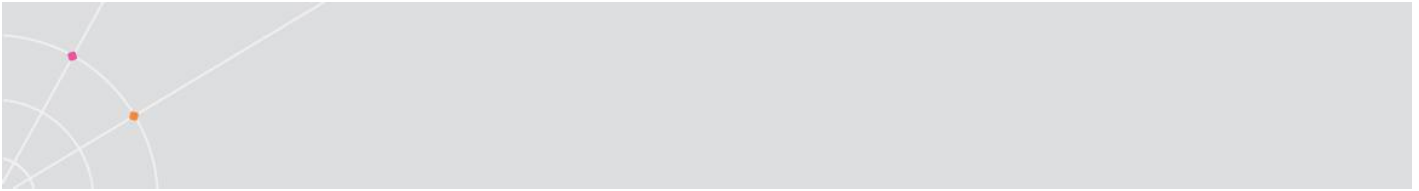
11	Change Password
12	Language
13	Time Zone Offset
14	GUI Font

Example:

```
var sParamDisableMenuItems = '<param name="disable_menu" value="1,3,5,6">';
```

The HTML starts the PowerTerm WebConnect Client applet with the following menu options removed: New Terminal Window, Print Job List, Paste from Clipboard, Select Screen.

8.4. Creating PrintView (LPD) Queues

PrintView queues can be crated in advance by the administrator and thus be provided to the user upon logging in.

To create a PrintView queue:

1. Select Files | Defaults | PtLpd.ini. The PtLpd.ini file is displayed in a text editor.

2. Copy the following lines and paste them in the adjacent area.
```
[Queue=<?PLACEHOLDER?>]
AccessFrom=
AccessMode=Unlimited
AppendFormFeed=False
Device=<default printer>
Enabled=True
EscapePrefix=
EscapeSuffix=
HoldPrinting=False
TranslateLineFeed=False
```

3. Change the user name <?PLACEHOLDER?> to the user name of your choice.

4. Select File | Save.

9. Security

An organization's server systems typically constitute the computational backbone of the organization. Thus, an effective server access solution must provide the appropriate capabilities to ensure that the security of these systems is not compromised. This is especially important when access to these systems is extended beyond the local network to the entire intranet, and even the extranet. PowerTerm WebConnect provides these capabilities by enabling you to configure global security policies and settings, as well as enabling you to configure clients according to the specific needs of the users.

9.1. Security Levels
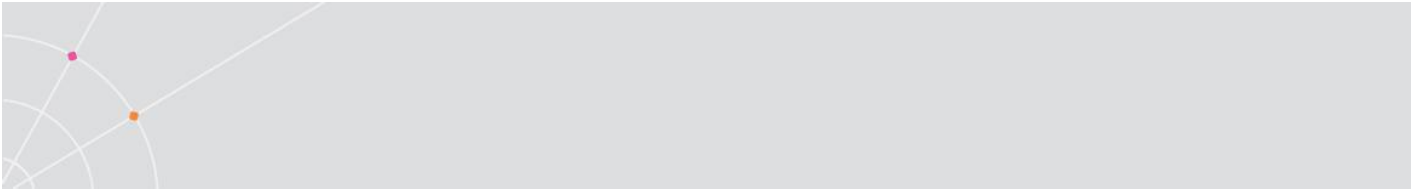
PowerTerm WebConnect uses Secure Socket Layer (SSL) for establishing secure communication between the PowerTerm WebConnect server and the clients.

WebConnect supports three levels of communication security:

- Unsecured (No SSL)
  Communication between the server and the client is not secured by WebConnect. Telnet communication in Gateway mode, for example, is transmitted as clear text, including such information as user names and passwords.

- Encryption without Authentication (Anonymous SSL)
  SSL is used for encryption only. The client cannot verify the WebConnect server's identify. This is the default security level used by 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 establish this level of operation a pair of files, certificate and primary key, must be placed on the server. The client will access a copy of the certificate through the 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 WebConnect server and saved on the client's machine upon receiving confirmation from the end-user.

To see the communication security level, open the client's About dialog. The security level is indicated in the dialog's lower left-hand corner.

- Anonymous SSL

- SSL with Server Certificate

- Absence of any of the indicators signifies that the communication is not secured.

> NOTE The security level of the communication between the PowerTerm WebConnect server and clients, does not effect the security of direct connections between clients and hosts. These can be secured or unsecured regardless of the security level used.

9.1.1. Setting No SSL Security Level

Steps must be taken on both the client and server side to ensure the desired security level.

Client side

Modify the parameter on the command line with the following switch: /NOSSL

> NOTE For clients that are activated by a Web page, modify the command-line value specified as a parameter to the Downloader component. For clients that are activated using a Desktop shortcut, modify the command-line value in the shortcut's properties.

Server side

Locate the ConnectionPoint heading in the PtServer.ini file.

Modify the parameter to be: SSL_Required=False. This will allow the server to accept unsecured client connections.

Result

On the client side, the absence of any icon in the lower left hand side of the client's About dialog indicates that no SSL exists.

9.1.2. Setting Anonymous SSL Security Level

Steps must be taken on both the client and server side to ensure the desired security level.

Client side

Modify the parameter on the command line with the following switch:

/SSL

> NOTE For clients that are activated by a Web page, modify the command-line value specified as a parameter to the Downloader component. For clients that are activated using a Desktop shortcut, modify the command-line value in the shortcut's properties.

Server side

Verify that the pair of files PTS.crt and PTS.key is not found in the same folder as PtServer.exe. If they are situated in the same folder, the server will use them for authentication. If they are not found in that folder, the server will use anonymous SSL.

If you want to allow only secured client connections, make sure to set the following parameter in the PtServer.ini file:

SSL_Required=True

Result

On the client side, the following icon appears in the lower left hand side of the client's About dialog:

- (Anonymous SSL)

- Absence of any icon indicates that unsecured communication is used.

9.1.3. Setting SSL with Certificate Security Level

Steps must be taken on both the client and server side to ensure the desired security level.

Client side

Modify the command line parameter: /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 specified as follows:

/SSLCERTFILE=filename or /SSLCERTPATH=path

> NOTE   The certificate path is not searched recursively.

Multiple certificates

Both command line parameters can reference multiple files or paths:

/SSLCERTFILE="file1;file2;file3"

/SSLCERTPATH="path1;path2;path3"

> For clients that are activated by a Web page, modify the command-line value specified as a parameter to the Downloader component. For clients that are activated using a Desktop shortcut, modify the command-line value in the shortcut's properties.

Server side

The pair of files PTS.crt and PTS.key must be located in the same folder as PtServer.exe.

If you want to allow only secured client connections, make sure to set the following parameter in the PtServer.ini file:

SSL_Required=True

> NOTE The first time the above files are placed in the server's folder and every subsequent time that these files are replaced, the server must be restarted.

By default, if the server's certificate does not match a certificate file referenced by /SSLCERTFILE, or is not located in a directory referenced by /SSLCERTPATH, the connection is rejected. For non-Java clients, this behavior can be overridden by placing an asterisk "*" in front of the certificate file name, or directory path. In such a 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 using that file name, or to that directory, 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 because 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

For example:

steven= 127.0.3.37-4000.crt

Ericom-folder is a private-per-user folder. It is located under the user's "profile". In Windows NT, 2000, 2003, XP this folder is typically:

C:/Documents and Settings /User-Account-Name/Application Data/Ericom
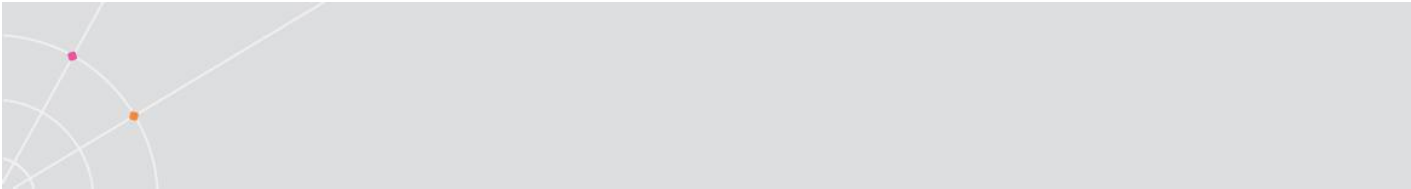
Important Recommendation from Ericom

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
```

For example:

```
https://www.customer.com/WebConnect5.1/server.crt
```

This https path is also the default certificate path for the JAVA client.

Result

On the client side, the icon appears in lower left hand side of the client's About dialog.

9.2. SSL with Server Certificate (Administrative Workaround)

A special option exists for the Administrator in the Connect dialog that allows the Administrator to connect to a server without a certificate. A dialog appears specifying the file path of the certificate for which the program searched and failed to find. It also states the name of the server's certificate.

The administrator can then choose one of the following options:

- Reject this certificate.

- Accept this certificate.

- Accept and Save this certificate to the specified server location.

9.3. SSL Security Level Negotiation

The following workflow diagram of the SSL Security Level Negotiation makes a rather complicated process easier to understand:

Security Level Negotiation
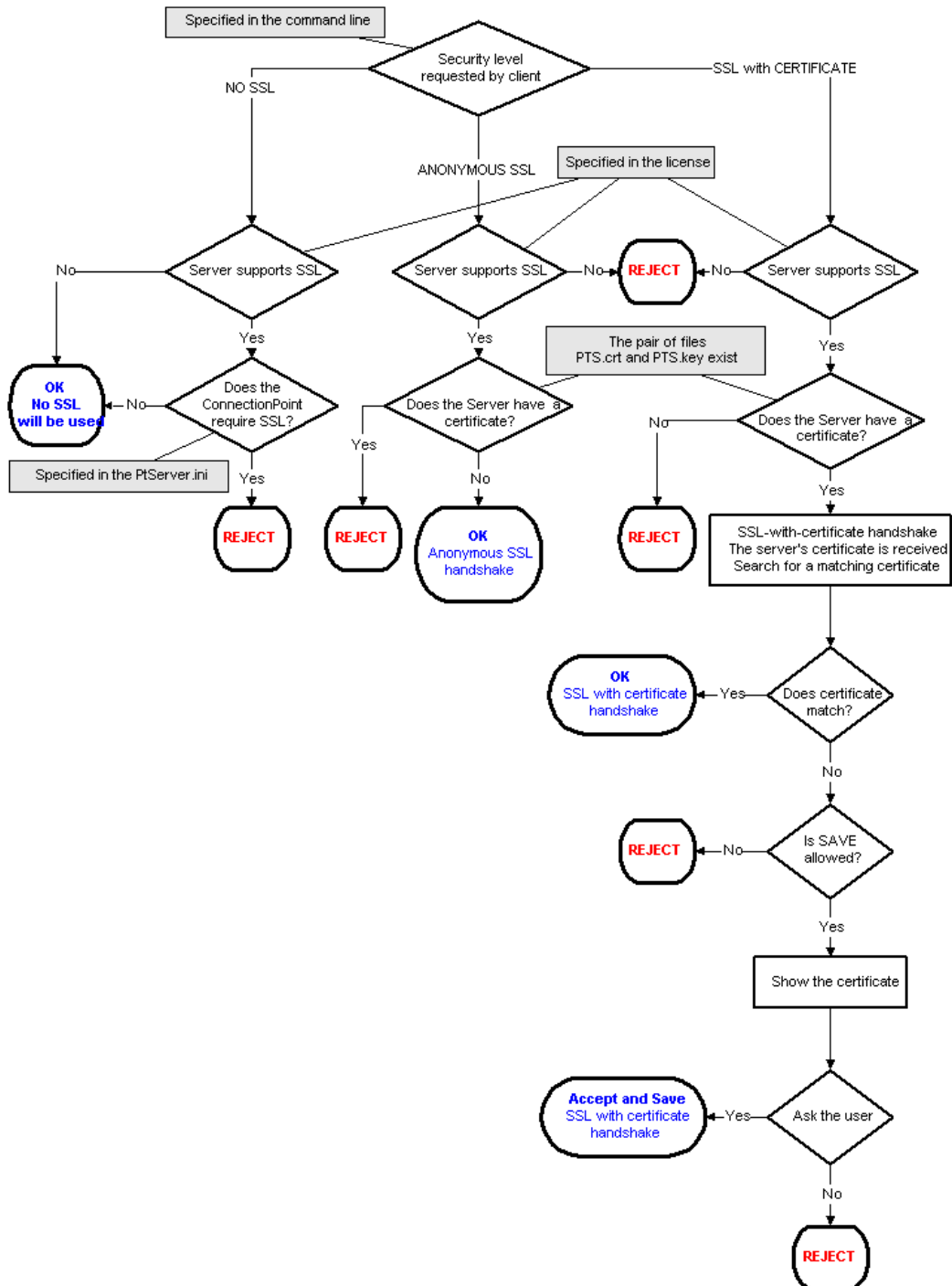
10. Authentication Methods

PowerTerm WebConnect provides single-factor-authentication based on user credentials that are stored 'built-in' in PowerTerm WebConnect Server or reside on the organization's Directory Server database.

By integrating with either RSA SecurID or Radius protocols, this solution is enhanced with two-factor-authentication.

You need to set PowerTerm WebConnect Server in the PtServer.ini configuration file, in the **Connection Point** section. The parameter is **AuthenticationMethod** and can have one of three values:

- **Regular**, single-factor-authentication based on the user's credentials in PowerTerm WebConnect Server database or Directory Server database.

- **RsaSecurID**, two-factor-authentication using the RSA SecureID protocol.

- **Radius**, two-factor-authentication using the Radius protocol.

To synchronize the user's name between the two-factor-authentication server and the user database, the parameter **Use_userPrincipalName** should be set to **True** or **False** (default), where True gives the user's full name, i.e. user name including location.

For example, if **Use_userPrincipalName** is set to False, the user "*name@company.local*" will be authenticated with "*name*".

Setting the credentials

When RSA SecureID, Radius and SSO are used to authenticate user credentials in the LDAP server, PowerTerm WebConnect does not receive the password from the user. However, it needs to find the user path in the LDAP server and to obtain all user data (e.g. path, groups that the user is a member of). In this case, PowerTerm WebConnect Server connects to the LDAP server according to the credential settings.

The credentials settings are specified in PowerTerm WebConnect Administration Tool, in the Directory Services Properties dialog:
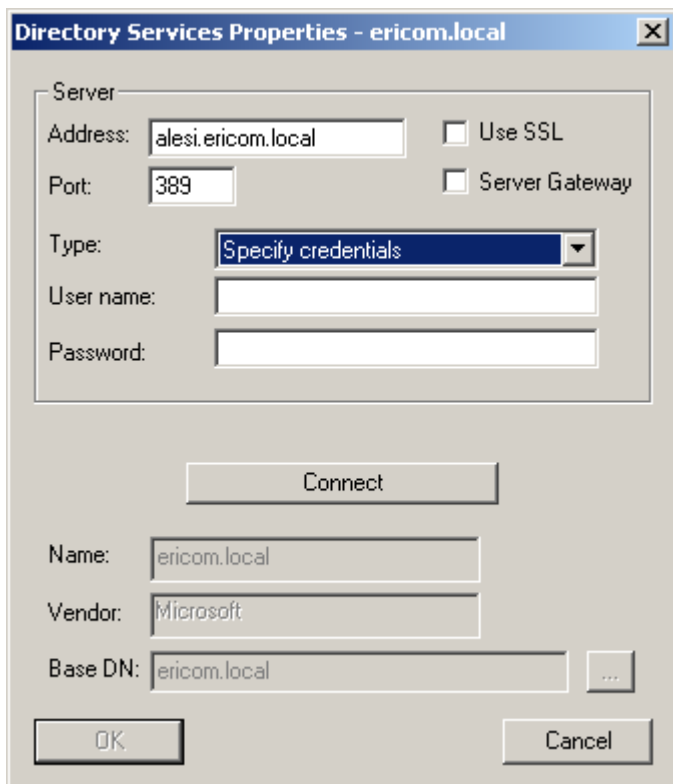
For more information about Directory Services, please see chapter 4.

You have to specify **Type** to match the LDAP server configuration:

- **Specify credentials** – recommended

- **Windows authentication (Kerberos)**, will only work on Windows Directory Services if PowerTerm WebConnect Server runs as a user account.

- **Anonymous**, will work for Novell eDirectory.

10.1. RSA SecureID

In RSA SecureID, the client connects to the PowerTerm WebConnect server and transmits the user's ID and PIN. The client communication is encrypted using SSL. PowerTerm WebConnect server then transmits the User ID and PIN to the RSA Authentication server for authentication. After authentication is completed, PowerTerm WebConnect connects the client to the target system, either a Legacy host or a Terminal server.

WebConnect RSA Architecture
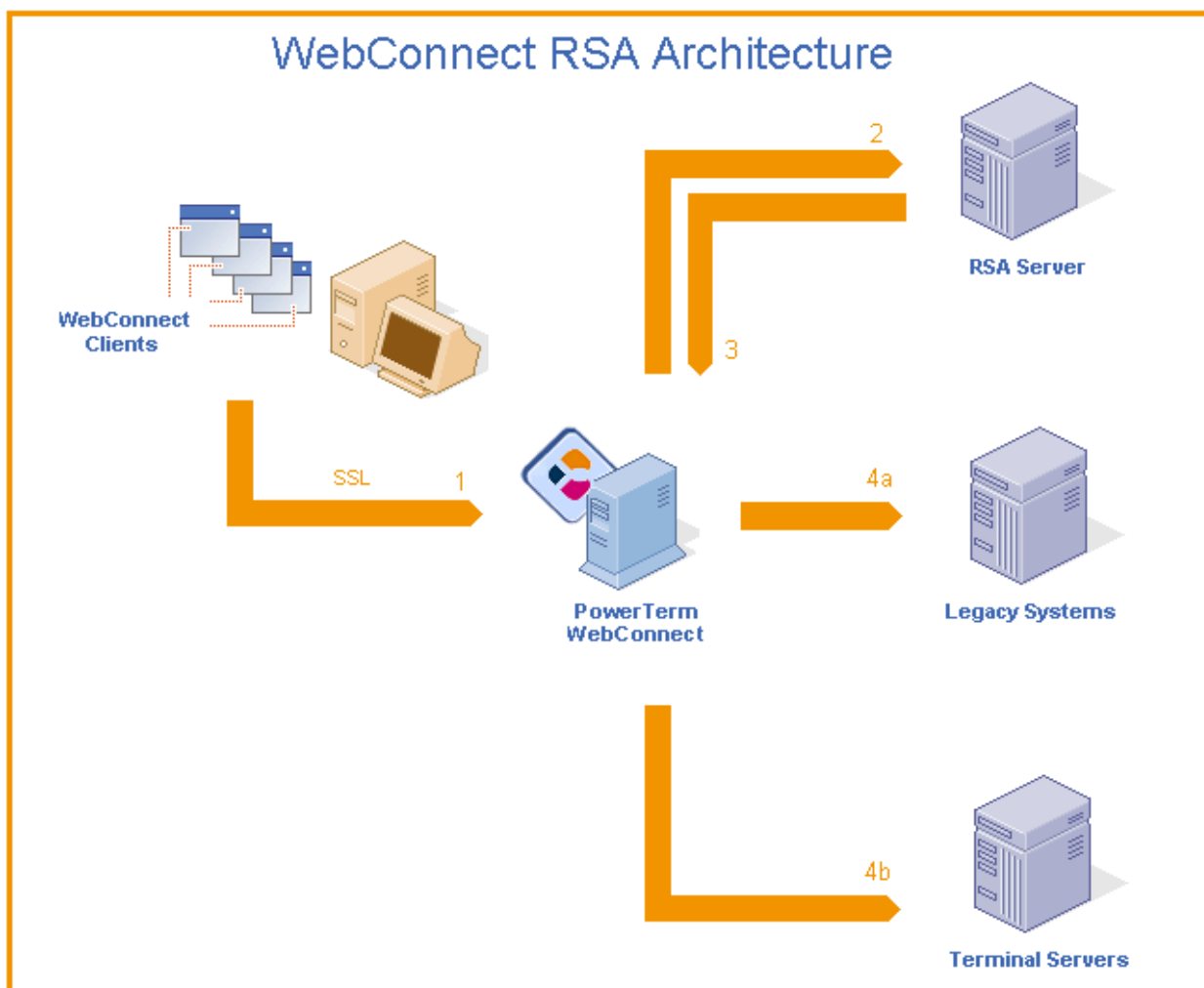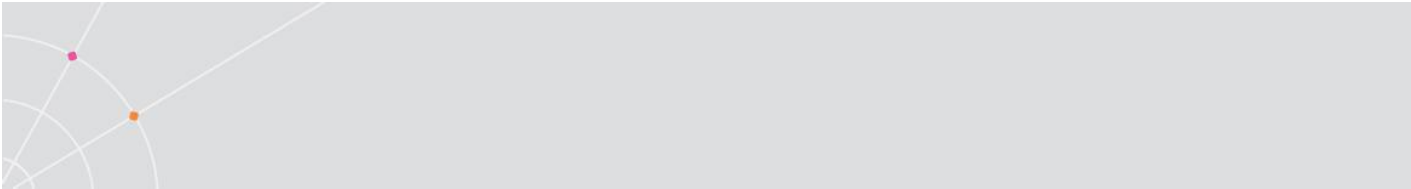
10.1.1. Agent Host Configuration

To facilitate communication between the PowerTerm WebConnect and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the PowerTerm WebConnect within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Host name of PowerTerm WebConnect Server

- IP Addresses of PowerTerm WebConnect Server

When adding the Agent Host Record, you should configure the PowerTerm WebConnect as Net OS. This setting is used by the RSA Authentication Manager to determine how communication with the PowerTerm WebConnect will occur.

NOTE   Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

10.1.2. Authentication Agent Configuration

1. **For Windows:**
   Copy **sdconf.rec** that was generated by the RSA Authentication Manager to windows/system32
   For Linux:
   Verify that an ACE folder exists.
   Copy **sdconf.rec** that was generated by the RSA Authentication Manager to /var/ace

2. Install PowerTerm WebConnect Server 5.6

3. Create a new user in PowerTerm WebConnect:
   Launch the PowerTerm WebConnect Administration Tool
   Select Action | New | User… - the Add User dialog appears:

Fill the user properties:

Type the user name in the "User Name" field.

Click on the Password button, the Set Password dialog appears, press OK

Check the "Allow Concurrent Machine".

Select the "Unlimited" option in the "Access Limit Mode" field.

4. Configure PowerTerm WebConnect to authenticate to RSA Authentication Manager:

Launch the PowerTerm WebConnect Administration Tool.

Open PtServer.ini - Select Files | Configurations | Main.

In the **[ConnectionPoint=Internet]** section set the option **AuthenticationMethod=RsaSecurID**. This setting specifies that all client sessions on the PowerTerm WebConnect default port (port 4000) will be authenticated with RSA SecurID.

The Login Screen:
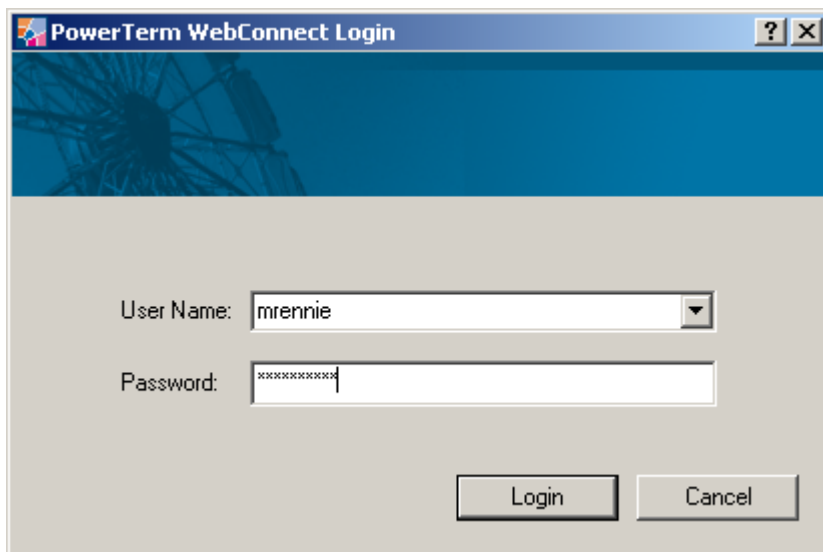
How does it work?

For a new user:

The user types the user name in the User Name field and the token code in the Password field and gets a dialog box depend on the settings in server:

The user required to create a PIN:
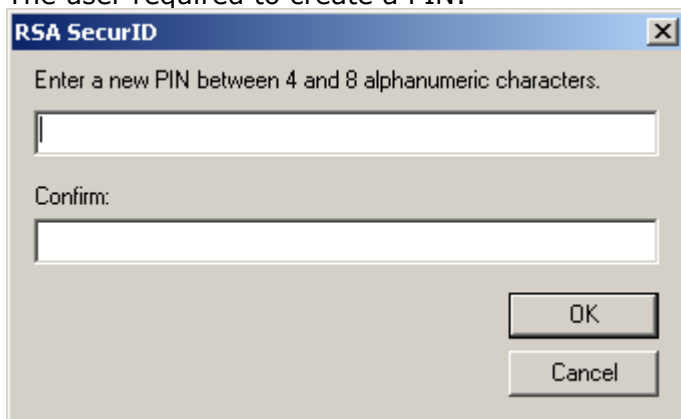
If no PIN was entered:
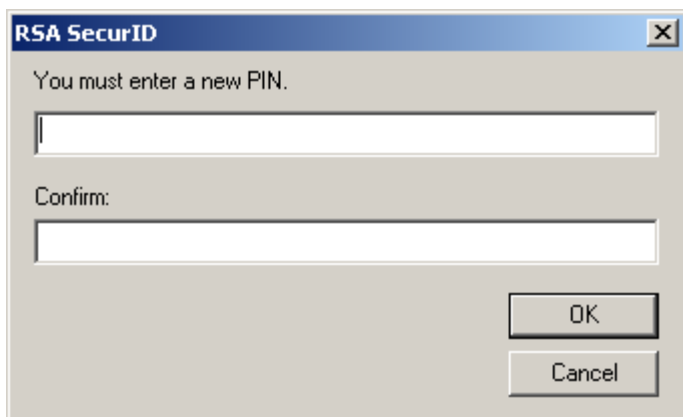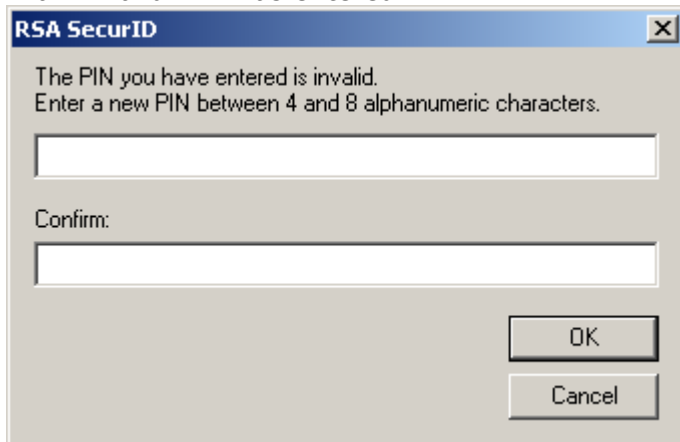
The user allowed to create a PIN:
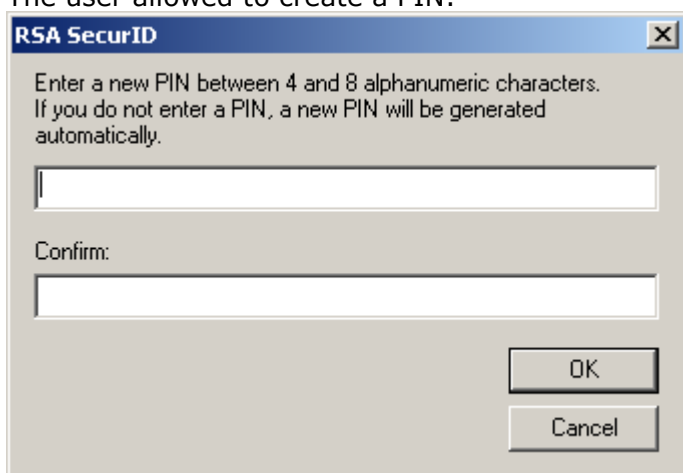
The system generated a PIN or - The user allowed to create a PIN and pressed the OK button:

If an invalid PIN was entered:

For an existing user:
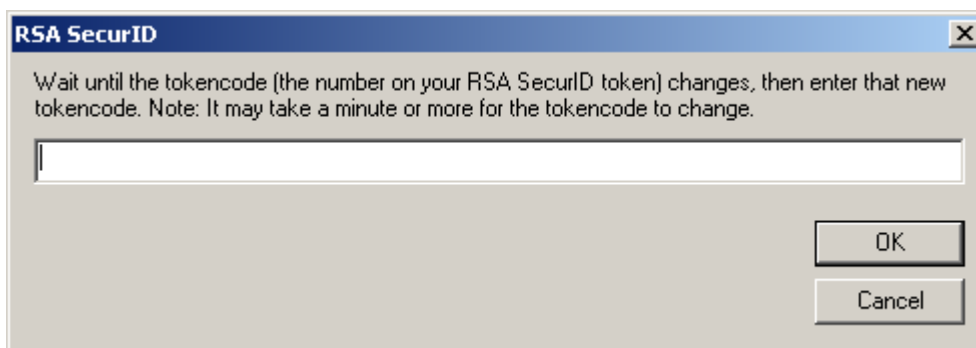
The user gets the Login dialog and types the user name in the User Name field (usually already appears) and the pass code (PIN + token code) in the Password field.

When the PIN has expired:

The user gets a dialog box depend on the settings in server as described in a new user.

If the token code has been changed

The user types the user name in the User Name field and the pass code (PIN + token code) in the Password field and gets a dialog:

The user gets the Login dialog again with the user name in the User Name field, and now types the PASSCODE (PIN + next token code) in the Password field.

10.2. Radius

To use the Radius protocol for two-factor-authentication you have to set **AuthenticationMethod=Radius** in PtServer.ini. You also have to set the following parameters:

- **Radius_server**, the IP or the hostname of the Radius server.

- **Radius_port**, the (UDP) port that the Radius server is listening on. Default: 1812

- **Radius_sec_timeout**, the timeout to wait for response from the Radius server. Default: 2

- **Radius_retries,** the number of times to retry to send the authentication request if a timeout occur. Default: 3

- **Radius_secret**, the Radius server's **secret** password.

NOTE   PowerTerm WebConnect Server supports only one Radius server at any given time.

11. Downloading and Installing Clients

A primary feature of PowerTerm WebConnect is its ability to remotely install and update clients. The initial client download and installation is usually invoked via the browser, and includes the following steps:

1. The user visits a Web site that includes links to activate PowerTerm WebConnect connections.

2. The user selects a desired link.

3. If this is the first time the user activates the client associated with the requested connection, the client is downloaded and installed.

4. The client is activated and establishes the requested connection.

Once a client is installed, it can be activated again automatically through a Web page, skipping the download and installation steps. Alternatively, the administrator or the user can create a desktop link for direct activation of the client.
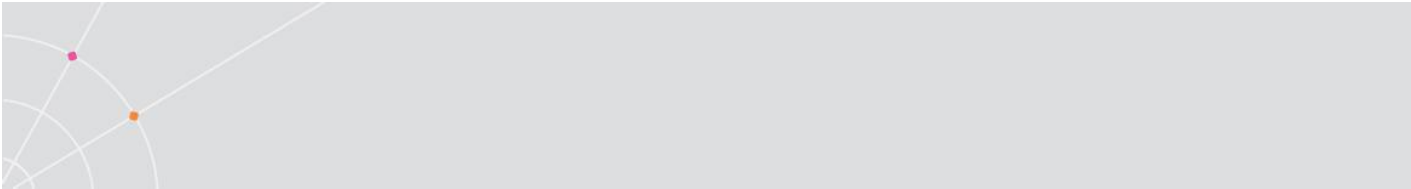
In order to minimize the download size, PowerTerm WebConnect clients only download those components that are essential for their operation. Additional components are downloaded automatically if and when they are required. For example, the online help is usually downloaded the first time it is requested. In addition, all PowerTerm WebConnect components are downloaded in a compressed format (CAB or ZIP).

PowerTerm WebConnect clients also have a self-update capability: whenever a PowerTerm WebConnect client is activated, it verifies via the server whether a newer version of itself exists. If such a version is available, the client automatically downloads the latest version and installs it, and then restarts itself. This guarantees that the clients are always updated.

NOTE   In previous PowerTerm WebConnect versions, most clients were registered as ActiveX (COM) controls on the user's computer. This is no longer the case. Instead the clients are activated as standard processes. An exception is PowerTerm WebConnect WebView (previously OCX), which is still installed and activated as an ActiveX control. For backward compatibility reasons, other clients can be activated as ActiveX Controls as well, but this requires manual customization of the Web pages used for client activation.

11.1. Activating a Client from a Browser

As explained above, the initial installation of PowerTerm WebConnect clients is usually initiated by a Web browser. PowerTerm WebConnect provides two primary methods for downloading and installing clients from the Web: using Microsoft ActiveX (COM) and

using a Java applet. A third mechanism, using Mozilla XPI, is also available for some clients.

Using ActiveX for downloading and installing clients is the preferred method when:

- The user's operating system is Windows.

- The user's browser is Internet Explorer or some other ActiveX compatible browser.

- The user's security settings enable the use of signed ActiveX components.

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

- The HTML used for activating the download and installation can be very concise and simple.

- Minimal download size.

- Does not require any external components beyond the browser itself (such as the JVM).

- Provides the greatest control over the download destination.

- Provides a high level of interaction between scripts hosted on the Web page and the download and installation process.

Using a Java applet for downloading and installing clients is the preferred method when:
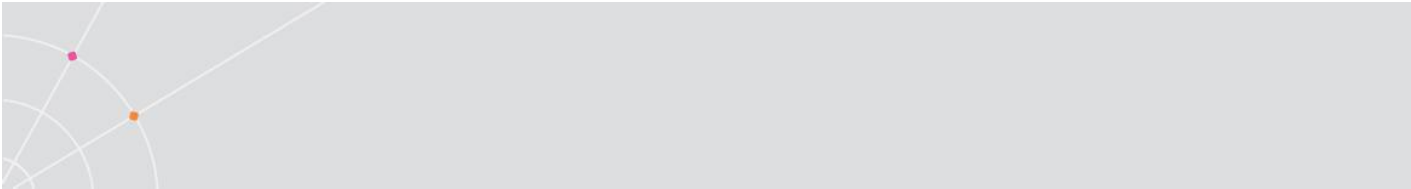
- The user's operating system is not Windows, e.g. Linux.

- The user's browser does not support ActiveX, but does support Java applets.

- The user's security settings prevent the use of any ActiveX, but do allow signed Java applets to run.

The advantages of using a Java applet for downloading and installing PowerTerm WebConnect clients are:

- Cross-platform

- Cross-browser

- Works when security settings do not allow ActiveX.

NOTE   For the Java applet to work, the JVM must be installed on the user's computer.

Both the ActiveX and Java applet do not directly activate the requested client. Instead, they activate the PowerTerm WebConnect Agent and instruct it which client to activate. It is the PowerTerm WebConnect Agent that performs the actual download, installation and activation of the requested client. As a result, the client activation process follows these steps:

1. If not installed on the user's computer, the downloading component is downloaded and installed by the browser.

2. The component is activated by the browser.

3. The component searches for the PowerTerm WebConnect Agent in the destination directory.

4. If the PowerTerm WebConnect Agent is not found, it is downloaded and installed from the Web server.

5. The PowerTerm WebConnect Agent is activated with command-line arguments that instruct it which client to activate.

6. The PowerTerm WebConnect Agent connects to the PowerTerm WebConnect server. This operation may require the user to fill in a login dialog.

7. The PowerTerm WebConnect Agent searches for the requested client in the same directory where it is installed.

8. If the requested client is not found, it is downloaded and installed by the PowerTerm WebConnect Agent from the PowerTerm WebConnect server.

9. The client is activated with command-line arguments that instruct it as to what action to perform, e.g. establish a specific connection.

10. The user need not login again into PowerTerm WebConnect when the client is activated because login was successfully accomplished by the PowerTerm WebConnect Agent.
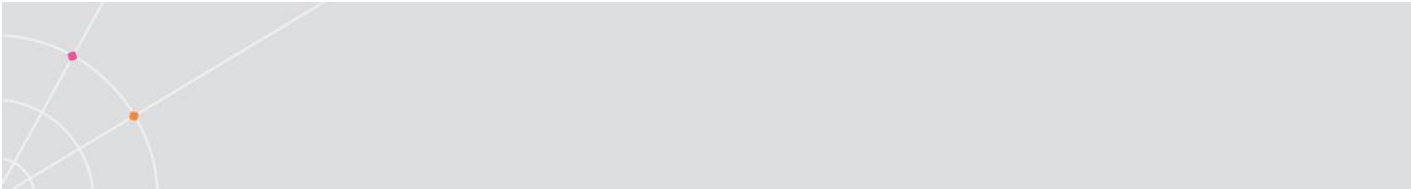
NOTE   The download and installation of PowerTerm WebConnect WebView does not utilize the PowerTerm WebConnect Agent. Instead it is downloaded, installed and activated directly by the ActiveX download component.

11.1.1. Windows Downloader

The ActiveX download component is referred to as the Windows Downloader, although the Java download component can also be used on Windows. The Windows Downloader can only be activated by a browser that is compatible with Windows technology, such as Microsoft Internet Explorer, because it is an ActiveX component. It is an extremely lightweight component: packaged as a CAB it is only 51K bytes. The component itself 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, and similarly from the command prompt (see below).

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 authorize the component's installation. To circumvent this message, place the Web server (from which the Windows Downloader will be downloaded) in the browser's "Trusted sites" security zone. Alternatively, the user can select always trust content from Ericom Software. Once selected, the certificate will not be shown again, even if updates are downloaded.

The Windows Downloader provides the following features:

- Displays a clear download progress indicator, showing the name and version of the component being downloaded, a progress bar, component's total size and portion downloaded, and an estimate of the remaining download time.

- A Cancel button for terminating the download.

- Configurable download destination.

- It will continue to download and install even if a user closes the browser.

- Security notice is presented only once – the same Windows Downloader can download multiple client types.

- Once installed, it can download components to locked systems (those which require write access to download destination).

- Supports side-by-side installation of multiple client versions.

- Revert to old client versions, if necessary.

- Error messages and an optional log to help analyze failed installations.

The Windows Downloader does not connect to the PowerTerm WebConnect server, and thus does not require the user to login. It connects and downloads components from any standard Web server or FTP server. It can also copy components from a specified file path.

Downloadable Packages

For a component to be downloaded by the Windows Downloader, it must be packaged in a specific format:

- A CAB file containing all the files that need to be installed on the target computer.

- A Version file specifying the version information of the component.

- An optional installer inside the CAB.

- An optional executable inside the CAB.

The PowerTerm WebConnect installer places two such components on the Web server:

- The PowerTerm WebConnect Agent, which is used to download and activate all the other clients, as explained above.

- PowerTerm WebConnect WebView, which is invoked directly by the Windows Downloader.

The version file is a text file that has a .ver.txt extension. It must have the same name as the CAB file, and be placed in the same directory on the server. The version file contains the display name of the component, its version number, and the preferred installation destination. The Downloader will not perform the client download if the version file is missing, inaccessible or corrupt. For example, the contents of the version file for the PowerTerm WebConnect Agent:

`5.1.0.90`

PowerTerm WebConnect Agent

`5.1.0 Build 90`

<root>/PowerTerm WebConnect 5.1/<WebServer<

> NOTE The version files are provided by Ericom Software as a part of the PowerTerm WebConnect installation. Do not modify these files since any modifications you make will be overwritten when a newer version of PowerTerm WebConnect is received from Ericom Software. Instead, you can override some of the values, such as the download destination, using properties in the HTML.

Activating the Windows Downloader

The Windows Downloader is activated by the browser when the appropriate <OBJECT> tag is embedded in the HTML:

<OBJECT ID=Downloader WIDTH=0 HEIGHT=0 STYLE="DISPLAY:none"
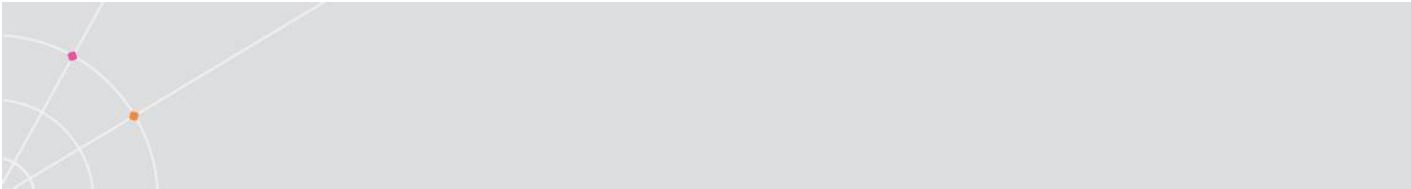
CODEBASE="ptdownloader.cab"

CLASSID="CLSID:7EC816D4-6FC3-4C58-A7DA-A770EE461602">

The <OBJECT> tag instructs the browser to activate an ActiveX component whose GUID is specified in the CLASSID attribute. If that component is not installed, the browser can download and install it automatically if a source location for the download is specified by the CODEBASE attribute. For more details on the use of the <OBJECT> tag, see the relevant documentation at http://msdn.microsoft.com.

The Windows Downloader does not display anything inside the browser window itself. As a result, its width and height are usually set to zero, and its style is set to hidden.

The Windows Downloader implements a collection of properties that can be used to control its operation. The values of these properties can be specified using the <PARAM>

tag, or using JavaScript. For example, use the Src property to specify the source location of the PowerTerm WebConnect client to download:

<OBJECT ID=Downloader WIDTH=0 HEIGHT=0 STYLE="DISPLAY:none"

CODEBASE="ptdownloader.cab"

CLASSID="CLSID:7EC816D4-6FC3-4C58-A7DA-A770EE461602">

<PARAM NAME="Src" VALUE="ptagent.cab">

...

</OBJECT>

By default, the Windows Downloader will initiate the download and installation process immediately when the browser activates it. This behavior can be altered by setting the value of the AutoActivate property to 0.

NOTE   For examples of how to use the Windows Downloader, see the HTML files whose names end with _X in the web/windows directory, e.g. HostView_X.html.

The property values can also be set by JavaScript code. This method is more complex but offers a greater degree of flexibility. For an example of how to use JavaScript with the Windows Downloader, see WebView_X.html in the web/windows directory. For example, to specify the source location using JavaScript:

Downloader.Src ="ptagent.cab";

Client Download and Installation

The first time Windows Downloader is activated to download and install a specific client, it performs the following operations:

Using the value of the Src property, it determines the online location of the client to download.
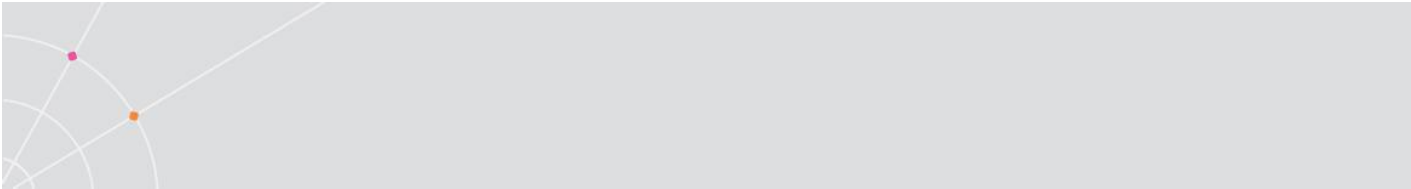
It downloads and parses the version information from the online version file.

It downloads the CAB file containing the client. During this operation, it displays the client name and version retrieved from the version file.

The CAB file is written to a local directory specified by the Dst property. If this directory does not exist, it is created.

The contents of the CAB file are extracted to the same directory.

If the CAB file contains an installation program, the program is activated to perform the client installation.

If the CAB file contains an executable with the same name as the CAB file, this executable is assumed to be the client and is launched with the command-line arguments specified by the Parameters property.

A copy of the version file is written to the same directory.

If, at any step of the process, the download and installation fails or is aborted, the subsequent steps are not performed. The version file is written (step 8) only if the entire process was successful. If the CAB file does not contain an installation program (step 6) or an executable (step 7), these actions are skipped, but the process is still considered successful. The Windows Downloader does not perform cleanup operations, e.g. the destination directory is not removed in the case of a failed installation.

NOTE   The CAB file is not erased after its contents are extracted. Instead it remains on the disk unless it is explicitly erased by the client's installation program.

In subsequent activations of the Windows Downloader, the destination directory already exists and contains both the client and a copy of the version file. For this reason, Windows Downloader first searches for an existing local copy of the version file in the destination folder before initiating the client download and installation process. If the local version file exists, the numbers of the versions in the local and remote files are compared. The download and installation process is initiated only if the version in the remote file is newer than the local file. If the version in the local file is the same or higher than the remote file, Windows Downloader skips directly to step 7 and attempts to launch the local executable.

Client Installer

Some clients require custom installation operations to take place in order for them to be usable. For example, PowerTerm WebConnect WebView is itself an ActiveX (COM) Control, and needs to be registered on the local computer in order to work. Custom installation operations are achieved by packaging a client-specific installation program inside the client's CAB file. Windows Downloader looks for one of the following files in the following order:

1. Install.exe

2. Setup32.exe

3. Setup.exe

Windows Downloader activates the first of these three that it locates, and waits for it to complete before continuing with the client activation process.

If the installation program activated is Install.exe, Windows Downloader inspects the program's return value. If Install.exe returns a negative value, the installation is assumed to have failed, and Windows Downloader aborts with the appropriate message.

Windows Downloader Properties

Windows Downloader implements a set of properties whose values control its behavior. As shown above, the values of these properties can be set using the <PARAM> tag, or using a script. When using a script, it is also possible to retrieve the values of these properties. In addition, Windows Downloader implements several properties whose value can only be retrieved — not set. These properties are used to indicate the dynamic state of the Windows Downloader, and are only usable from within a script.
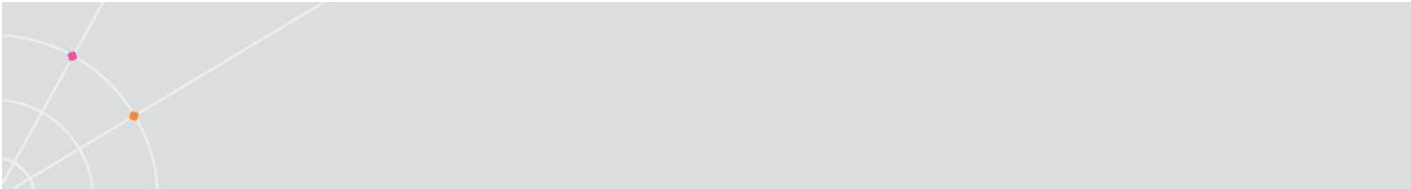
The following table lists all the Windows Downloader properties, and indicates if their value can be set:

Property name	Can be set	Description
Src	Yes	Specifies the source for the download (the URL to the CAB file). Can be a relative URL, in which case it is relative to the browser's base URL.
HREF	No	The full (absolute) URL to the CAB.
Dst	Yes	Specifies the destination (local) directory for the download. Overrides destination settings in the version file. Can contain macros as described below.
Parameters	Yes	Command-line arguments to the client executable. Can contain macros.
Modal	Yes	A Boolean property specifying whether Windows Downloader dialogs must be closed prior to viewing the browser window. Default: False.
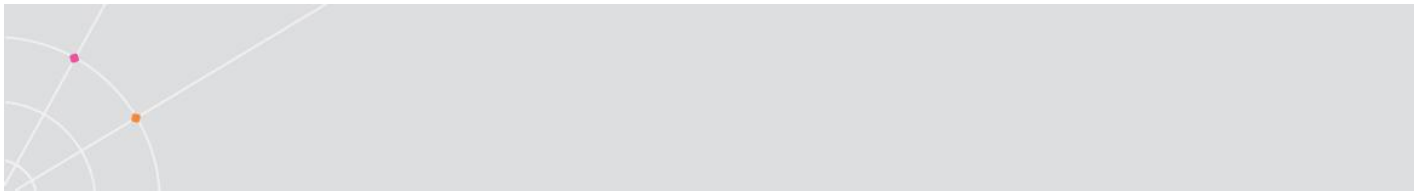
State	No	A numeric property representing the current state of Windows Downloader.
OnStateChange	Yes	Set a script callback to be activated when the Windows Downloader's state changes.
Log	Yes	Specifies the full path to a log file for logging Windows Downloader events. If set to empty string, no logging is performed. Default: empty string.
AutoActivate	Yes	A Boolean property specifying whether to initiate the activation process immediately (TRUE), or whether to wait for an explicit invocation of the Activate method (FALSE). Default: False.
Locked	Yes	A Boolean property specifying whether to prohibit a client download even if the remote version is newer than the local version. If set to TRUE, the local old version will be used instead of downloading the new version. Default: False.

When using the <PARAM> tag to set property values, use the value "0" to indicate a FALSE Boolean value, and "1" to indicate a TRUE Boolean value. In JavaScript, use the reserved words false and true, respectively.

In some cases you may be required to place double-quotes in a property value. This can be problematic because the double-quote is also used as the value terminator. To overcome this limitation:

- When using the <PARAM> tag, represent the double-quote using a "

- When using JavaScript, either use single-quotes to surround the string, or represent the double-quote value as \" (backslash followed by a double-quote).

Windows Downloader also implements a single method: Activate. This method initiates the client activation process based on the current property values. This method is useful in two cases:
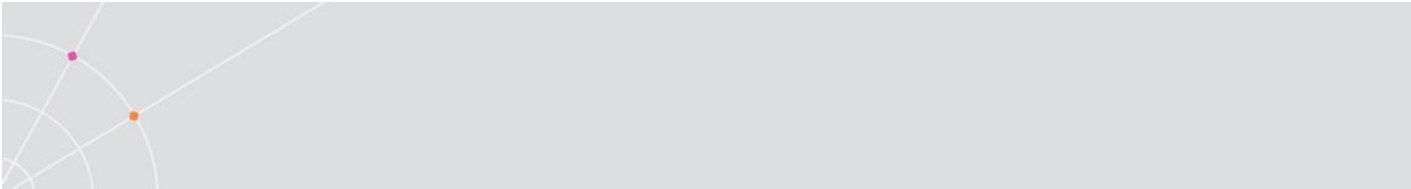
- AutoActivate is set to FALSE in order for activation not to take place until Activate is invoked.

- The same Web page is used to activate multiple PowerTerm WebConnect clients by loading different values into the properties and invoking Activate iteratively.

Managing Windows Downloader State

As explained in the previous section, Windows Downloader provides a read-only State property that contains the current state of the activation process. The State values are represented as numeric constants, as detailed in the following table:

State	Description
-1	Failure during client download or installation.
0	Not started. The initial state before any operation takes place.
1	Downloading remote version and comparing to local version.
2	Downloading and installing client.
3	Download and installation of this client is already in progress by another instance of Windows Downloader on this computer -> aborting.
4	Done successfully.
5	Download and installation cancelled by the user.

Any negative value of the State property should be considered failure.

Unless the AutoActivate property is set to FALSE, Windows Downloader will immediately change from state 0 to state 1. If AutoActivate is set to FALSE, this transition will occur when the Activate method is invoked. It is also possible to use the same Windows Downloader instance to download multiple clients, in which case Windows Downloader will reiterate through these states.

In some cases it may be desirable to associate a script in the HTML with specific States. For example, successful client activation may close the Web page because it is no longer required. Conversely, failed activation may redirect the user to a page at which assistance can be requested. The Windows Downloader makes it possible to assign a JavaScript function to be activated when its State changes using the OnStateChange property, for example:

```
Downloader.OnStateChange = function() {

    alert(Downloader.State);

};
```

This code will display the current State whenever it changes. For a more complete example, see WebView_X.html in the web/windows directory.
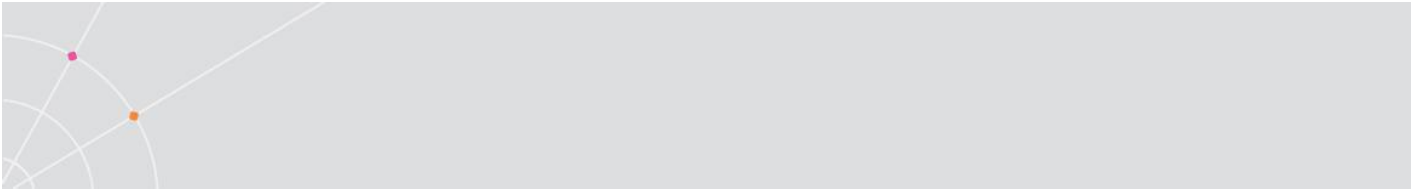
NOTE   Do not confuse the State property with the stock property readyState. The Windows Downloader provides the readyState property as well as the OnReadyStateChange notification. However, readyState transitions from 0 to 4 as soon as the Windows Downloader is loaded, before it performs any operations.

NOTE   In some cases it may be desirable to receive a JavaScript notification if the browser fails to activate the Windows Downloader itself (for example, due to security restrictions). In order to receive such a notification, place an onerror event handler on the <OBJECT> tag itself.

Windows Downloader Macros

The Windows Downloader Dst and Parameters properties, as well as the version file itself, can contain macros whose values are computed by the Windows Downloader at runtime. Macros are useful because they enable dynamic values even if <PARAM> tags are used to specify values (instead of the more complicated and error-prone JavaScript). In addition, some macros are translated to values that are inaccessible from within HTML.

Macros are placed in the property's value string surrounding their name in < and >, for example <WebServer>. Internally, when using the property's value, Windows Downloader substitutes the entire expression with the macro's value. If the macro name is not recognized by Windows Downloader, it inspects the Windows environment variables so the macro <Path> will be replaced by the user's path value. If the name does not appear in the environment table either, it is discarded (the macro is replaced with an empty string).

NOTE   Macro names are non-case sensitive.

The following table lists the macros supported by Windows Downloader:

Macro name	Description
WebServer	The name of the Web server from the HTML page's based address. Same value as the window.location.hostname HTML property.
Name	The name of the client's CAB file, e.g. "ptagent".
Display	The client's display name from the version file.
Version	The client's version value from the version file.
OSDir	Windows' installation directory, e.g. "C:\Windows".
OSDrive	Window's installation drive, e.g. "C:".
Root	Same value as OSDrive.
Home	The "Ericom" directory under the user's private "Application Data" folder.
Common	The "Ericom" directory under the common "Application Data" folder.

In order to place the < >character itself in the property value, i.e. not have it interpreted as a macro, then precede it with the percent symbol %. In order to place the percent symbol in the property value, use consecutive instances: %%.

URL Files

At the end of a successful download and installation, the Windows Downloader creates two URL files in the destination directory. URL files are files that have the .url extension. Windows uses such files as shortcuts (links) to online content: the file contains a URL value, and opening it directs the browser to that URL.

The first URL file has the same name as the client's display name as defined in the version file. It points at the HTML page that activated the Windows Downloader. The second URL file has the same name as the CAB file, e.g. ptagent.url. It points to the remote CAB file that was downloaded by the Windows Downloader.

Command-line activation

The Windows Downloader is primarily intended for browser-based use. In addition, the Windows Downloader supports a command-line activation mode in which some property values can be provided using command-line arguments. For example:

PtDownloader.exe http://www.ericom.com/ptagent.cab

126.0.1.10 /RUN=HostView

This command downloads and installs the PowerTerm WebConnect Agent from the specified URL, instructs it to connect to the PowerTerm WebConnect at the IP address 126.0.1.10, and to launch PowerTerm WebConnect HostView.

Instead of specifying the URL, you can specify a path to a URL file by preceding the file path with an ampersand (&). In that case, the URL designated by the URL file will be used as the source of the download.

The rest of the command-line, following the download source, is used as the value for the Parameters property. While macros are supported, the <WebServer> macro will return an empty string because there is no Web server.

Troubleshooting Failed Downloads and Installations

If the Windows Downloader fails to perform any operation, it displays a message to the user before terminating. Likewise, if the operation is aborted by the user, a message is also displayed. Since these messages are displayed to the end-user, they are terse and provide very little information about as to the reason activation was unsuccessful. The administrator can extract detailed information about the download and installation process, as well as any errors or problems that occurred, using the Windows Downloader log facility. When this facility is activated, Windows Downloader will log operations that it performs, including their success or failure, as well as reasons for failure in a log file on the user's computer. To activate the logging facility, designate the complete path for the log file as the Log property VALUE, for example:

<PARAM NAME="Log" VALUE="C:\Temp\PtDownloader.log">

NOTE   The Log property does not support the use of macros.

Log behavior:

- The path is the complete path to the file, including the file name and extension. It is not just the name of the directory inside it, which will be created.

- If the directory or file does not exist, it will be created.

- If the file does exist, the new logging information will be appended at the end of the file.

- Changing the Log property value will direct the logging information to the new file.

- Setting the Log property to an empty string will suspend logging. This is the initial value of the Log property.

- If the log cannot be written, e.g. no write-access permissions have been granted for the specified location, it will not prevent Windows Downloader from performing the operation.

- The log is written as a text file, and can be viewed using any text editor.

- It is possible to open and read the log file while it is being generated by the Windows Downloader.

- Each line in the log file represents a specific event. The line has the following format: user-name – time-and-date – event data.

- The first line in a log session contains the string "====> Starting" and the last line contains "====> Done" if the Windows Downloader session ends, or "====> Stopping" if the log stopped while the session is running.

NOTE   The log is generated by the Windows Downloader itself. Consequently if Windows Downloader fails to load, no log will be generated.

In the event that logging is required in order to analyze installation problems, it is not recommended to enable logging for all users. This is because logging may clutter their computer with files they do not need. Instead, it is recommended to create an alternate Web page that is identical to the main one, except that it enables logging, and directs users with installation problems to that page.

11.1.2. Java Downloader

The Java Downloader is a signed Java applet that is compatible with a 1.4.0 or higher JVM. The Java Downloader should be used when either:

- The user's operating system is Windows but the browser does not support ActiveX.

- The user's operating system is not Windows.

NOTE   If the user's operating system is Windows and ActiveX can be used, it is recommended to use the Windows Downloader instead.

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 authorize the component's installation. To circumvent this message, place the Web server (from which the Java Downloader will be downloaded) in the browser's "Trusted sites" security zone. Alternatively, the user can select always trust content from Ericom Software. Once selected, the certificate will not be shown again, even if updates are downloaded.

The Java Downloader provides the following features:

- HTTPS protocol support

- Usage of environment variables in destination and executable parameters

- Clear download progress indicator, showing the name and version of the component being downloaded and a progress bar

- A Cancel button for terminating the download

- 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

- Ability to revert to old client versions

- Error messages and log file to help analyze 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 any 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. To facilitate the Java Downloader adaptation, all its customizable parameters are located in the Java Script file PtAgentSettings.js, see 'Java Downloader Properties and Customization' below.

IMPORTANT   The Java Script functions located in PtAgent.js should not be changed.

IMPORTANT   The Java Downloader utilizes JavaScript to adjust its behavior based on the user's operating system and browser type. For this reason, browser scripting must be enabled in order to use the Java Downloader.

Downloadable Packages

The Java Downloader supports two types of downloadable packages depending on the target operating system. For Windows, the Java Downloader uses the same package format used by the Windows Downloader (see chapter 11.1.1). For Linux, the Java Downloader uses ZIP files instead of CAB files.

In order to be able to handle CAB files, the Java Downloader requires access to a cabarc.exe.txt file. This file must be placed in the same remote directory as the CAB file being processed.

For both CAB and ZIP files, the Java Downloader requires a version file having the format described in chapter 11.1.1. In addition, the contents of the CAB or ZIP file must be the same as described in that section. Consequently both the Java Downloader and the Windows Downloader use the same packages on Windows.

Activating the Java Downloader

The browser activates the Java Downloader when the appropriate <APPLET> tag is embedded in the HTML:

<applet width="1" height="1" code="Downloader.class" archive="…">

The <APPLET> tag instructs the browser to activate a Java applet whose class name is specified in the code attribute. The archive attribute provides the URL from which the applet is downloaded. This URL will designate a CAB or ZIP file, depending on the user's operating system.

Because it is a signed applet, the Java Downloader displays a security notification each time it is activated. The Java Downloader does not display anything inside the browser windows itself. In fact, the Applet's width and height are usually set to 1 making it practically invisible to the user.

The Java Downloader implements a collection of parameters that can be used to control its operation. The values of these properties are specified using the Java Script variables in the proper PtAgentSettings.js and HTML file. The Java Downloader will initiate the download and installation process immediately when the browser activates it, using the values of these properties.

> NOTE For examples of the use of the Java Downloader for the Windows platform, see the JavaScript file PtAgentSettings.js in the web\windows directory. For examples of the use of the Java Downloader for the Linux platform, see the Java Script file PtAgentSettings.js in the web/linux/ix86 directory.

Client Download and Installation

The Java Downloader performs the same operations as the Windows Downloader, as described in chapter 11.1.1, with the following exceptions:

- The Java Downloader can handle both CAB and ZIP files. The choice of which compression format is used depends on the operating system of the target computer.

- Before extracting the contents of a CAB file, the Java Downloader must download cabarc.exe.txt.

- The Java Downloader does not examine the return value of the packaged installer.

Java Downloader Properties and Customization

The Java Downloader implements a set of properties whose values control its behavior. As explained above, the values of these properties can be set using the JavaScript variables in the proper PtAgentSettings.js file or by setting the different parameter values for the various PowerTerm WebConnect clients in the proper HTML file.

Java Downloader properties and the respective JavaScript variable name:

Java Downloader Applet parameter name	JavaScript variable name	Description
Src	url	Specifies the source for the download (the URL to the CAB or ZIP file). Can be a relative URL, in which case it is relative to the browser's base URL. Default: The downloaded archive name.
Dst	dest	Specifies the destination (local) directory for the download. Overrides destination settings in the version file. Can contain macros and environment variables as described below.
Parameters	parameters	Part of command-line arguments to the client executable, placed after the PowerTerm WebConnect server IP address. Can contain macros and environment variables.
Log	log_path	Specifies the local directory for the Downloader Log file creation. Default: Empty
		The Java Downloader creates the Log file by default in <User Home Directory>/Ericom/Downloader.log where <User Home Directory>is browser and operating system dependent: For Windows OS it is defined as C:\Documents and Settings\<user>\Ericom For Linux it is /root/Ericom/ptjdownloader/Downloader.log
	server	Specifies PowerTerm WebConnect Server IP and port. It is not a self-dependent applet property but an important configurable part of 'parameters' variable (see above).
add param	add_parameters	Additional parameters for Java Downloader delimited by space:
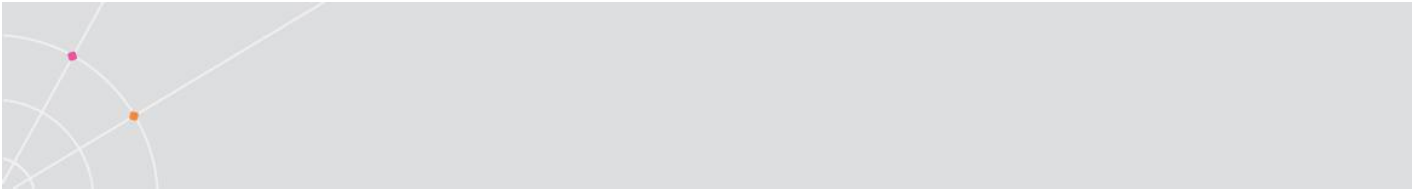
		• **Shortcut** (Linux only): **Shortuct_desktop**, default. Create a shortcut on the desktop during installation. **Shortcut_disable**, do not create a shortcut on the desktop during installation.

In some cases it may be required to place the double-quotes symbol in a property value. This can be problematic because the double-quote is also used as the JavaScript value terminator. To overcome this limitation, represent the double-quote using "

It is recommended to change the variables mentioned in the table above **only in the PtAgentSettings.js or in the proper html file**.

There are two ways to customize the specific Java Downloader parameter:

- All PowerTerm WebConnect clients will utilize the same value of the specific parameter. For example, you want to redirect all clients to a PowerTerm WebConnect Server running on another machine than the Web server, and accepting another port than the default port.
  Customize the **PtAgentSettings.js** file. It is located in:
  Windows: `<WebConnect Installation>/web/windows`
  Linux: `<WebConnect Installation>/web/linux/ix86`

- Different PowerTerm WebConnect clients will utilize different values of the same specific parameter. For example, you want to launch multiple clients to automatically connect and login to a PowerTerm WebConnect Server with different user names and passwords. In this case you need to modify the value of the proper java Script variable in the corresponding J.html file. It is located in:
  Windows: `<WebConnect Installation>/web/windows`
  Linux (Application Zone enables the access to HostView and RemoteView only):
  `<WebConnect Installation>/web/linux/ix86`

  Example:
  You want to launch PowerTerm WebConnect HostView client from ClientURLs.html or HostView_J.html to automatically connect to PowerTerm WebConnect Server, running on a machine that's IP is 'adminserver'. The HostView client logins as user 'Smith' with password 'qwerty' and opens connection 'EnterpriseLegacyHost', predefined in PowerTerm WebConnect Server database and acceptable by the user.

  Open HostView_J.html and update it as follows:

```
//-----------------------------
// Head Actions
```

```
//-----------------------------
var component = "HostView";
// update here
server = "adminserver";
parameters =
" /NOSELFUPDATE /SHORTCUT=BOTH /AUTLOGIN=NO /RUN=HostView " +
" /USER=*Smith /PASS=qwerty" +
" EXTRA_PARAMS=/CONNECTION= EnterpriseLegacyHost "'
add_parameters = "SHORTCUT_DISABLE RUN_EXE";
// end of update
// Identify browser
…
```

The following table lists the HTML file names for PowerTerm WebConnect clients:

Client	HTML Name
Application Zone	Agent_J.html
RemoteView	RemoteView_J.html
HostView	HostView_J.html
QuickVNC	QuickVNC_J.html
SupportView	suppoprtView_J.html
PrintView	PrintView_J.html
Administration Tool	AdministrationTool_J.html
Secure FTP	FTP_J.html
Quick FTP	QuickFTP_J.html
AS/400 Data File Transfer	DFT_J.html

Java Downloader Macros

The Java Downloader Dst and Parameters properties, as well as the version file itself, can contain macros whose values are computed by the Java Downloader at runtime. Macros are placed in the property's value string surrounding their name in < and >, for example <WebServer>. Internally, when using the property's value, the Java Downloader substitutes the entire expression with the macro's value. The Java Downloader does not support the use of environment variables as macros.

NOTE   Macro names are non-case sensitive.

The following table lists the macros supported by the Java Downloader:
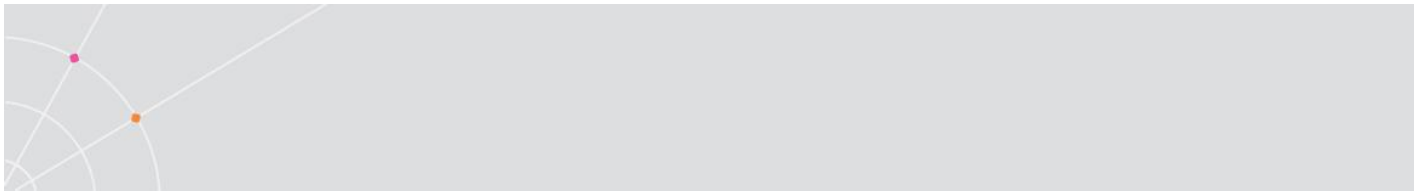
Macro name	Description
WebServer	The name of the Web server from an HTML page's based address. Same value as the window.location.hostname HTML property.
Name	The name of the client's CAB or ZIP file, e.g. "ptagent".
Display	The client's display name from the version file.
Version	The client's version value from the version file.
Root	The default root location. On Windows it is "C:", on Linux/Unix it is an empty string.
OSDir	For Windows operating systems: Windows' installation directory, for example: "C:\Windows"
	For Linux based operating systems: The empty value.
OSDrive	For Windows operating systems: Windows' installation drive, for example "C".
	For Linux based operating systems: The empty value.
HomePath	Macro for access the HOMEPATH environment variable on Windows or HOME environment variable on Linux.
Home	The **Ericom** directory under the user's home directory:
	Windows: `C:\Documents and Settings\<user>\Application Data\Ericom`
	Linux: `/<user>/.Ericom`

In order to place the "<" character itself in the property value (i.e. not have it interpreted as a macro), precede it with the percent symbol %. In order to place the percent symbol in the property value, use consecutive instances: %%.

In addition to the predefined macros listed above, the Java Downloader supports thte usage of environment variables in **Dst** and **Parameters** properties.

System properties available for users on Windows XP, SP2:

Java System Property Name	Value Example
java.version	1.4.2_09
java.vendor	Sun Microsystems Inc.
java.vendor.url	http://java.sun.com/
java.home	C:\PROGRA~1\Java\J2RE14~2.2_0
java.vm.specification.version	1.0
java.vm.specification.vendor	Sun Microsystems Inc.
java.vm.specification.name	Java Virtual Machine Specification
java.vm.version	1.4.2_09-b05
java.vm.vendor	Sun Microsystems Inc.
java.vm.name	Java HotSpot(TM) Client VM
java.specification.version	1.4
java.specification.vendor	Sun Microsystems Inc.
java.specification.name	Java Platform API Specification
java.class.version	48.0
java.class.path	C:\PROGRA~1\Java\J2RE14~2.2_0\classes
java.library.path	C:\Program Files\Internet Explorer;.;C:\WINDOWS\system32;C:\WINDOWS;C:\Program Files\Internet Explorer;;c:\eclipse;C:\Program Files\Java\j2sdk1.4.2_09\bin;C:\eclipse\plugins\org.eclipse.swt.win32_3.1.2\os\win32\x86\;C:\Ant 1.5.2\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\JBuilder7\jdk1.3.1\bin;
java.io.tmpdir	C:\DOCUME~1\diana\LOCALS~1\Temp\
java.compiler	null
java.ext.dirs	C:\PROGRA~1\Java\J2RE14~2.2_0\lib\ext
os.name	Windows XP
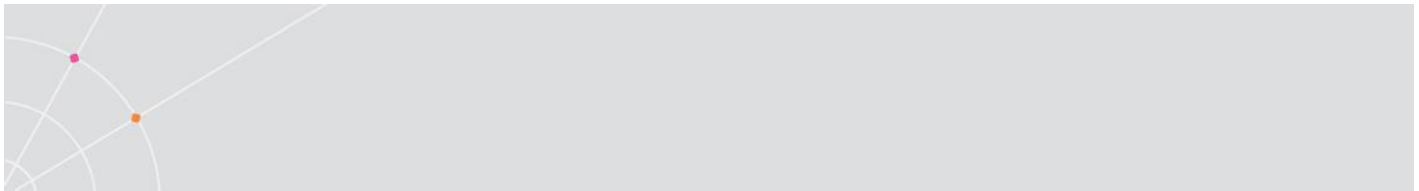
os.arch	x86
os.version	5.1
os.separator	Null
path.separator	;
line.separator	
user.name	<user name>
user.home	C:\Documents and Settings\<user name>
user.dir	C:\Documents and Settings\<user name>\Desktop
package.restrict.access.sun	true
path.separator.applet	true
deployment.user.home	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment
deployment.javaws.jre.1.platform	1.5
deployment.javaws.jre.0.location	http://java.sun.com/products/autodl/j2se
deployment.javaws.jre.0.osname	Windows
https.protocols	SSLv3,SSLv2Hello
deployment.system.tray.icon	true
java.version.applet	True
deployment.javaws.jre.0.product	1.4.2_09
deployment.browser.path	C:\Program Files\Internet Explorer\iexplore.exe
deployment.javaws.jre.0.enabled	true
javaplugin.proxy.config.type	direct
os.name.applet	True
browser.version	1.1
deployment.user.cachedir	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\cache
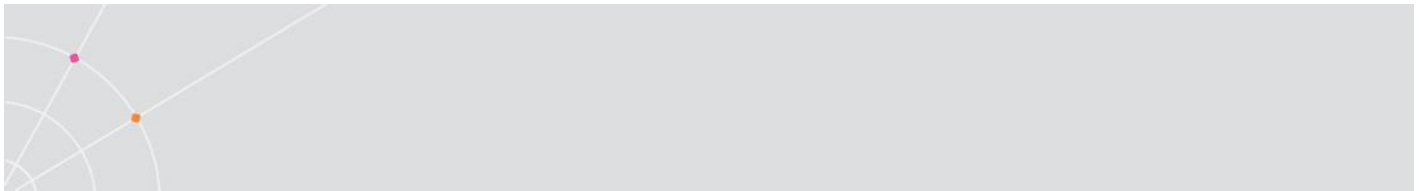
deployment.javaws.jre.0.registered	True
deployment.browser.vm.mozilla	false
acl.read	+
user.timezone	GMT+02:00
deployment.javaws.jre.1.osarch	X86
deployment.user.jssecerts	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\security\deployment.jssecerts
sun.net.client.defaultConnectTimeout	120000
javaplugin.console	hide
line.separator.applet	true
deployment.browser.vm.iexplorer	true
javaplugin.proxy.usebrowsersettings	true
javaplugin.cache.disabled	true
acl.write	+
deployment.system.profile	C:\WINDOWS
deployment.system.security.policy	file:/C:/WINDOWS/Sun/Java/Deployment/security/java.policy
http.auth.serializeRequests	true
acl.read.default	
java.protocol.handler.pkgs	sun.plugin.net.protocol|sun.plugin.net.protocol
deployment.system.home	C:\WINDOWS\Sun\Java\Deployment
deployment.javaws.jre.1.registered	true
javaplugin.jre.params	-DTEMP=C:/Enterprise/Installations/Web
deployment.user.extdir	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\ext
javaplugin.exception	False
http.agent	Mozilla/4.0 (Windows XP 5.1)
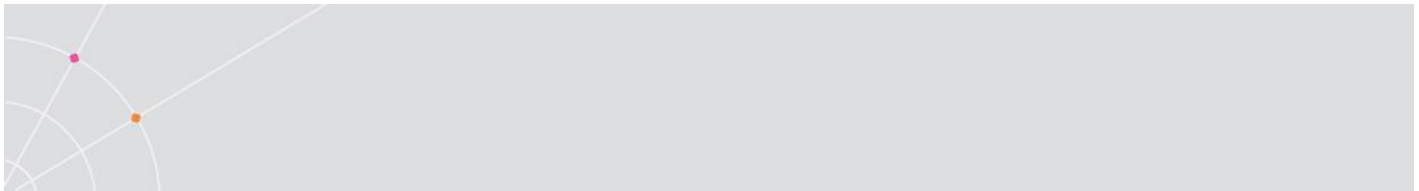
deployment.javaws.jre.1.osname	Windows
package.restrict.definition.sun	True
java.class.version.applet	True
file.separator.applet	True
deployment.javapi.jre.1.5.0_05.path	C:\Program Files\Java\jre1.5.0_05
deployment.javaws.jre.0.platform	1.4
deployment.user.certs	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\security\deployment.certs
deployment.javaws.jre.1.location	http://java.sun.com/products/autodl/j2se
deployment.user.security.policy	file:/C:/Documents%20and%20Settings/<user name>/Application%20Data/Sun/Java/Deployment/security/java.policy
java.vendor.applet	True
package.restrict.access.netscape	false
deployment.javaws.jre.1.product	1.5.0_07
deployment.javaws.jre.0.path	C:\Program Files\Java\j2re1.4.2_09\bin\javaw.exe
deployment.javapi.jre.1.5.0_05.osarch	x86
deployment.javaws.jre.1.enabled	True
java.vendor.url.applet	true
deployment.javapi.jre.1.5.0_05.args	
deployment.version	1.5.0
package.restrict.definition.java	true
package.restrict.definition.netscape	true
deployment.system.cacerts	C:\PROGRA~1\Java\J2RE14~2.2_0\lib\security\cacerts
os.version.applet	true
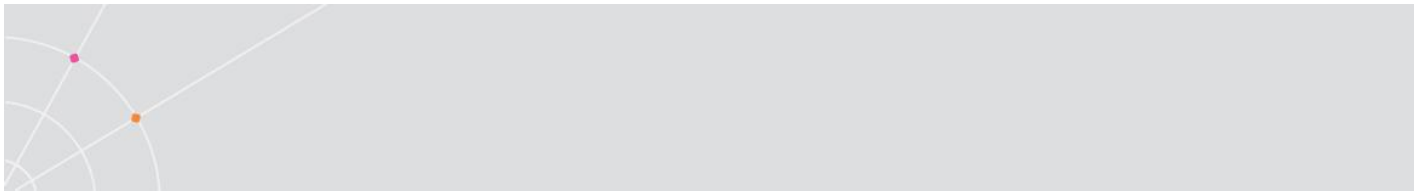
deployment.javaws.version	javaws-1.4.2_09
os.arch.applet	True
deployment.user.tmpdir	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\cache\tmp
deployment.javaws.jre.1.path	C:\Program Files\Java\jre1.5.0_07\bin\javaw.exe
deployment.javaws.jre.0.osarch	x86
deployment.user.profile	C:\Documents and Settings\<user name>\Application Data
deployment.javaws.splash.index	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\cache\javaws\splash\splash.xml
acl.write.default	
browser.vendor	Sun Microsystems, Inc.
javaplugin.jre.path	Default
deployment.system.jssecacerts	C:\PROGRA~1\Java\J2RE14~2.2_0\lib\security\cacerts
deployment.console.startup.mode	SHOW
javaplugin.jre.type	Default
deployment.javapi.jre.1.5.0_05.osname	Windows
deployment.user.logdir	C:\Documents and Settings\<user name>\Application Data\Sun\Java\Deployment\log

System properties available for users on Linux RedHat 9:

Java System Property Name	Value Example
java.version	1.5.0_07
java.vendor	Sun Microsystems Inc.
java.vendor.url	http://java.sun.com/

java.home	/usr/java/jre1.5.0_07
java.vm.specification.version	1.0
java.vm.specification.vendor	Sun Microsystems Inc.
java.vm.specification.name	Java Virtual Machine Specification
java.vm.version	1.5.0_07-b03
java.vm.vendor	Sun Microsystems Inc.
java.vm.name	Java HotSpot(TM) Client VM
java.specification.version	1.5
java.specification.vendor	Sun Microsystems Inc.
java.specification.name	Java Platform API Specification
java.class.version	49.0
java.class.path	/usr/java/jre1.5.0_07/classes
java.library.path	/usr/java/jre1.5.0_07/lib/i386/client:/usr/java/jre1.5.0_07/lib/i386:/usr/lib/mozilla-1.2.1:/usr/lib/mozilla-1.2.1/plugins
java.io.tmpdir	/tmp
java.compiler	null
java.ext.dirs	/usr/java/jre1.5.0_07/lib/ext
os.name	Linux
os.arch	i386
os.version	2.4.20-8
os.separator	Null
path.separator	:
line.separator	
user.name	root
user.home	/root
user.dir	/root
vaplugin.proxy.config.list	
package.restrict.access.org.mozilla.js	true
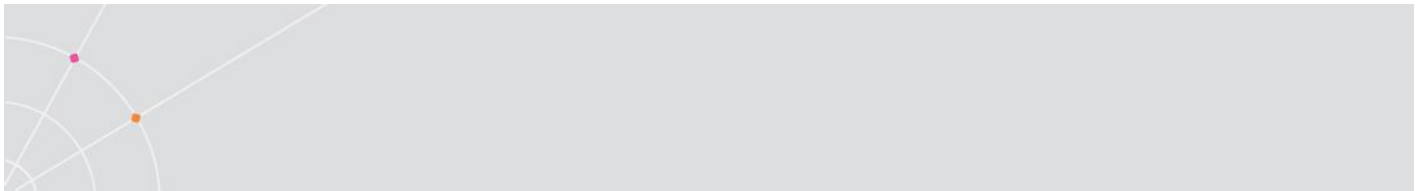
s	
java.version.applet	true
http.auth.serializeRequests	true
os.version.applet	true
file.separator.applet	true
sun.net.http.errorstream.enableBuffering:	true
package.restrict.definition.netscape:	true
os.name.applet	true
package.restrict.access.netscape	false
acl.read.default	
package.restrict.definition.sun:	true
browser.version	1.1
line.separator.applet	true
java.class.version.applet	true
java.vendor.url.applet	true
package.restrict.access.com.sun.deploy	true
javaplugin.proxy.config.type	browser
http.agent	Mozilla/4.0 (Linux 2.4.20-8)
package.restrict.definition.java	true
acl.write.default	
os.arch.applet	true
package.restrict.definition.com.sun.deploy	true
package.restrict.definition.org.mozilla.jss	true

These system properties names are placed in the property's value string within <> (like macros).

Processing of Java Downloader State

You can configure the Java Downloader to notify the Java Script about the state of the downloading and activation process. To enable this you have to customize PtAgentSettings.js and set the Java Downloader parameter 'call_js' to 'true'. PtAgentSettings.js is located in:

Windows: `<WebConnect Installation>/web/windows`
Linux: `<WebConnect Installation>/web/linux/ix86`

Find the lines:

```
// Feature to enable Java Script invocation from Java Downloader
// in order to notify about Java Downloader state changes
var call_js = "false";
```

and change the default "`false`" to "`true`":
```
var call_js = "true";
```

When the feature is enabled, the Java downloader invokes the Java Script function **onStateChange( )** on the change of state and passes the state value as a String parameter. The State values are:

State represented by String	Description
-1	Failure during client download or installation.
0	Not started. The initial state before any operation takes place.
1	Downloading remote version and comparing to local version.
2	Downloading and installing client.
4	Executable is run
5	Download and installation cancelled by the user.

Any negative value of the State property should be considered as failure.

The **PtAgent.js** contains the prototype of the **onStateChange( )** function:

Function onStateChange(sState)

{

    // On Downloader state was changed
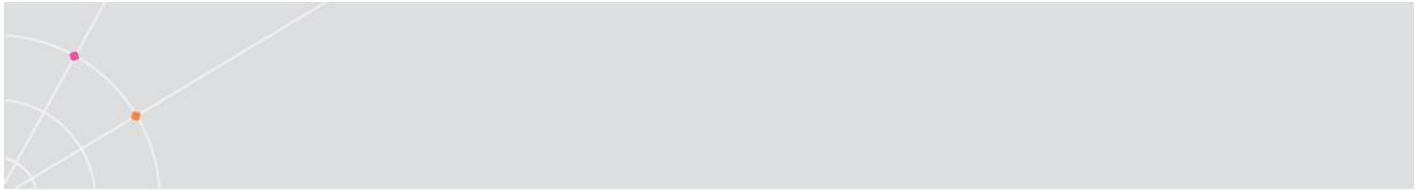
```
//type the state processing here
switch(sState)
{
        case "-1":
        {
                //Failure during client download or installation
                return;
        }
        case "0":
        {
                //Not started. The initial state before any operation takes place
        return;
        }
        case "1":
        {
                //Downloading remote version and comparing to local version
        return;
        }
        case "2":
        {
                //Downloading and installing client
        return;
        }
        case "4":
        {
                //Downloading and installing succeeded. Executable was run.
        return;
        }
        case "5":
```

```
                {

                        //Download and installation cancelled by the user

                return;

                }

        }

}
```

> IMPORTANT The implementation of this function has to be done very carefully.
> It is strongly recommended to avoid prolonged operations and modal dialogs (like
> **alert( )**) in this function implementation.

Known Issues

On Mozilla, Mozilla FireFox and Netscape 6 browsers powered by Java Virtual Machine version earlier then 1.4.2, the Java Downloader will throw an exception and fail to work without any message.

Solution: Download and install the JVM version 1.4.2 and higher.

11.1.3. XPI Downloader

XPI is the Mozilla Cross-Platform Installer. It is the mechanism provided by the Mozilla browser to download and install software packages. PowerTerm WebConnect provides an XPI package, which contains PowerTerm WebConnect HostView for Linux. This enables the installation of that client on Linux Desktops using the Mozilla browser but do not have Java.

> NOTE For examples of the use of XPI, see the AgentXPI.html in the web/linux/ix86
> directory.

11.2. PtStart Downloader

PtStart is an application that will download, install, and launch PowerTerm WebConnect Application Zone mainly on 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 is located. This file contains the paths to the Install folder and the Working folder (see *PtStart.ini options* below). The path to these folders depends on the type of thin client you have as well as the of the downloaded PowerTerm WebConnect Application Zone.

It is also possible to define all PtStart.ini parameters, in a parameter file located in the Web server next to where PowerTerm WebConnect Application Zone is downloaded from.

NOTE 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

11.2.1. PtStart for XPe Thin Client

The thin client device is usually purchased from an OEM with Ericom PowerTerm WebConnect Client pre-installed and you only have to run the "Ericom PowerTerm WebConnect Client" shortcut to start the PowerTerm WebConnect Client.

The Install and Working folders are by default located:

- Install folder: `C:\Documents and Settings\<user>\Application Data\Ericom\Clients\<WebConnect Host name>`

- Working folder: `C:\WebConnectClient\<WebConnect Host name>`

It is possible to customize 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 should be:

`[General]`

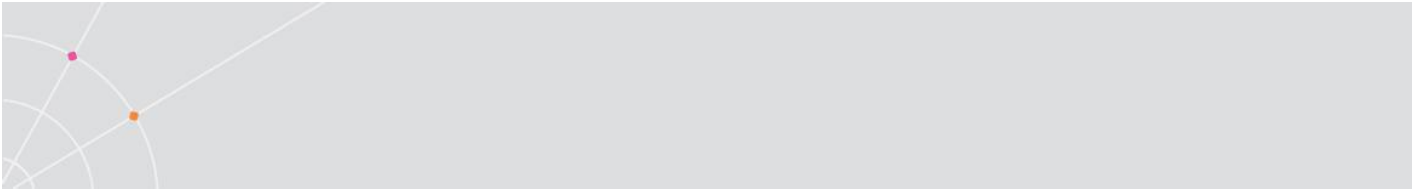`Install-Folder=<desired path – where the WebConnect-Client-Windows.cab and WebConnect-Client-Windows.ver.txt are downloaded>`

`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 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 folder where to unzip all the client components.

11.2.2. PtStart for Linux Thin Client

The thin client device is usually purchased from an OEM with Ericom PowerTerm WebConnect Client pre-installed. Select **Add** in the **Connection Manager** and then "Ericom WebConnect Client" type to start the Ericom PowerTerm WebConnect Client.

The Install and Working folders are by default located:

- `$HOME/Ericom`

It is possible to customize 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 should be:

```
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 require a double minus --)

Option	Description
--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.
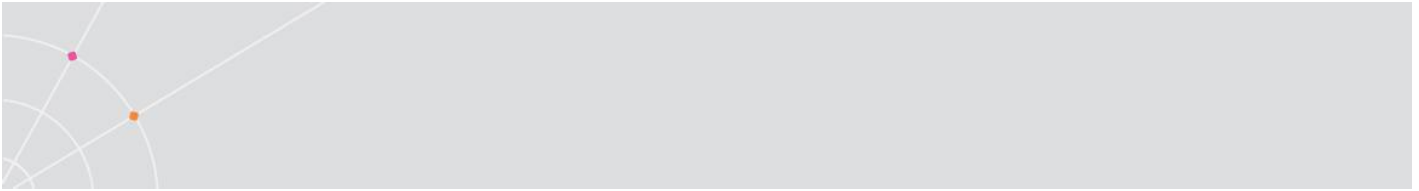
--working-folder=xxx	The folder where to unzip all the client components.
--config-file=xxx	Specifies the full path and name to the PtStart.ini.
--parameters=xxx	qterm-wc parameters. Default: none
--locked	Does not save any changes to the PtStart.ini. Default: off
--log=xxx	Full path and filename to 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 to work with the --thin-client command-line option

Option	Description
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 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 all the client components.
	It is recommended to set the value of **/tmp/Ericom for thin clients** 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.

11.2.3. PtStart for Windows CE Client

The thin client device is usually purchased from an OEM with Ericom PowerTerm WebConnect Client pre-installed. Select **Add** in the **Connection Manager** and then "Ericom WebConnect Client" type to start the Ericom PowerTerm WebConnect Client.

The Install and Working folders are by default located:

- Install folder: …\[persistent folder name]\WebConnect\<WebConnect Host name>

- Working folder: …\WebConnect\<WebConnect Host name>

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

It is possible to customize 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 folder where to unzip all the client components.

11.3. Client Self Update

As detailed above, PowerTerm WebConnect clients are downloaded and installed on demand the first time they are invoked. For example, when the FTP client is invoked from PowerTerm WebConnect HostView, if it is not already installed on the user's computer, it will automatically be downloaded and installed. During the download and installation, a progress indicator will be displayed.

In order to minimize download size, some client components are not downloaded until they are required. For example, PowerTerm WebConnect HostView's online help is not downloaded until the first time it is used. Another example is the PowerTerm font files.

PowerTerm WebConnect clients can also update themselves by downloading newer versions that have been placed on the PowerTerm WebConnect server. When a client starts up, it compares a checksum of its own CAB file with a checksum of the CAB file in the server's Downloads directory. If the two checksums are different, the client downloads the newer version and restarts itself.

In order to place a new client on the server, copy the relevant CAB files over to the server's Downloads directory. This mechanism can also be used to revert to old clients. Just copy the older CABs on top of the new ones.

NOTE   If the downloader attempts to update a client while it is active, the user will be prompted to shutdown the application, after which the update will take place.

11.4. Maintaining Backward Compatibility

In previous PowerTerm WebConnect versions, most clients were registered as ActiveX (COM) Controls on the user's computer. This is no longer the case. Instead the clients are activated as standard processes. An exception is PowerTerm WebConnect WebView (previously OCX), which is still installed and activated as an ActiveX. For backward compatibility reasons, other clients can be activated as ActiveX Controls as well, but this requires manual customization of the Web pages used for client activation.

In order to activate PowerTerm WebConnect clients as ActiveX Controls, their CAB files must be first copied over from the PowerTerm WebConnect server's Downloads directory to the Web server. Then the HTML must be updated to contain an <OBJECT> tag that references to the client's GUID. The following table lists the CABs and GUIDs of PowerTerm WebConnect clients:

Client name	CAB name	GUID
Agent	ptagent.cab	BC2C7665-344E-4277-A405-8AEB70BBD2C2
HostView	ptermx.cab	BBC72F64-2AC3-4942-A8CD-B88857BB21C3
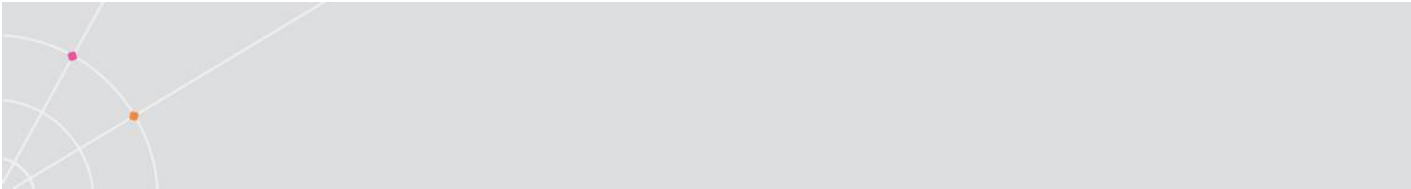
PrintView	plpd.cab	DFCFAFE3-6B3F-4028-A320-5A10E57B65E5
WebView	Webconnectocx.cab	56DA5E7C-6A81-4ED9-A82C-944AC0E401C5

12. Failover

Failover is a redundancy system where if one WebConnect server fails, another will take its place. This system requires at least four components to function properly:

- Primary WebConnect server

- Secondary WebConnect server (can be more than one)

- File server

- Web server (not a WebConnect server)

NOTE   You need an appropriate server license to use the Failover mechanism, but you do not need more client licenses since all the servers participating in the system utilize the same client license pool.

12.1. Configuring the Servers

Verify that you have PowerTerm WebConnect installed on the Primary and Secondary servers.

12.1.1. Configuring a Windows server

To configure the File server:

1. Create a folder for PowerTerm WebConnect server on the file server, for instance WebConnectRoot.

2. Define the newly created folder (WebConnectRoot) on the file server as a hidden share, for instance WebConnect$.

3. Copy the DataBase and Downloads folders from the Primary WebConnect Server to the newly created folder (WebConnectRoot) on the File Server.

4. Copy the PTS.LF, and PTS.LFd if exist, from the Primary WebConnect Server bin directory, e.g. C:\Program Files\Ericom Software\WebConnect 5.1\bin to the DataBase folder on the File Server.

5. For HostView client only:
   Open PtServer_Connections.ini file on the File Server 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$

To configure the Primary server:

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

2. Edit the PtServer.ptr file with Notepad to specify the location of the main configuration file (PtServer.ini), located on the File Server, for instance:
   \\FileServerIP-addressOrName\WebConnect$\DataBase\PtServer.ini

3. Restart the PowerTerm WebConnect Primary server.

To configure the Secondary server:

1. Copy PtServer.ptr from the \bin folder on the Primary server to the same folder on the Secondary server.

2. Restart the PowerTerm WebConnect Secondary server.

To configure the Web server:

1. Copy the web directory from the Primary WebConnect server to the Web server.

2. Start the Web server.

12.1.2. Configuring a Linux server

The Linux server can work in three different modes:

- **Singleton** (default), one PowerTerm WebConnect Server works against one database.

- **Failover**, one PowerTerm WebConnect Server works against one database while other servers are in "waiting" mode.

- **Cluster**, several PowerTerm WebConnect Servers work against one database where the first server to access will be the 'updating' server and the other servers will be 'monitoring (read-only) servers.

Verify that the **ServerType** parameter in the **PtServer.ini** file is set to **Failover**.

To configure the File server:

1. Create a directory "filesrv".

2. Find the /etc/exports file and update it with the "filesrv" directory path and the ip addresses of the Primary and Secondary servers, with permissions:
   /filesrv <ip address of Primary server>(rw,no_root_squash) <ip address of Secondary server>(rw,no_root_squash).

3. Restart the NFS server.

To configure the Primary server:

1. Create a new directory, for example "mysrv".

2. Connect the Primary server to the File server:
   mount <ip address of File server>:/<path>/filesrv /<path>/mysrv

3. Go to your directory "mysrv" and create another directory "WebConData".

4. Copy the DataBase and Downloads into the new folder.

5. Go to the PowerTerm WebConnect installation folder /bin and create a pointer file "PtServer.ptr".

6. Write the path of the PtServer.ini file in this newly created file. For example …/mysrv/WebConData/DataBase/PtServer.ini

7. Run the server.

To configure the Secondary server:

1. Create a new directory, for example "mysrv".

2. Connect the Secondary server to the File server:
   mount <ip address of File server>:/<path>/filesrv /<path>/mysrv

3. Got to the PowerTerm WebConnect installation folder /bin and create a pointer file "PtServer.ptr".

4. Write the path of the PtServer.ini file in this newly created file. For example …/mysrv/WebConData/DataBase/PtServer.ini

5. Run the server.

To configure the Web server:

1. Copy the web directory from the Primary WebConnect server to the Web server.

2. Start the Web server.

12.2. Redirecting to the Secondary Server in Case of Primary WebConnect Server Failure

After you have configured the different servers, you need to modify the client's activation code so that it will attempt to connect to a Failover server in case the primary server fails.

To redirect the client to the Secondary server:

1. Edit the HTML file used to activate the client, e.g. HostView X.html.

2. Change the value of the Parameter attribute used to activate the client: instead of the <WebServer> macro, list the WebConnect server, starting from the primary server. Separate the server names using a semi-colon. For example:
   <PARAM NAME="Parameters" VALUE="PrimaryWC;SecondaryWC;TertiaryWC /RUN=HostView">
   This command line will instruct the Agent to attempt to connect to the "PrimaryWC" server first. If that fails, it will attempt to connect to the "SecondaryWC" server. If that also fails, it will attempt to connect to the "TertiaryWC" server. Failing to connect to that server will cause the Agent to display a failure message to the user.

3. Save the file. You may need to close and reopen the browser window for this change to take effect.

To redirect the Administration Tool to the Secondary server:

1. Launch the Administration Tool. The Connect dialog appears.

2. Type the WebConnect server names in Host Name.

NOTE   A semi-colon must be placed between any of the server names. For example: firsthost; secondhost

3. Complete any other necessary details.

4. Click Connect.

13. Universal Printing

13.1. Introduction

Remote printing in a Terminal Server environment is often problematic, mainly due to the following issues:

- Network traffic overhead of large print jobs being transported from the Terminal Server's Print Manager to the client at which the printer is connected. This causes printing to be slow and network performance to degrade.

- The requirement to install the appropriate printer drivers on all of the Terminal Servers. If a required printer driver is not installed on a particular Terminal Server, it may not be possible to print to that printer type from that server.

- Installing a large number of printer drivers on a Terminal Server can adversely impact its stability and performance.

- It may be necessary to create a printer driver mapping file in order to support clients running on Windows 98/ME.

- Various printer manufacturers do not yet provide a 64 bit version of their drivers. As a result, printers from these manufacturers cannot be used with Windows 2003 x64.

Universal Printing is achieved by having a single, general-purpose printer driver installed on the Terminal Server along with appropriate software on each client. This driver can be used to print to any type of printer. Using this system, maintenance of the Terminal Server is minimal and the server will be more stable.
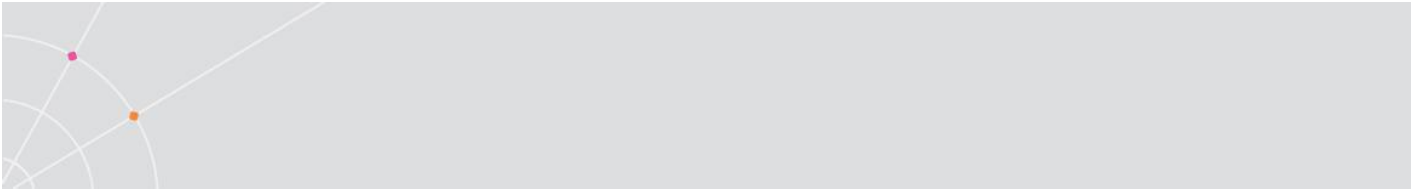
Communication between the server printer and the client printer can work in both PowerTerm WebConnect Direct and Gateway modes. The client software is available for both 32 and 64 bit platforms, and supports USB, LPT, serial, and TCP/IP connections to printers.

PowerTerm WebConnect bundles different printing solutions:

- **triCerat ScrewDrivers** Universal Printing package

- **Net2Printer**

13.2. Integrating triCerat ScrewDrivers into PowerTerm WebConnect

> NOTE Currently the triCerat solution is only available for clients running Windows 98/ME/XP/2000/2003/2003 x64. Thus, triCerat ScrewDrivers cannot be used with RemoteView for Linux or RemoteView for Windows CE.

The triCerat Universal Printer can be installed and used independently of PowerTerm WebConnect, however, doing so will mean that there is no integration of the client print facility into PowerTerm WebConnect.

The triCerat ScrewDriver installers are bundled with the PowerTerm WebConnect server installation. After installing the server, the installers for the various ScrewDriver components will be located in the AddOns\triCerat folder in the PowerTerm WebConnect server folder. These include the installers for both the Terminal Servers and clients.

13.2.1. Terminal Server Installation

To enable universal printing for a Terminal Server, the appropriate ScrewDriver components must be installed on that server. Two installers are provided:

- v405_srvr.msi—installation for Windows 2000/2003.
- v405_srvr_x64.msi—installation for Windows 2003 x64.

13.2.2. Client Side Installation

When RemoteView is provisioned to the client through the browser, the installation procedure will automatically download and install the appropriate ScrewDriver plugin. If RemoteView is installed using MSI, then the appropriate ScrewDriver MSI must also be used to install the client.

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 seeing duplicate printers on the Terminal Server.

13.2.3. Administration

Server side

The ScrewDriver server installation includes a Control Panel Applet that can be used to configure its functionality. Each Terminal Sever installation needs to be managed independently. Please refer to the triCerat ScrewDriver documentation and online help for further details.

Client side

The following Universal printing environmental variables are used:

- **RDP_DisableUniversalPrinting**—globally enables/disables the ScrewDriver client download and usage for all users. This variable should be set at the PowerTerm

WebConnect server level.
Default value—TRUE, Universal Printing is disabled.

- **PRIV_UniversalPrinting—**sets the user privileges to download/use the ScrewDriver client. This variable should be set at the user or group level. Default value—FALSE, the user cannot use ScrewDriver.

- **TriceratUniversalPrintingVersion—**string that defines the ScrewDriver client version. The format of the variable is "_Vx.y.z". This is a control variable for supporting multiple versions of the ScrewDriver client on the same machine. Default value—EMPTY STRING, no version.

**To run the client configuration sdclient.cpl file applet:**

If the client installation has been done using the MSI, the triCerat Client Configuration Tool is accessible from the Windows Control Panel.
1. Open the Windows Control Panel.
2. Click triCerat Client Configuration.

If the ScrewDriver client was downloaded and installed by RemoteView, its Client Configuration Tool is available from the PowerTerm WebConnect client menu as follows:

From the RemoteView client running a seamless application:
1. Launch a seamless application using the RemoteView client.
2. Right-click on the Ericom Software menu from the taskbar.
3. Select *Ericom Software* menu item to open sub-menu.
4. Select *Printer Configuration Tool* item.
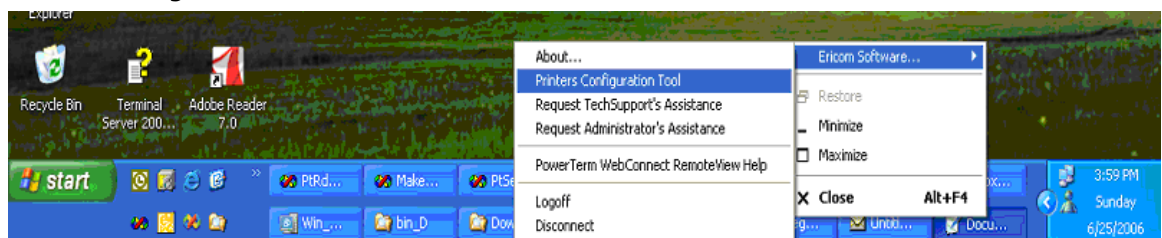
Launching the Printers Configuration Tool

If working with RemoteView in full desktop mode, the Printers Configuration Tool may be accessed through the Windows | Options submenu.
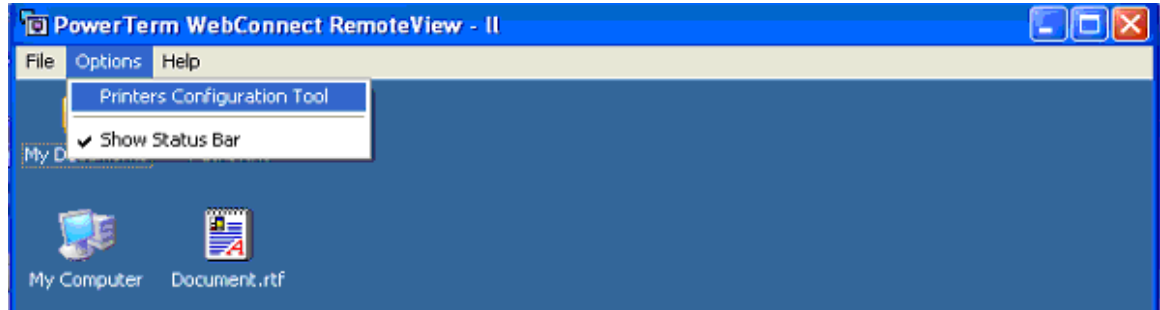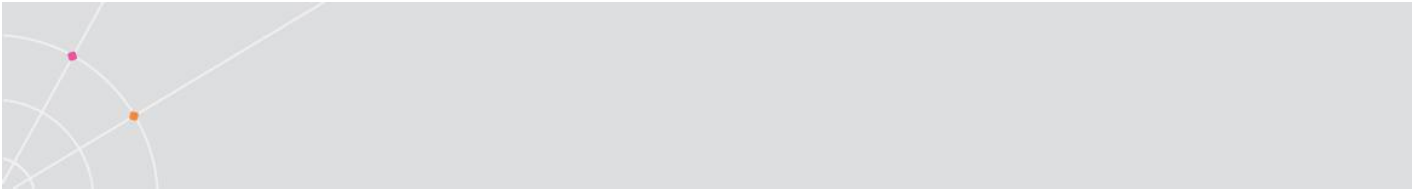
Full Desktop Access to the Printers Configuration Tool

The Printers Configuration Tool is also available from within the Application Zone.

To run the Printers Configuration Tool:

- Select File | Printers Configuration Tool

13.2.4. Licensing and Activation

NOTE   PowerTerm WebConnect does not include a license for ScrewDrivers. All purchasing and licensing must be done directly with triCerat at www.tricerat.com.

For detailed information regarding the installation and configuration of the triCerat ScrewDriver software please see the documentation provided by triCerat.

13.3. Integrating Net2Printer into PowerTerm WebConnect

The Net2Printer installers are bundled with the PowerTerm WebConnect Server installation. After installing the server, the installers for the various Net2Printer components will be located in the **AddOns\Net2Printer** folder in the PowerTerm WebConnect server folder. These include the installers for both the Terminal Servers and clients.

To use Net2Printer Universal Printing you need to install the **NPSetupRDPServerEricom.exe** on each Terminal Server that you are using with PowerTerm WebConnect as well as to configure the relevant Environment Variables. By configuring the Environment Variables, PowerTerm WebConnect will install the Net2Printer client automatically on each user's Pc when running RemoteView. The printers will be mapped by Net2Printer during the logging on process to the Terminal Server.

To configure Environment Variables for Net2Printer Universal Printing:

1. Launch PowerTerm WebConnect Administration Tool.

2. Select **Server | Configuration**. The **Server Configuration** dialog opens.

3. Double-click, in the **Environment Variables** table, **PRIV_UniversalPrinting** and set its value to **1**.

4. Double-click, in the **Environment Variables** table, **RDP_DisableUniversalPrinting** and set its value to **0**.

5. Double-click, in the **Environment Variables** table, **Net2PrinterUniversalPrintingVersion** and set its value according to the syntax `_Vx.x.x` (where 'x.x.x' is the version number). The up-to-date version number is found in the current ReadMe.

6. Click **OK**.

A yellow Net2Printer icon will be displayed in the System Tray when the Net2Printer client is connected properly to the Net2Printer server, otherwise the icon will be white.
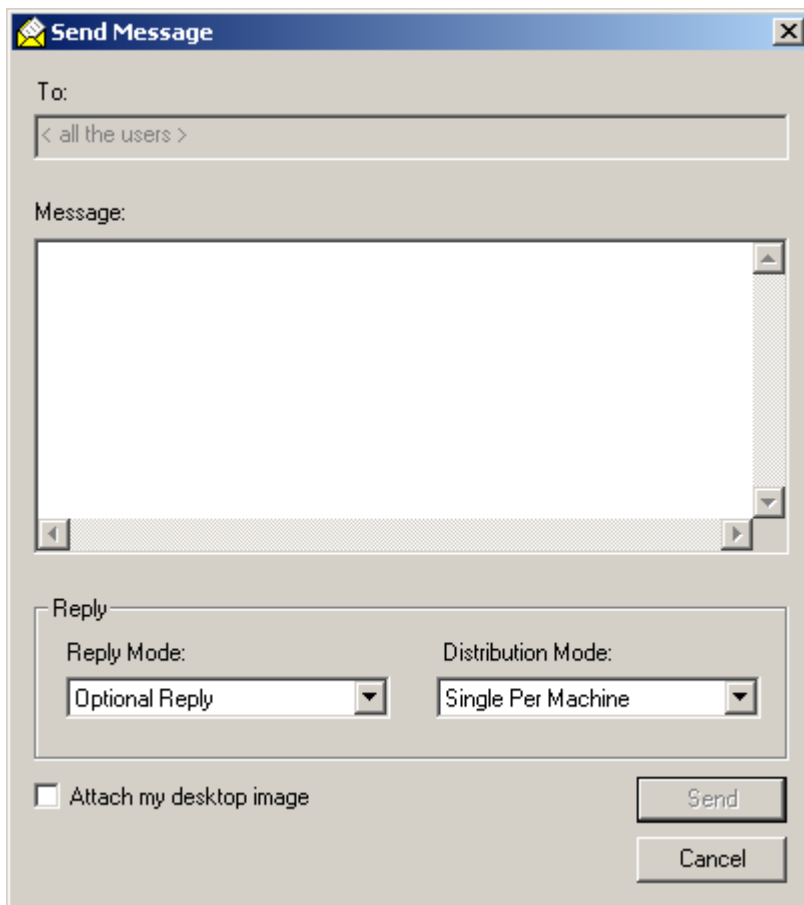
- Right-click the Net2Printer icon to configure the Net2Printer client.

13.3.1. Licensing and Activation

In order to purchase Net2Printer licenses please contact Ericom Software Ltd. or your local distributor.
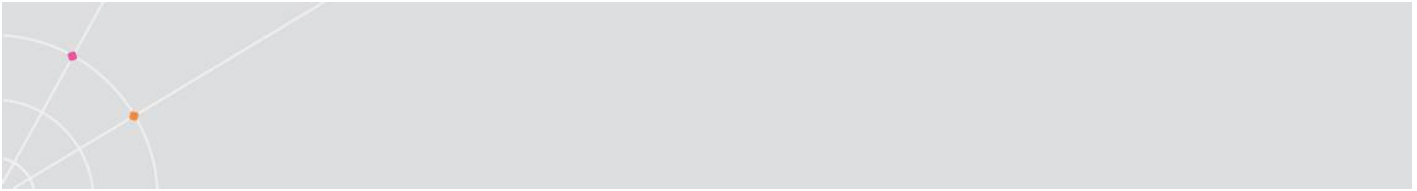
14. Messaging

The administrator can send a message to a particular user/group or to all system users. The administrator can also specify in advance if replies are allowed or not.

The fields in the Send Message dialog are:

To	Specifies the recipient of the message being sent.
Message	Specifies the text of the message being sent.
Distribution Mode	Specifies who the recipients will be.
	Single per machine, only one session on a given machine and user will

	receive the message.
	All clients, the message is broadcast to all sessions (users) of the recipients on the list regardless of the number of sessions opened by the particular client, (i.e. if the user has 5 sessions open, that many messages are received).
Reply Mode	Specifies what action the recipient(s) can take.
	Reply, the recipient is expected to reply.
	Optional reply, the recipient has the option to reply.
	No reply, the recipient does not have the option to reply.

To send a message to a particular User:

1. Select the user(s) to whom you want to send message from the appropriate section of the Administration Tool's main screen.

2. Select **Action | Send Message**. Alternatively right-click **Send Message**. The **Send Message** dialog appears with the designated **Message** recipient.

NOTE   You can add additional recipients by typing their names in the **To** text box.

3. Type the text of your message in the **Message** box.

4. Specify the **Distribution** and **Reply Mode**.

5. Click **Send**. The message is sent to the designated recipient(s).

OR

1. Select the user/group from the appropriate section of the Administration Tool's main screen.

2. Right-click and select **All Sessions**. The appropriate **All Sessions** view appears.

3. Select the user/group and right-click **Send Message**. The **Send Message** dialog box appears with the designated **Message** recipient.

4. Type the text of your message in the **Message** box.

5. Specify the **Distribution** mode.
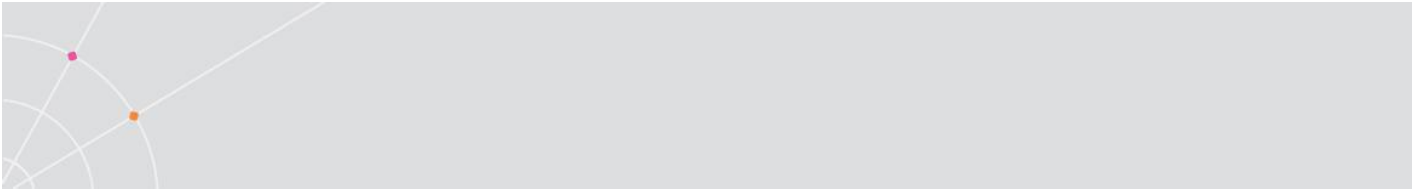
6. Click **Send**. The message is sent to the designated recipient(s).

To send message to a specific Group:

1. Select the group, from the appropriate section of the Administration Tool's main screen, to whom you want to send a message.
2. Select **Action | Send Message**. Alternatively right-click **Send Message**. The **Send Message** dialog appears with the designated **Message** recipient.

NOTE You can add additional recipients by typing their names in the **To** text box.

3. Type the text of your message in the **Message** box.
4. Specify the **Distribution** and **Reply Mode**.
5. Click **Send**. The message is sent to the designated group recipients.

OR

1. Select the group from the appropriate section of the Administration Tool's main screen.
2. Right-click **Sessions**. The appropriate **All Sessions** view appears.
3. Select the group and right-click **Send Message**. The **Send Message** dialog box appears with the designated **Message** recipient.
4. Type the text of your message in the **Message** box.
5. Specify the **Distribution** mode and **Reply Mode**.
6. Click **Send**. The message is sent to the designated group recipients.

To send a message to all users in the system:

1. Select **Server | Send Message to All Users**. The **Send Message** dialog appears with the designated message recipient.

NOTE You can add additional recipients by typing their names in the **To** text box.

2. Type the text of your message in the **Message** box.
3. Specify the **Distribution** and **Reply Mode**.
4. Click **Send**. The message is sent to all the users.

15. Reconnect

The reconnect feature enables clients to automatically resume sessions that have experienced unintentional communication interruptions.

Every session has one of three-reconnect levels (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 reconnect mode of a session is set when the session is established, and cannot change for that session as long as it is active. The reconnect mode is requested by the client and is granted by the server. The Reconnect level to be implemented is negotiated according to the pre-defined Reconnect Mode Rules (see chapter 15.1).

The Reconnect Mode is configurable in multiple locations depending upon the desired configuration. Although there are several tiers where the Reconnect Mode can be set, the lowest mode will be used. wrinkled

In the HostView and PrintView clients, the granted reconnect mode appears in the bottom of the **About** dialog, after the **ID=**... in the following format:
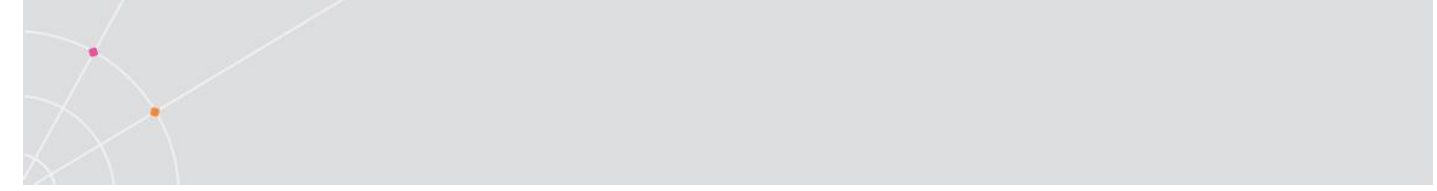
```
PowerTerm WebConnect Server: server:port (ID=hexnum, RM=reconnect-mode)
```

where reconnect-mode can be either **OnDemand** or **Wireless**. If **RM=** is left blank, the reconnect capability is not used.

LastSentMessagesMaxCount

When the Reconnect feature is used in wireless mode, PowerTerm WebConnect counts the numbers of packets for every connection and saves them so in case of disconnection/reconnection the lost data can be restored.

If the value of saved packets (**LastSentMessagesMaxCount**) is too low the server can fail to reconnect but if the value is too high, it may consume too much memory from the WebConnect server machine. However, if the network is not reliable and the application uses a lot of bandwidth then this value should be higher.

Since each user, system and network are not the same, by default the PowerTerm WebConnect server saves the 64 last packets (per connection point). Every time the server fails to reconnect, it automatically increases the **LastSentMessagesMaxCount** value so after one or two failed connections the number of saved packets will be in the optimal location, adjusted to the network being used.

15.1. Reconnect Mode Rules

The client request is specified in the HTML, command line or interactively.

In the event that the client Reconnect request is for None then there is no application of the following rules. Any inbound connection on the specified connection point must have a Reconnect Mode specified. If this is set to None, then any client request will be rejected. This is specified in the Server ConnectionPoints table located in the PtServer.ini file.

The reconnect mode is granted to the most specific reconnect level, as follows:

PowerTerm WebConnect
Reconnect Mode Rules

Client Login –
Requesting
OnDemand/Wireless

Setting of
ConnectionPoint in
PtServer.ini ──────None──────

OnDemand / Wireless

Determine User
Configuration ──────None / OnDemand / Wireless──────

Default

Determine Group
Configuration ──────None / OnDemand / Wireless──────

Default

Determine Server
Configuration ──────None / OnDemand / Wireless──────

Specified Setting
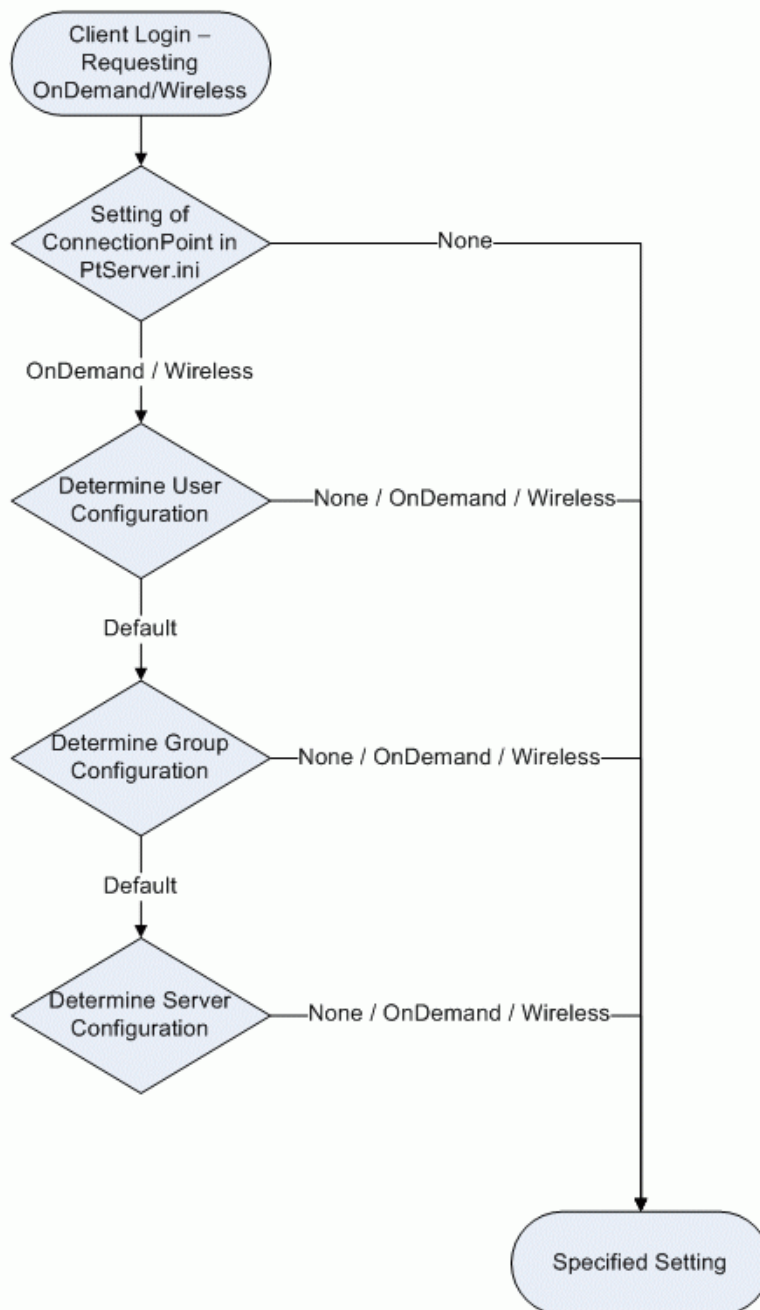
15.2. Enabling the Reconnect Mode

To enable the Reconnect mode the client must request it and the server must be pre-configured to allow it.

NOTE   After modifying the PtServer.ini the PowerTerm WebConnect Server must be restarted in order for the setting to take effect.

15.2.1. Client Request for Reconnect Mode

HostView, PrintView, RemoteView, QuickVNC, ApplicationZone clients

In order to configure the reconnect mode, you must add one of the command line arguments listed below in the appropriate HTML.

Command line arguments for Reconnect Mode:

/ RM_NONE (*)

/ RM_ON DEMAND

/ RM_WIRELESS

/RM_INTERACTIVE (only applicable for HostView and PrintView clients) enables the client to select the mode during login.

WebView

For PowerTerm WebConnect WebView the reconnect feature is implemented at the login stage using one of four different methods, depending on the reconnect level requested:

LoginToServer (	server_address,
	server_port,
	username,
	password,
	use_ssl,
	reconnect_mode,
	session_id);

LoginToServerConnection (	server_address,
	server_port,
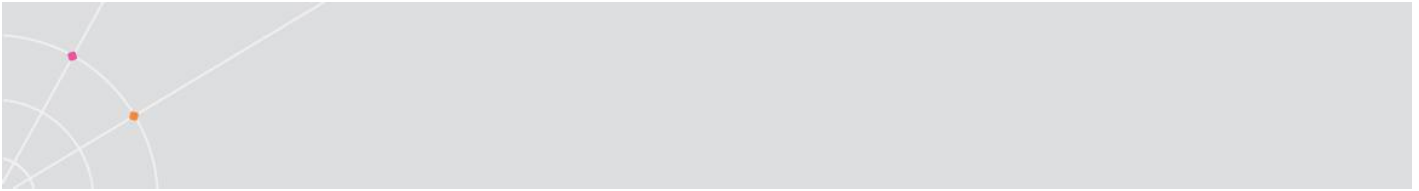
	username,
	password,
	connection_name,
	use_ssl,
	reconnect_mode,
	session_id);

LoginDialog (	server_address,
	server_port,
	use_ssl,
	reconnect_mode,
	session_id);

LoginDialogConnection (	server_address,
	server_port,
	connection_name,
	use_ssl,
	reconnect_mode,
	session_id);

15.2.2. Server Configuration for Reconnect Mode

In the Server you can specify Default Reconnect Mode for reconnecting to the PowerTerm WebConnect server, which has undergone unintentional communication interruptions. This is only applicable when the Highest Reconnect Mode of both the User and its default Group are not explicitly specified (<Default> is used).

To determine the Reconnect mode for the server:

1. Select Server | Configuration. The Server Configuration dialog appears.
2. Select the appropriate Default Reconnect Mode.

15.2.3. User Reconnect Limitations

The user Reconnect limitations are determined by the configurations on the User, Group and Server levels in that respective order.

Highest Reconnect Mode: Specifies the rule according to which the user/group is allowed to automatically reconnect to the PowerTerm WebConnect server, which has undergone unintentional communication interruptions.

To determine the Reconnect mode for the user:

1. Right-click the desired user and select Properties. The User Properties dialog appears.

2. Select the Highest Reconnect Mode.

When the Highest Reconnect Mode is not explicitly specified (<Default> is selected), then its Group's default Reconnect Mode will be used.

To determine the Reconnect mode for the group:

1. Right-click the desired group and select Properties. The Group Properties dialog appears.

2. Select the Highest Reconnect Mode.

When the Highest Reconnect Mode is not explicitly specified (<Default> is selected), then its Server's default Reconnect Mode will be used.

15.3. Disconnected Sessions and Session Reconnect

15.3.1. What is a Disconnected Session?

Disconnected Terminal Server sessions are user sessions on the Terminal Server that contain active applications, but to which no RDP client is attached.

Sessions may be become disconnected due to a number of causes, such as:

- A network fault, cable 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 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 they are still active, ie., have not yet been reset.

NOTE The PowerTerm WebConnect disconnected session management functionality does not utilize the Microsoft Session Directory service introduced in Windows 2003. As a result, it does not require Windows 2003 Enterprise Edition and will work with both Windows 2000 and Windows 2003.

Client Options

A user must be logged on to the PowerTerm WebConnect Server through the PowerTerm WebConnect Application Zone client in order to receive notifications regarding disconnected sessions.

When a user's session(s) has been disconnected, an icon will automatically appear in the System Tray and the following notification balloon will be briefly displayed:

"Power Term WebConnect Application Zone. You have disconnected sessions. Right click the icon in order to resolve them."

This balloon is a one-time event that will display for 10 seconds, after which it will automatically disappear.

Right clicking on the disconnected icon will offer the following three options to the user:

- Reconnect all.

- Close all.

- Hide notification.

Double-clicking the icon will reconnect all the sessions. The user can only reconnect to his disconnected sessions, ie., only sessions that he created using the same credentials. Once the user has reconnected to all his disconnected sessions, or these sessions have been closed or reset, the icon will automatically disappear from the System Tray.

The same icon will also be displayed in the Application Zone window. Double-clicking on this icon will reconnect the user to all his sessions.

Administration Tool Options

It is possible to close (logoff) a user's disconnected session from the Administration Tool.

To close a disconnected session:

1. Launch the Administration Tool.

2. Click on the Terminal Server Sessions button. A dialogue showing all Terminal Server sessions that are currently open, that is, those that are active as well as disconnected.
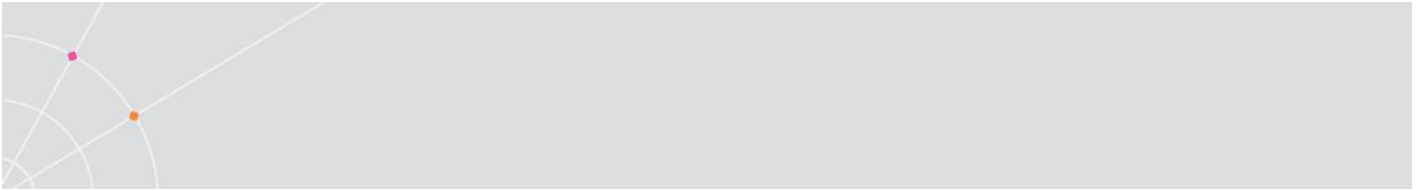
3. Select the disconnected session(s) that you want to close. Use the Ctrl key for multiple selections.

4. Right-clicking on the selected session(s) will display a menu offering the following options:

5. Log Off Disconnected Sessions.

6. Log Off All Disconnected Sessions.

7. Click on Close Disconnected Session.

NOTE   Disconnected Sessions will only work if:
The Administrator has configured the server farm to use the PowerTerm WebConnect Load Balancer component.
The sessions were created by the RemoteView Windows client.

NOTE   The Disconnected Sessions functionality is not supported for sessions created by the RemoteView for Linux client.

16. Remote Assistance and Support

Using the SupportView component of PowerTerm WebConnect enables you to provide remote assistance and support to users. Once activated, it allows you to take over a user's entire Desktop, so that you can view and modify local configurations. In this way, PowerTerm WebConnect's SupportView lets you view all the users' active sessions (Session Shadowing), as well as access external applications, such as the registry editor or Print Manager. This tool is based on the VNC protocol (www.TightVNC.com), but extends both its functionality and security.

PowerTerm WebConnect's SupportView is comprised of two complimentary components: daemon (VNC server) and viewer (VNC client), where the daemon side is "taken over" by the viewer side. Thus, it is the daemon that is activated on the user's computer when a SupportView session is started, and the viewer that is launched on the administrator's or support staff's computer.

Communication between the daemon and the viewer side is accomplished using TCP/IP sockets, where the daemon side is listening on port 5900. If that port is blocked by an intervening firewall, PowerTerm WebConnect Server is able to provide a gateway service allowing the SupportView to be used in situations where other remote control services do not work.

SupportView can be employed both to assist and/or train an End-user ("User Target"), and to remotely administer the PowerTerm WebConnect Server ("Server Target").

16.1. Targeted User

With SupportView, you can "take over" the user's computer. This means that on your desktop there will be a window displaying an exact image of the screens and the cursor movements occurring on the user's monitor. You can interact with this window, and your actions will determine the cursor's movements and its actions on the user's computer. In this way, upon request you can demonstrate to the user how a particular task is accomplished.

To attach to a computer whose user is requesting administrator assistance:

1. When a user requests administrator assistance, the administrator will receive a notification, identifying the user.

2. Click OK. The SupportView daemon is downloaded to the user's computer, the session is attached, and the administrator takes control of the remote desktop.
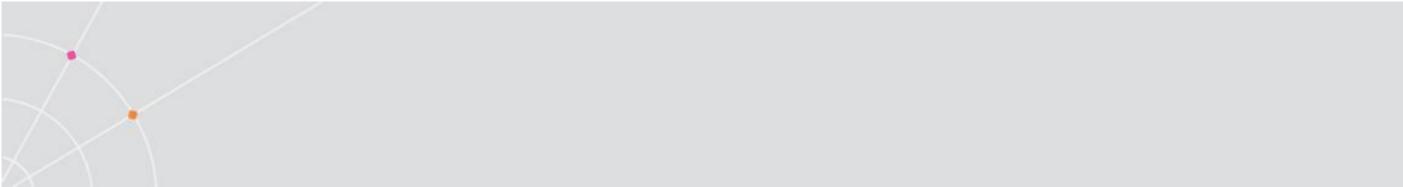
To attach to a computer whose user did not request administrator assistance:

1. Select View | Client Sessions. The Session dialog appears.

2. Right-click Attach on the desired user. The Verify Permission dialog appears.

3. Enter Password.

4. Click Verify. The session is attached and a notification message is displayed to the user.

Locally

Attaches to a particular user session that will run on the same computer.

1. In the Session screen, right-click Attach on the desired user. The Verify Permission dialog appears.

2. Enter Password.

3. Click Verify. The session is attached and a notification message is displayed.

Remotely

Attaches to any session running on a remote computer that has a VNC server.

1. In the main screen, right-click Run QuickVNC or select Tools | Run QuickVNC on the desired user. The PowerTerm WebConnect QuickVNC dialog appears.

2. Enter Password.

3. Specify Reconnect Mode if necessary.

4. Click Verify. The session is attached and a notification message is displayed.

To facilitate technical support, the following users have been created for run-time and therefore do not exist in the database:

- Generic Customer

- Software Installer

16.2. Targeted Server

With SupportView, the administrator is capable of remote access to PowerTerm WebConnect Server, making maintenance a simple straightforward task. By default, PowerTerm WebConnect installation sets the PowerTerm WebConnect server to run in interactive mode (i.e., to run as a local system account), which is essential to accomplish this remote access task.
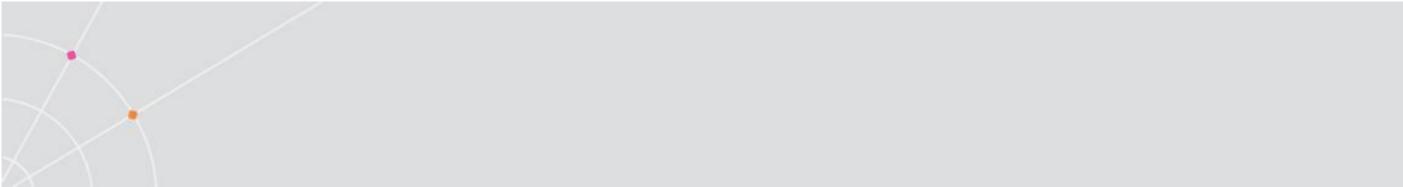
To attach to a server:

1. Select Server | Attach. The Verify Permission dialog appears.

2. Enter Password.

3. Click Verify. You now have access to the server.

16.3. Security

Because SupportView provides total remote control of the user's desktop, care was taken that the security and integrity of the user's computer is not compromised. SupportView's provides several security features:

- In gateway mode, the SupportView session can be encrypted using SSL.

- The VNC daemon on the user's computer is activated only when a SupportView session is started, and is shutdown immediately when the session is terminated.

- SupportView generates a random username and password for each session, sending it to the viewer, encrypted. When the session ends, these username and password are invalidated.

- When an administrator connects to the user's desktop, the user receives a visible notification. Thus SupportView cannot be used for eavesdropping.

- Combined, these features guarantee that SupportView cannot be used to jeopardize the security of the user's computer.

NOTE On Windows, the VNC daemon stores the username and password in the registry. Because the username and password are changed for every session, SupportView requires that the user has write-access to that area of the registry. This means that restricted users may not be able to use SupportView.

17. Presentation Virtualization

Using the RemoteView component of PowerTerm WebConnect enables you to publish and access remote applications running on Windows Terminal Servers as well as local applications. The RemoteView component utilizes the Remote Desktop Protocol (RDP), which provides remote display and input capabilities over network connections for Windows-based applications running on a server. You can design your RemoteView connection to let the end-user interact with the remote desktop in a windowed or in full-screen modes. You can also publish an application for full integration into the local desktop as a Seamless Window.

NOTE   PowerTerm WebConnect RemoteView does not support seamless windows for 16 bit applications.

17.1. Session Sharing

When you run more than one seamless application from your local computer on the same Terminal server, the applications share the same session. This eliminates extra login time as well as lowers the overhead on the Terminal server. (If needed, the Environment variable RDP_DisableSessionSharing can be flagged so that each seamless application will run on a separate session.)

You need to fulfill the following conditions to ensure Session Sharing:

- The new published application has to be launched on the same Terminal Server to where the user is already connected. This will happen automatically if the Load Balancer is used.

- 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 reuse the PowerTerm WebConnect credentials.

- The published applications need to have the same Direct/Gateway setting.

NOTE   Failing to properly configure the Terminal Serve to allow a user to connect more than once, may result in disconnection messages appearing when Terminal Server sessions are detached from one instance of RemoteView and passed to another.

17.2. RemoteView Connections

To use RemoteView you must define the connection through the Publish Application Wizard (see chapter 6.2). You can use this type of connection to connect to a Microsoft Terminal Server 2000/2003, as well as a Citrix Presentation server with RDP support. In order to use the seamless mode, you must install the included Terminal Server Agent Component on all your Terminal servers, i.e. you cannot use the seamless mode without the Terminal Server Agent. This installation is available as an independent feature, and also as an option of the PowerTerm WebConnect installer.
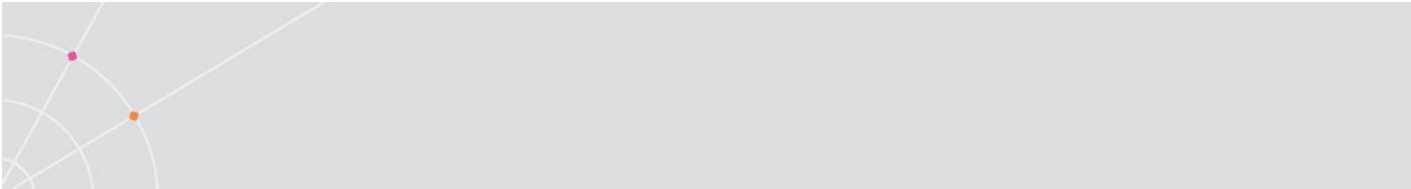
17.3. URL Redirection

URL redirection is a feature that intercepts activation of URLs by applications on the Terminal Server, and redirects that activation to the client side. For example, a user clicks a URL in a document running in MS Word on a Terminal Server. By default the browser would open for that URL on the Terminal Server. With redirection activated, the browser will open on the client device instead.

There are several reasons why opening a URL on the client may be preferable to opening it on the server:

- Reduced server load - Running the browser on the client offloads the effort from the server. This is especially true for web pages that contain streaming video or audio.

- Improved performance - Data streams directly to the client instead of going through the server. Also, RDP is not optimized for streaming content.

- Web Access - The Terminal Servers may not have access to Web-based resources for security reasons. In such a scenario, opening the URL on the Terminal Server will fail, but may succeed on the client.

- Security - For security reasons browsing on the Terminal Server may be much more restricted than on the client, e.g. no cookies, no scripts, no ActiveX. This will prevent various web sites from functioning properly.

- Email/News account - The user may not have an email or news accounts configured on the Terminal Server, but will have such accounts on the client. In such a scenario, opening a mail or news URL on the Terminal Server will fail, but opening on the client will succeed.

- Content downloads - Some types of content downloads may be more appropriate for the client rather than the server. For example, downloaded music files.

Configuration

Any standard URL may be redirected. A URL is a standard method to denote resource locations, and has the format scheme:

```
host/resource-path
```

For example http://www.ericom.com/ptj.asp where the scheme is http, the host name is www.ericom.com and that path is ptj.asp
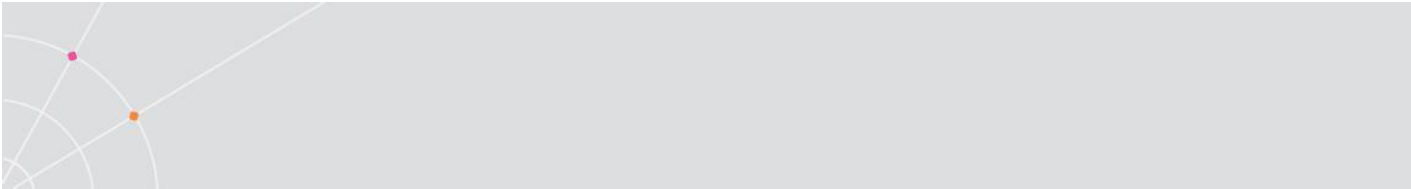
> NOTE   This is a generalization - URLs can contain additional parts, and some URLs have a somewhat different format.

PTWC 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
mailto	Send mail
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)

By default URLs are not redirected. In order to enable redirection, the RDP_RedirectSchemes PowerTerm WebConnect 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. If "all" is specified as the value for RDP_RedirectSchemes then all URLs will be redirected regardless of scheme.

In some cases it may be required to redirect some URLs but not others, although they use the same scheme. For example, URLs that reference external Web sites would need to be redirected, yet URLs that reference internal Web servers that are not externally accessible, should not. Using RDP_RedirectExclude PowerTerm WebConnect Environment Variable makes it possible to specify which URLs should be excluded from redirection based on the host name, or IP address. If RDP_RedirectExclude is not defined, no exclusion will be performed. RDP_RedirectExclude contains a delimited list of the hosts to exclude. Host names specified in RDP_RedirectExclude are compared to the host in

the URL from right to left, so 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. Exclusion based on IP address is not performed if a host name is used in the URL, even if the host name maps to that IP address.

Restrictions and Limitations

- Redirection is currently supported only for PowerTerm WebConnect RemoteView for Windows.

- Redirection is verified to work only with Internet Explorer on both the Terminal Server and the client.

- Installing a new browser or mail client on the Terminal Server after PtTSAgent has been installed may break the redirection mechanism. In such a case, uninstall both PtTSAgent and the new browser or mail, reinstall the new browser or mail and then reinstall PtTSAgent.

- Restricting the user for making any change 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 of RDP_RedirectSchemes and RDP_RedirectExclude. (For standard Windows configurations, even restricted users have permissions to modify that section of the registry).

- Exclusion based on IP address is performed only if the IP address is explicitly specified in the URL. Exclusion based on IP address is not performed if a host name is used in the URL, even if the host name maps to that IP address.

- The redirection mechanism does not verify that the client supports a particular URL type, or has Internet connection, before redirecting a URL. The URL will be redirected regardless, even if the operation will fail.

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

18. Remote Desktop Control

The QuickVNC component of PowerTerm WebConnect utilizes the Virtual Network Computing (VNC) to enable connection as a viewer to any standard VNC daemon. Thus it can be used to access and interact with remote computers. This capability can be used for online conferencing and online training as well as for enabling remote assistance and support.

NOTE   PowerTerm WebConnect QuickVNC provides the viewer side only of the VNC connection. The daemon side is external to PowerTerm WebConnect (in the same way that a legacy host is external in a terminal emulation connection.)

To configure a QuickVNC client connection:

1. Select Action | New | Connection or right-click Properties on the desired connection. The Add Connection dialog appears.

2. Type in your Connection Name.

NOTE   Names are not case-sensitive, however they must be unique.

3. Type in your Display Name (optional).

4. Specify Category as Remote Desktop Access.

5. Select VNC as the Communication Type.

6. Select the Owner of the connection.

7. Type in the Host name or IP address of the computer to which you want to connect.

8. Specify the Password for the connection. If a password is not specified, the user will be prompted for a password when the connection is established.

9. Type the Port Number on which the VNC daemon is listening. Default is 5900.

10. Specify the Display Number for the VNC connection. Default is 0.

11. Select whether you want the connection to appear in full screen or window mode, and whether it is for viewing only, or if it will allow interaction with the remote computer.

For more documentation about VNC, please see www.tightvnc.com/docs.html and www.realvnc.com/documentation.html.

19. Desktop Virtualization

DeskView is a PowerTerm WebConnect component that makes it possible to publish Desktops and applications that run on Virtual Machines and dedicated physical machines.

In a SBC environment, all users have access to a desktop via an individual session on a Terminal Server. The operating system and all the applications are installed on the Terminal Server. However, PowerTerm WebConnect DeskView utilizes the VDI model to grant each user access to his or her own desktop on a physical or virtual machine, where all Virtual Machines are provided by a hardware virtualization layer added to a centralized server. The operating system and all applications are installed on each Virtual Machine. This type of environment allows the organization to move control of many end-user desktops and data into a few centralized servers.
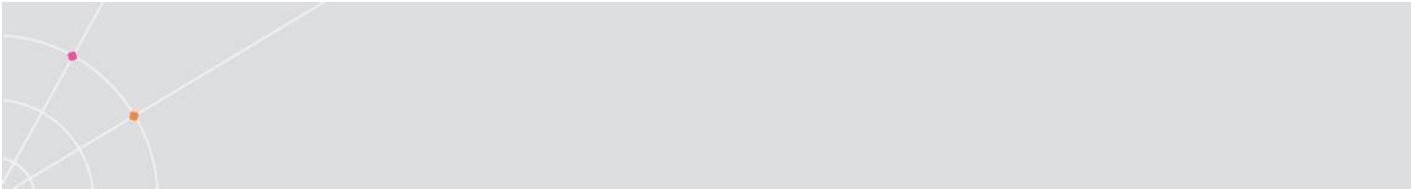
By using PowerTerm WebConnect DeskView, each user will have his or her own unique environment that can be customized without affecting other users. Thus, if a failure would occur on one machine (physical or virtual) it will not affect any of the other machines. The Administrator can also create customized pooled desktops to meet various different configurations. The end-user then connects to the designated physical or virtual machine by utilizing PowerTerm WebConnect RemoteView Client.
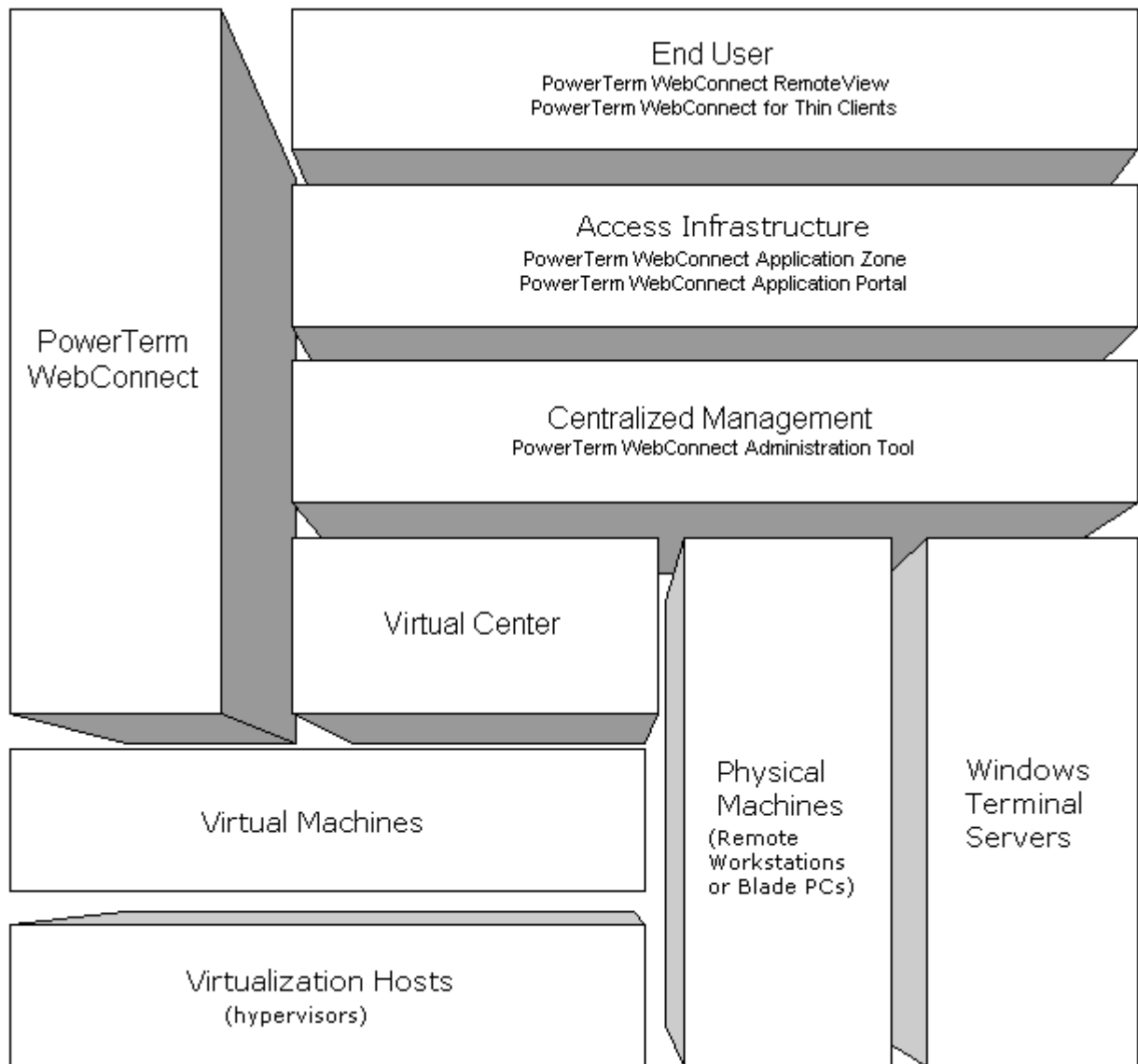
PowerTerm WebConnect DeskView consists of:

- **PowerTerm WebConnect DeskView Server**, a Connection Broker that interfaces with PowerTerm WebConnect Server and the Physical and Virtual Machines/Hypervisors.

- **PowerTerm WebConnect DeskView Administration Tool**, the user admin interface for configuring PowerTerm WebConnect DeskView Server.

PowerTerm WebConnect DeskView supports:

- VMware VirtualCenter 2.x and higher

- VMware ESX 3.0/ESXi 3.x and higher

- VMware Server 2.x

- Microsoft Hyper-V

- Microsoft Virtual Server 2005

- Microsoft Center Virtual Machine Manager 2008
  * Requires PowerShell 1.0 installed on the DeskView Server machine.

- Parallels Virtuozzo 4.0 and higher

- Oracle VM 2.1

- Virtual Iron Single Server/Enterprise 4.213

- XenServer 4.0 and higher

- Xen Community 3.2 and higher* (includes Red Hat Xen and Novell Xen)
  With Libvirt 0.3.0 and higher installed on the Xen hypervisor server and enabled in listening mode.

- KVM

- Teradici/PC-over-IP Managed Machines

- Physical Managed Machines

19.1. PowerTerm WebConnect DeskView Architecture

19.2. Requirements

Please read the ReadMe.txt attached to the installation, or on the Ericom Website (www.ericom.com/systemreq.asp) for the most up-to-date requirements.

19.3. Installation

PowerTerm WebConnect DeskView is automatically installed when you run PowerTerm WebConnect Installation wizard.
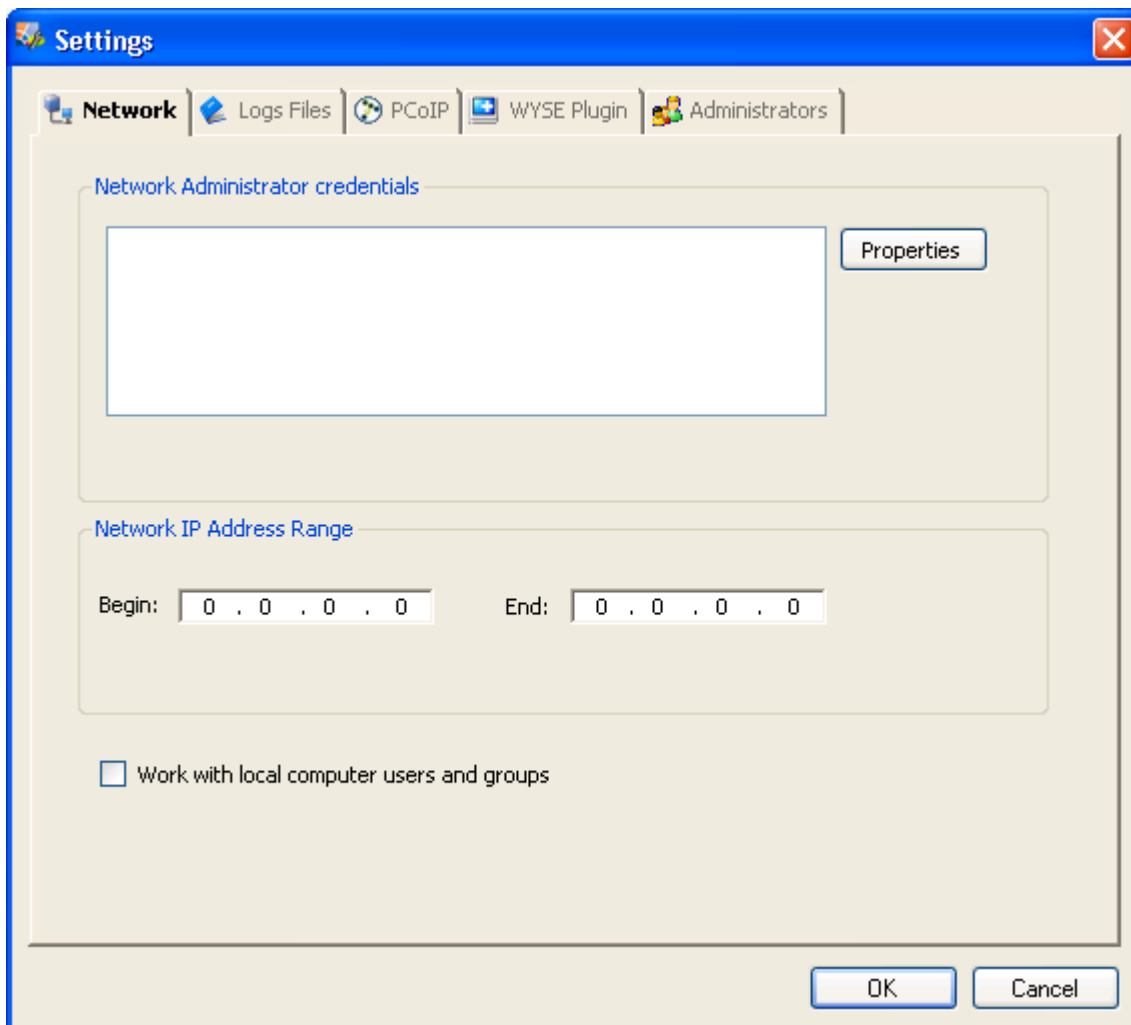
- Select **Full installation** when prompted.

You can also install PowerTerm WebConnect DeskView after you installed PowerTerm WebConnect (Full installation).

- Go to **<PowerTerm WebConnect Installation Folder>\WebConnect 5.6\AddOns\DeskView VDI** and run **DeskViewServerSetup.msi** and **DeskViewAdminSetup.msi**

19.4. Connection Broker Administration Tool – General View
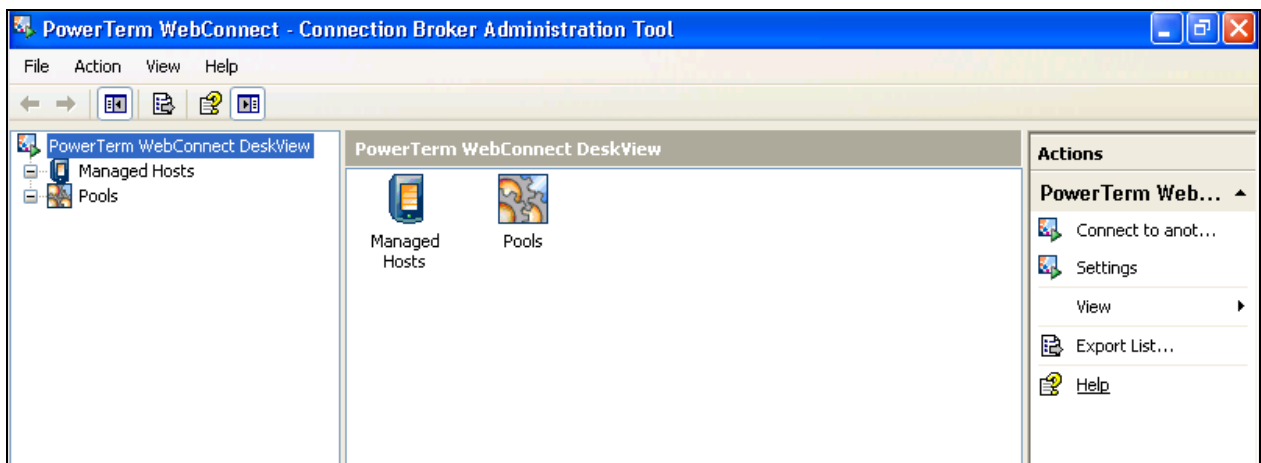
Tab	Description
Network	Lists domain administrators. Specifies the network search range.
Log Files	Specifies log criteria.
PCoIP	Specifies PCoIP configuration. Only enabled with PCoIP managed machines.
WYSE Plugin	Specifies WYSE Plugin configuration.

Administrators	Lists administrator's for the machine where DeskView Server resides.

19.5. Managed Hosts

19.5.1. Reference

Host Properties Dialog

NOTE   The **Host Properties** dialog may vary a bit depending on the type of host you selected.

Field	Description

Host Name	Specifies the host's name.
Type	Specifies type of server.
Default Pool	All machines on this host will automatically be added to the specified pool (unless another pool has been assigned to the machine directly).
Enable	Enables the connection for active use.
Description	(Optional) Enter free-form information about the host.
Address	Specifies the server's address.
Port	Specifies the host's port.
Username	Specifies the user account that is connected to the server.
Password	Specifies the user's password.
Test Connection	Checks correctness of information and if the connection to the virtualization hos is established.

* For Managed Physical Machines only

Field	Description
IP Range	Specifies the IP range for the host to search.
DNS Pattern	Specifies the DNS pattern for the host to search.

Action Menu

> NOTE The **Action** menu may vary a bit depending on the type of host you selected.

Menu item	Description
Properties	Opens the Host Properties dialog.
Reconnect	Reconnects the selected host.
Add Folder (for Managed Physical	Creates a virtual folder to easily arrange
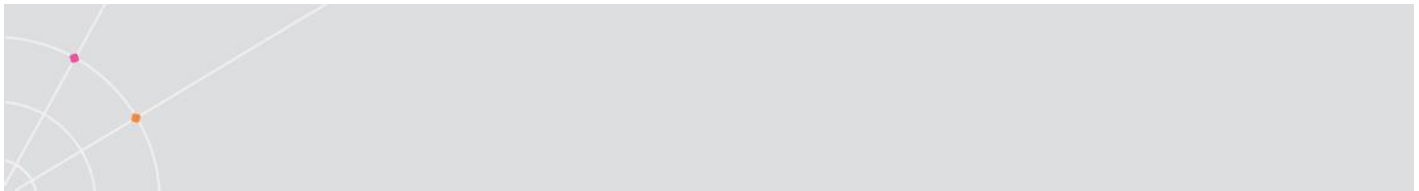
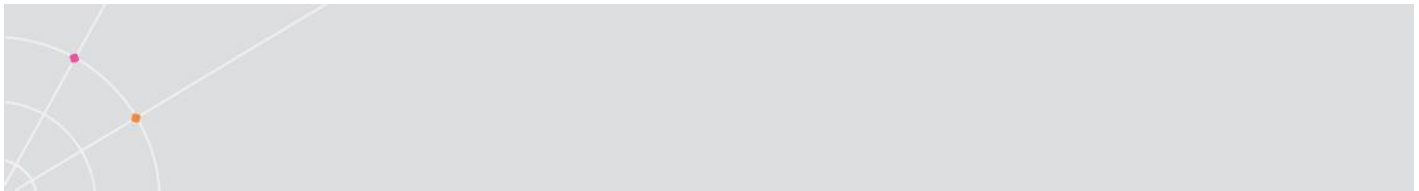| Machines only)	your virtual machines.
Add Physical Machines	Inserts new Blade PCs/machines on your host.
PC-over-IP Hosts	Lists the PC-over-IP hosts that are available.
PC-over-IP Clients	Lists the PC-over-IP clients that are available.
Delete	Deletes the selected host.
Rename	Renames the selected host.
Refresh	Refreshes the selected host.
Help	Opens the MMC online help.

View Menu

Menu item	Description
Customize	Enables customization of the View mode.

View Mode

Column	Description
Name	The machine name.
Current Owner	The current machine's "owner".
	User name, MAC address, or computer name of the client machine that currently uses this machine.
DNS Name	Specifies the machine's DNS.
Ericom Tools	Displays whether the VMAgent is running or not.
	Running, VMAgent is running and connected to this DeskView server.
	Disconnected, VMAgent was running and connected to this DeskView server but is currently disconnected.
	Unknown, VMAgent was never connected

	to this DeskView server.
Host	The host name.
Host Type	Specifies the Virtualization Server type.
IP Address	Specifies the machine's IP address.
	Microsoft Virtual Server will show this information only after the Ericom Tools is installed on the machine.
Login Status	Displays the machine's user status.
	Logout, the user is logged out.
	Connect/Disconnect, the user is logged in and connected/disconnected.
	Only enabled when Ericom Tools are installed.
Login User	Specifies the last logged in user.
	Only enabled when Ericom Tools are installed.
Operating System	Specifies the OS on the machine.
	Unknown, the OS is not known or the machine does not give this information.
State	Displays whether the machine is connected to the Virtualization Host or not.
Status	Displays whether the machine is running, stopped or paused.
	Changing, specifies an in-between mode.

19.5.2. Work with Hosts

To add a host:

- Right-click **Managed Hosts** and select **Add Host**. The **Add a New Host** wizard opens. Follow the wizard steps. For more information refer to the PowerTerm WebConnect Getting Started Guide.

To change the Windows Service account:

You need to change the Service account when working with Microsoft Virtual Server.

1. Open **Control Panel | Administrative Tools | Services** and locate **PowerTerm WebConnect DeskView Server**.
2. Right-click the service and select **Properties | Log on**.
3. Select **This account** and enter the account name that has the administrative permission for the MS Virtual Server with correlating **Password**.
4. Click **OK**.
5. Restart the PowerTerm WebConnect DeskView Server service.
6. Re-launch PowerTerm WebConnect Admin Tool and PowerTerm WebConnect Connection Broker Admin Tool if they are running.

To change the view:

1. Right-click any of the column headings and select **More**. The **Choose Columns** dialog opens.
2. Select the columns you want to appear in the view.
3. Clear the columns you want to remove from the view.
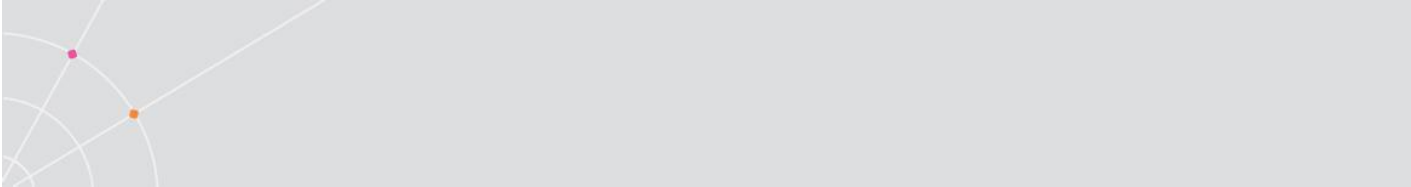4. Click **OK**.

To assign a MAC address as Owner:

The MAC address of selected computers/devices may be assigned directly to the hosted Desktop. This allows a "fixed seating" association where the hosted desktop may be accessed only by predetermined locations. More than one client device may be assigned to any host device. If there is no MAC address entered, fixed seating is disabled for this device.

1. Select the machine and right-click **Properties**.
2. Select the **Owners** tab.
3. Click **Add MAC Address** and enter the MAC address of the client machine to associate with.

To assign a DNS Name:

Another option of "fixed seating" association is to assign a client machine by its DNS name.

1. Select the machine and right-click **Properties**.

2. Select the **Owners** tab.

3. Click **Add DNS Name** and enter the DNS name of the client machine to associate with.

To assign a PC-over-IP client as Owner:

1. Select the machine and right-click **Properties**.

2. Select the **Owners** tab.

3. Click **Add PC-over-IP Client** and select the desired client to associate the host with.

To configure a 'free seating' user:

Selected users and groups based on Active Directory may be assigned directly to the hosted Desktop. This allows a "free seating" association where the host desktop may be accessed only by predetermined users from any location. More than one user or group may be assigned to any host device.
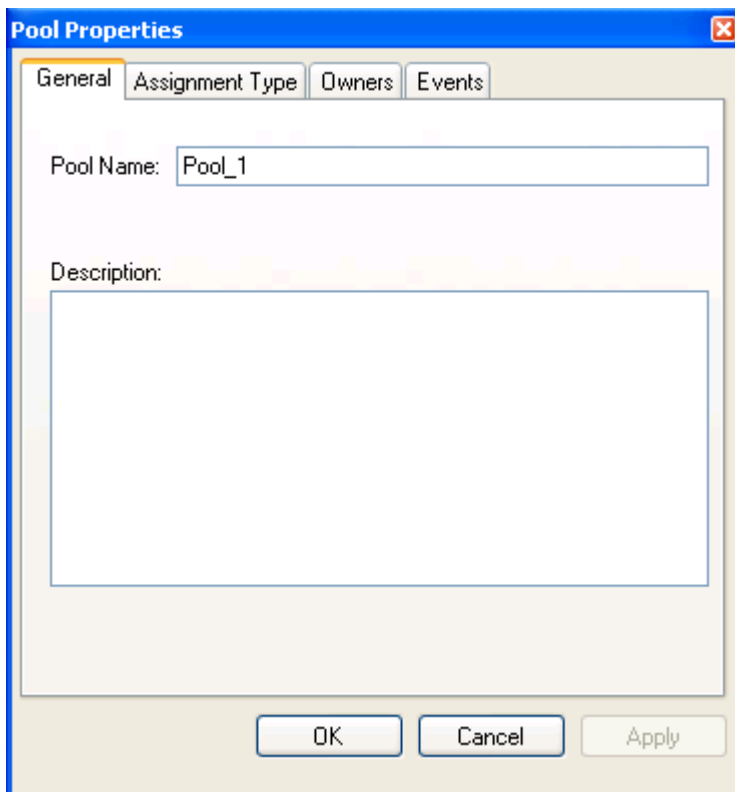
1. Select the device and right-click **Properties**.

2. Select the **Owners** tab.

3. Click **Add Users** and browse the **Directory Service** to find the desired user or group to be assigned.

19.6. Pools

Pools provide a method to organize devices into logical groups to be assigned to users. For example, devices hosting a sensitive HR application will be added to the HR Pool. The HR Pool is then assigned only to HR users in the Active Directory to secure the desktops.

19.6.1. Reference

Pool Properties Dialog

Field	Description
Pool Name	Specifies the pool's name.
Description	(Optional) Enter free-form information about the pool.
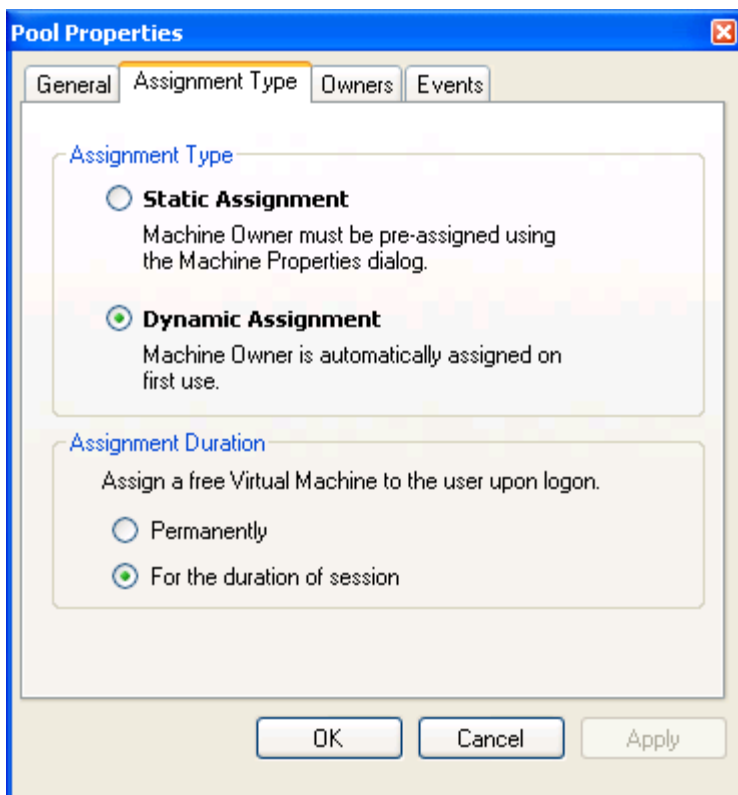
Field	Description
Static Assignment	Resources are manually mapped to users, computers, and MAC addresses.
Dynamic Assignment	A free resource in the pool will be assigned to the user making a request.
Permanently	The machine will be permanently assigned to the user, until the Administrator resets the mapping.
For the duration of session	The machine will be assigned to the user only for the specific session. After the user logs off the machine returns to the pool and will be available for the next user.
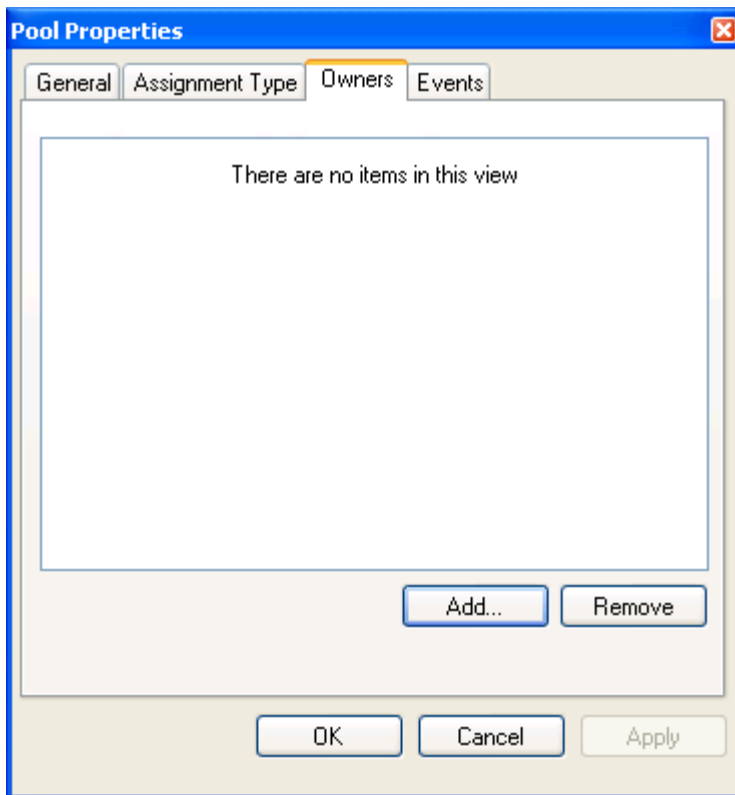
The Owners tab lists all the users and groups that have access to this resource.
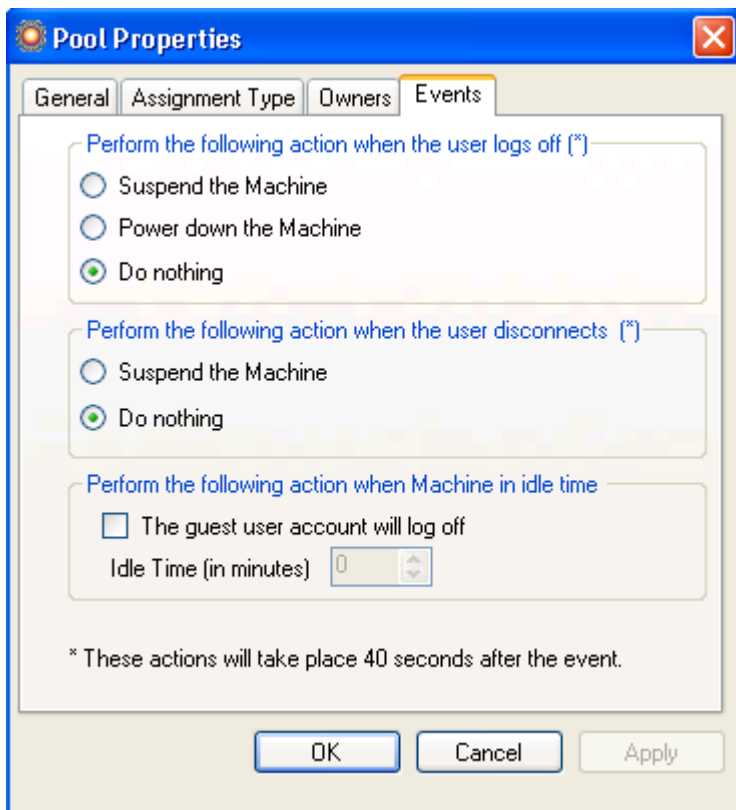
Option	Description
Suspend the Virtual Machine	Deactivates the virtual machine.
Power down the Virtual Machine	Shuts down the virtual machine

Assign Machine to Pool Dialog
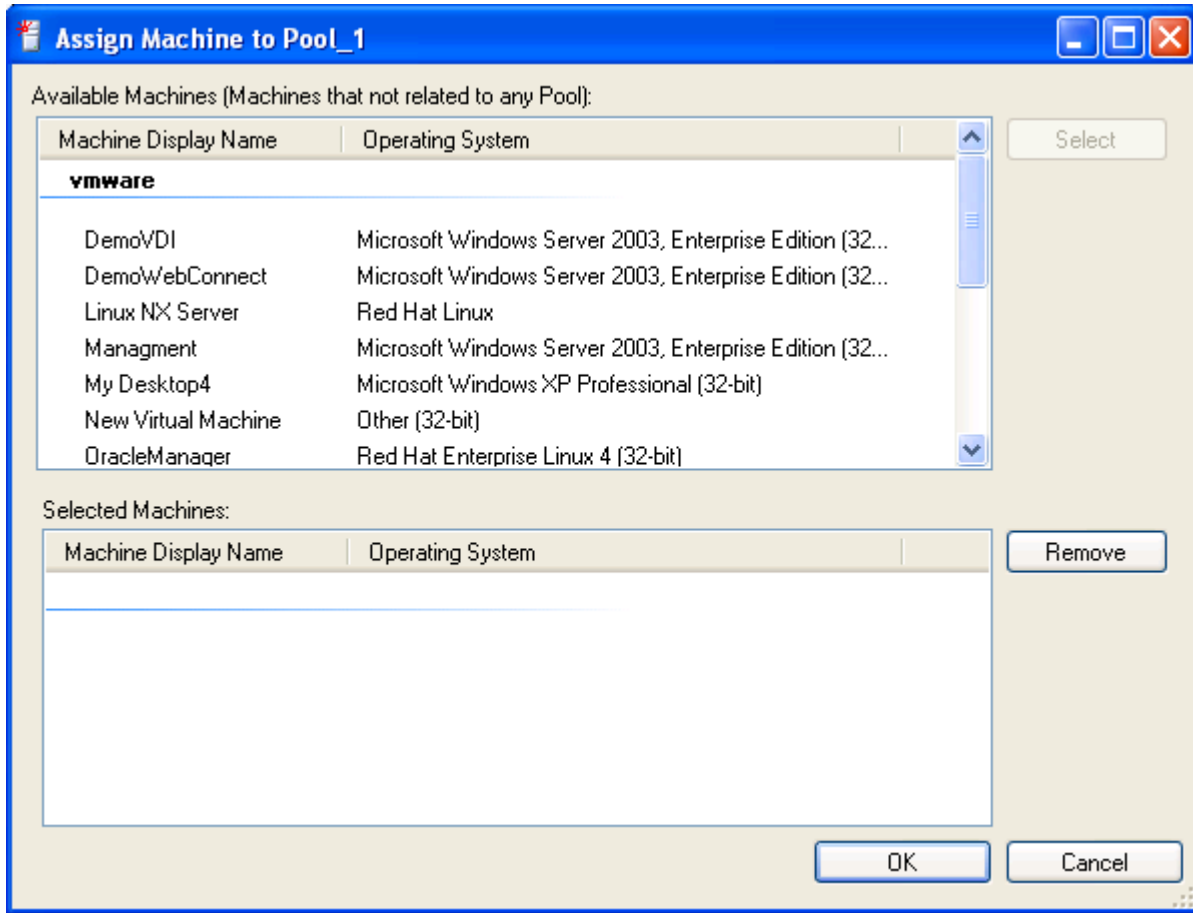
Field	Description
Available Machines	Shows the machines that are not yet assigned to any pool.
Selected Machines	Shows the machines assigned to this specific pool.

Action Menu

Menu item	Description
Properties	Opens the Host Properties dialog.
Assign Machines	Opens the Assign Machine to Pool

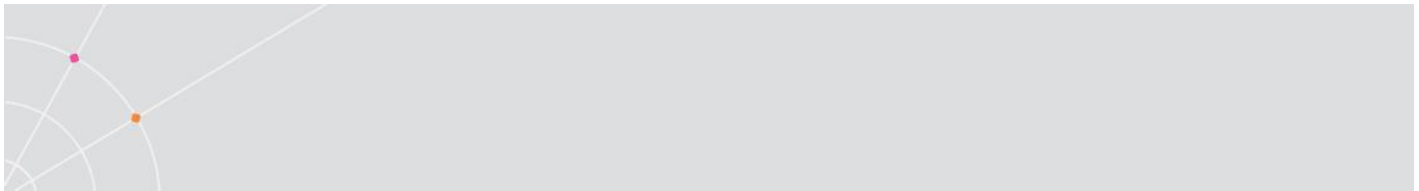|	dialog.
Import and Export	Imports/Exports the Owner's Pool configuration to/from a csv file.
Delete	Deletes the selected host.
Rename	Renames the selected host.
Refresh	Refreshes the selected host.
Help	Opens the MMC online help.

View Menu

Menu item	Description
Customize	Enables customization of the View mode.

View Mode

Column	Description
Name	The machine name.
Current Owner	The machine's "owner". Depending on the user's Assignment type this parameter can be permanent or temporary.
DNS Name	Specifies the machine's DNS.
Ericom Tools	Displays whether the VMAgent is running or not. **Running**, VMAgent is running and connected to this DeskView server. **Disconnected**, VMAgent was running and connected to this DeskView server but is currently disconnected. **Unknown**, VMAgent was never connected to this DeskView server.
Host	The host name.
Host Type	Specifies the Virtualization Server type.

IP Address	Specifies the machine's IP address.
	Microsoft Virtual Server will show this information only after the Ericom Tools is installed on the machine.
Login Status	Displays the machine's user status.
	Logout, the user is logged out.
	Connect/Disconnect, the user is logged in and connected/disconnected.
	Only enabled when Ericom Tools are installed.
Login User	Specifies the last logged in user.
	Only enabled when Ericom Tools are installed.
Operating System	Specifies the OS on the virtual machine.
	Unknown, the OS is not known or the machine does not give this information.
State	Displays whether the machine is connected to the Virtualization Host or not.
Status	Displays whether the machine is running, stopped or paused.
	Changing, specifies an in-between mode.
Task progress	A progress bar for **Status** changes.

19.6.2. Work with Pools

To add a pool:

- Right-click **Pools** and select **Create Pool**. The **Create a Pool** wizard opens. Follow the wizard steps. For more information refer to the PowerTerm WebConnect Getting Started Guide.

To change the view:

1. Right-click any of the column headings and select **More**. The **Choose Columns** dialog opens.

2. Select the columns you want to appear in the view.

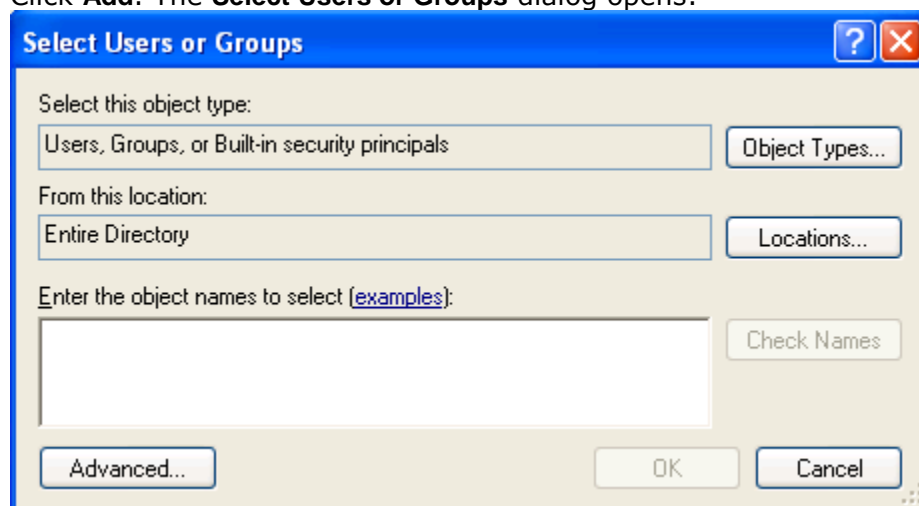3. Clear the columns you want to remove from the view.

4. Click **OK**.

To change an allocated user:

When you create a pool, you can decide that a machine will be permanently assigned to a specific user (/group/MAC Address/DNS name). However, you might want to change the assignment type.

1. Right-click **Properties** for the machine that you want to change Allocation Status. The **Machine Properties** dialog opens.

2. Click **Remove Owner** in the **Owner** tab. **Current Owner** field is emptied and **Assignment Time** will show current time.

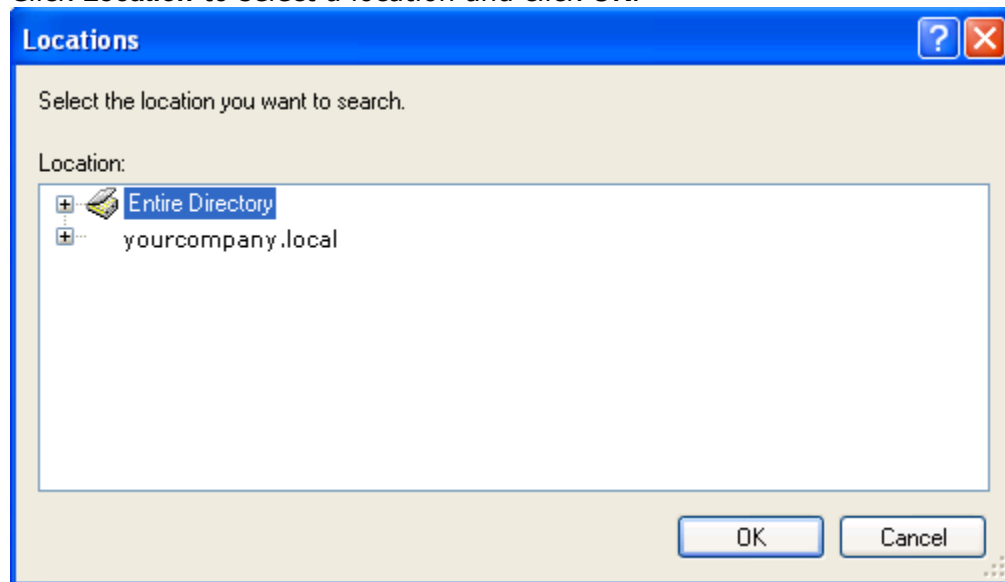3. Click **OK**.

To add an owner to the pool:

1. Right-click **Properties** on the machine that you want to add owners and select the **Owners** tab.

2. Click **Add**. The **Select Users or Groups** dialog opens:

3. If desired, click **Object Types** to select an object and click **OK**.

Object Types

Select the types of objects you want to find.

Object types:

☑ Built-in security principals
☑ Groups
☑ Users

OK   Cancel

4. Click **Location** to select a location and click **OK**.

Locations

Select the location you want to search.

Location:

⊞ Entire Directory
⊞   yourcompany.local

OK   Cancel

5. Enter an object name. You can click **Check Names** to verify that the entered object exists.

6. If the object is not found, click **Advanced** to search users/groups.

7. Click **OK**. The user/group was added.

To remove an owner :

1. Right-click **Properties** on the machine that you want to add owners and select the **Owners** tab.

2. Select the owner you want to remove and click **Remove**. The user/group is deleted from the list.

19.7. Client Machines

19.7.1. Reference

Field	Description

General	Specifies the machine details.
System Information	Specifies the system details.
Login Status	Specifies the last logged user details.
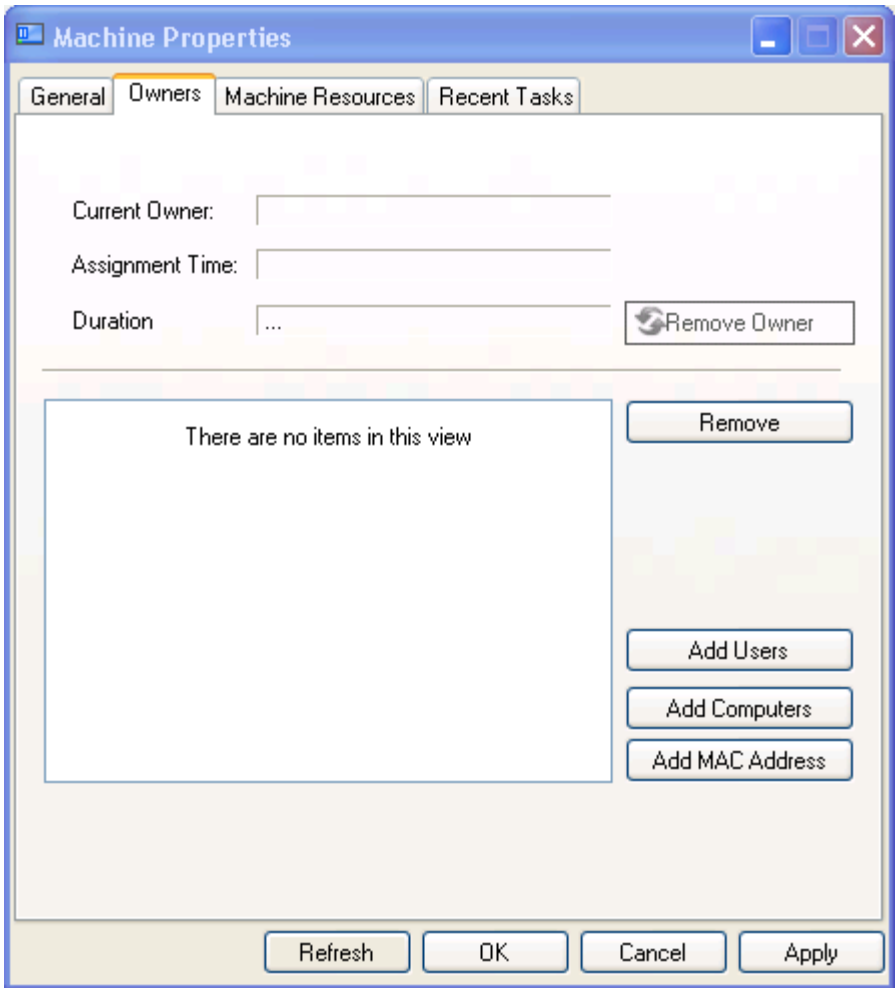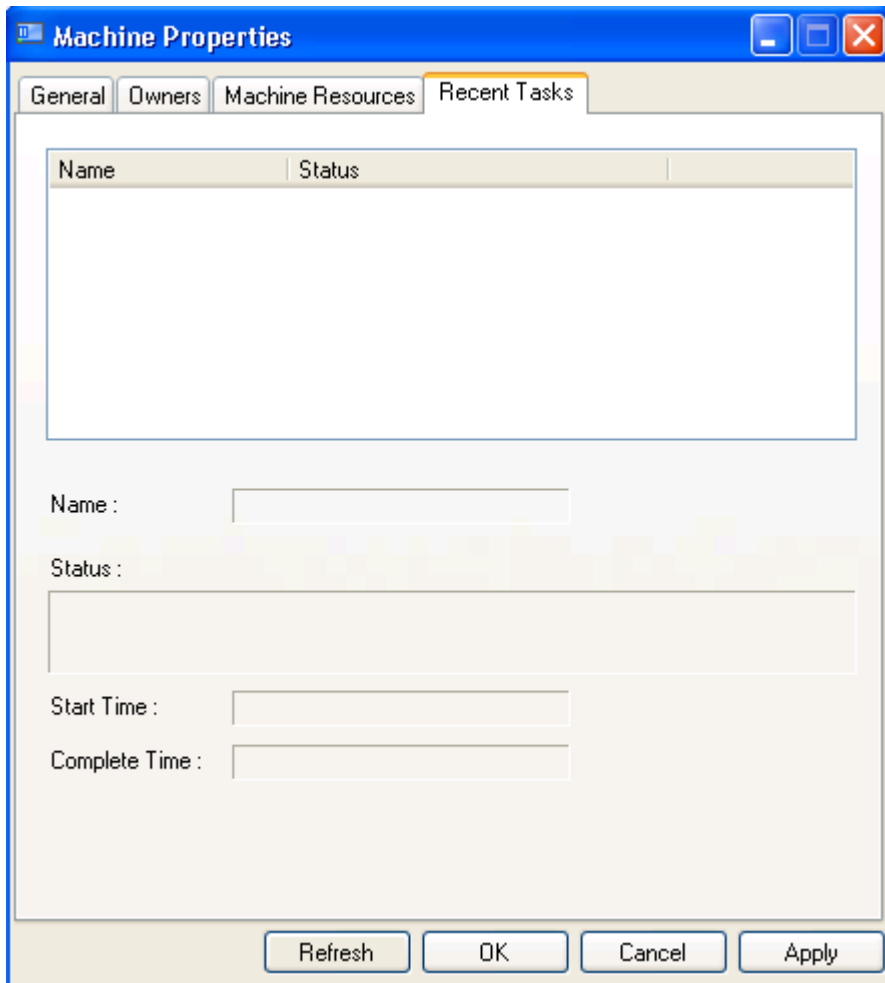
Field	Description
Current Owner	Specifies which user/MAC/computer is the owner of this machine.
Assignment Time	Specifies the last time the Current Owner was changed.
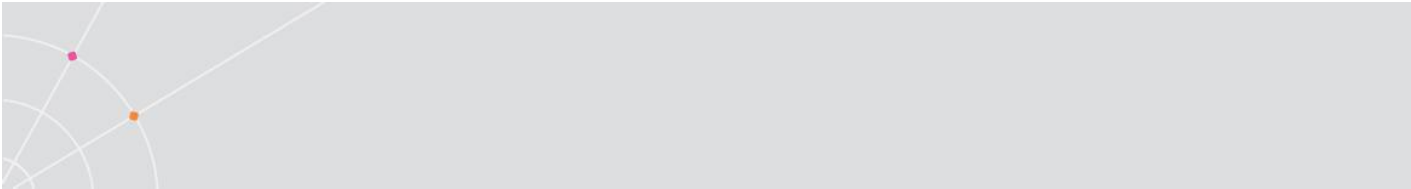
Owner's View	Lists the users/MACs/computers that have the right to take this machine.
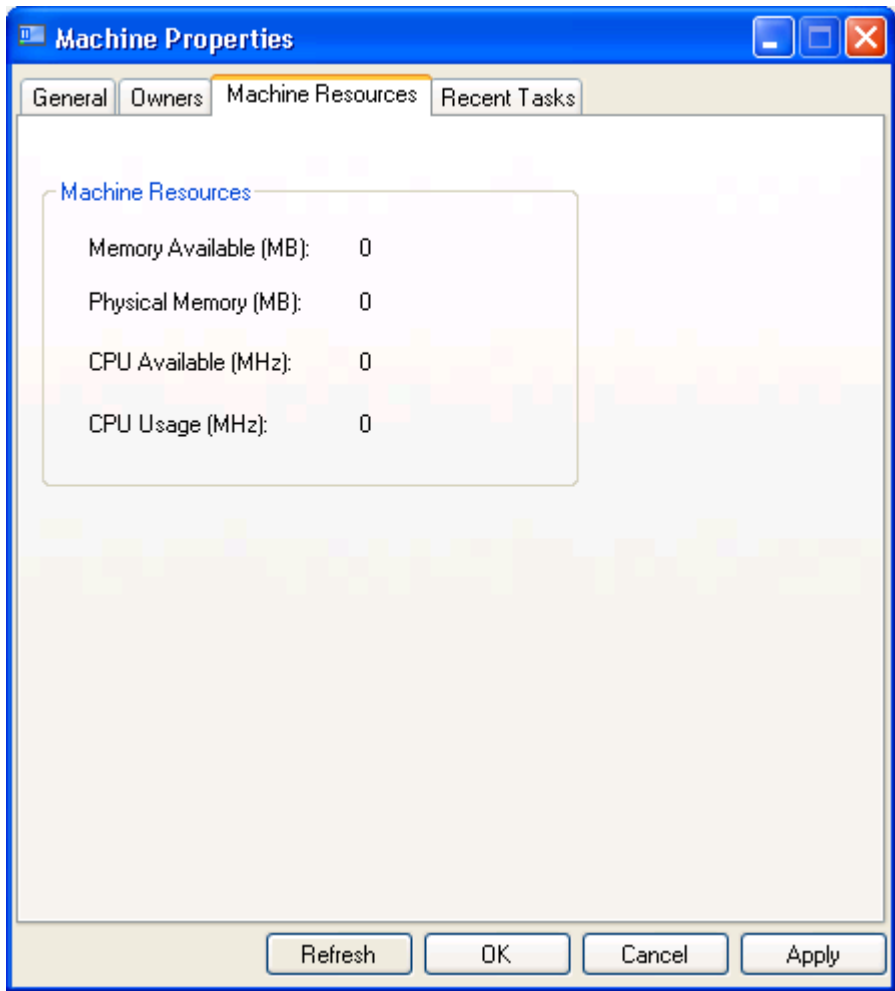
The Machine Resources tab specifies the machine's resource details.

Field	Description
Recent Tasks table	Lists the machine's events.
Name	Specifies the operation (e.g. start, stop, etc.)
Status	Indicates the operation status (e.g. success, failed, pending, etc.)
Start Time	Specifies the operation's starting time.
Complete Time	Specifies the operation's total time.

19.7.2. Work with Clients

To add an owner to the machine:

1. Right-click **Properties** on the machine that you want to add owners and select the **Owners** tab.

2. Click **Add User**. The **Select Users** dialog opens:
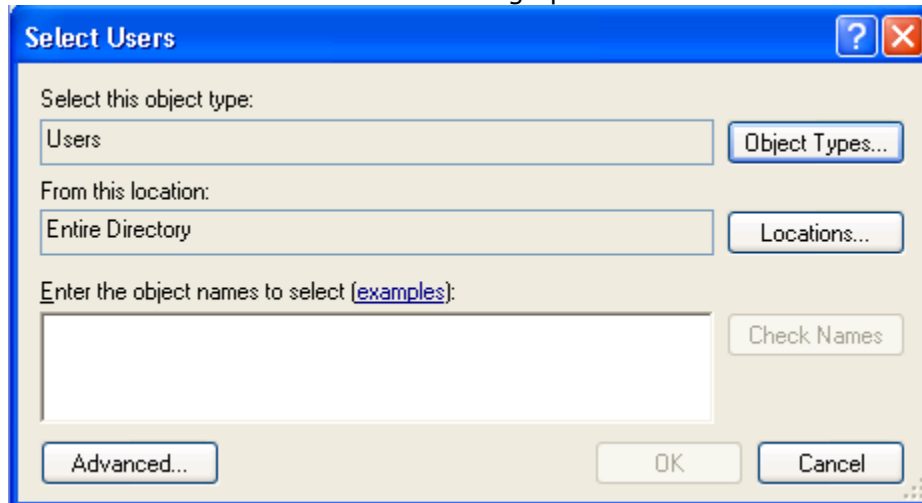
3. If desired, click **Object Types** to select an object and click **OK**.
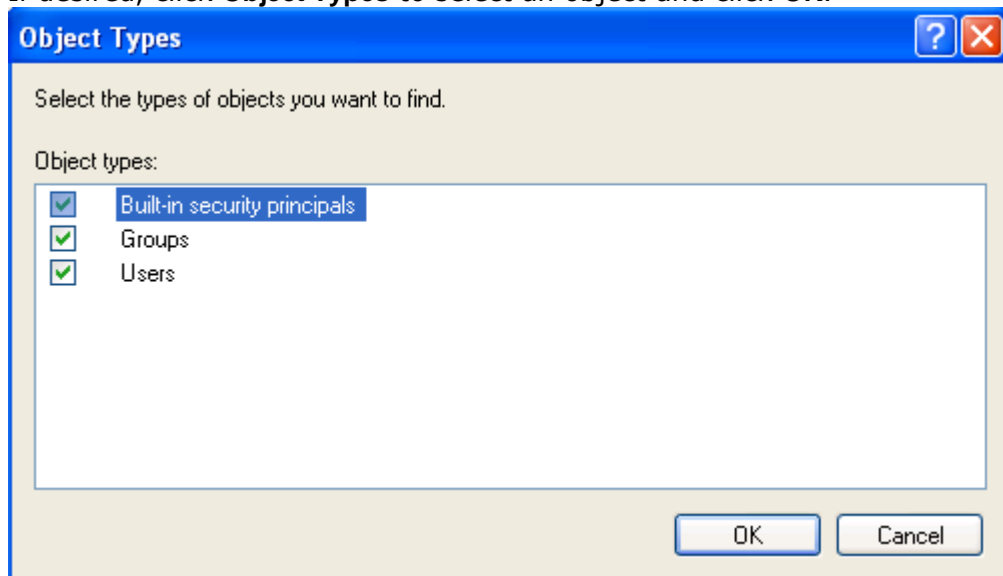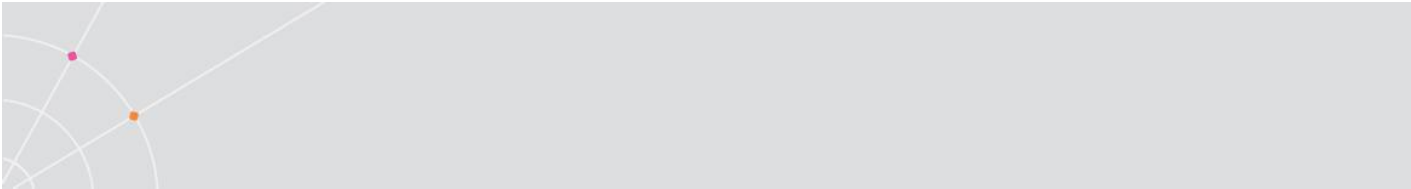
4. Click **Location** to select a location and click **OK**.
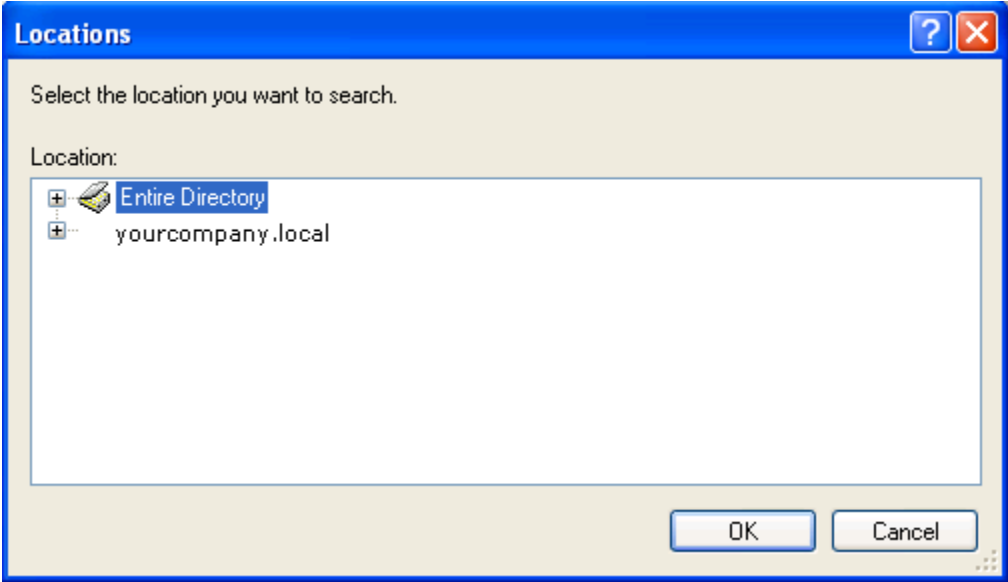
5. Enter an object name. You can click **Check Names** to verify that the entered object exists.

6. If the object is not found, click **Advanced** to search users/groups.

7. Click **OK**. The user/group was added.

19.8. Troubleshooting

When I try to connect from the PC-over-IP client I get a message that "No Machines are available".

- Verify that PC-over-IP Host guest OS is not logged in by another user.

- Verify that Ericom Tools are installed on PC-over-IP Host guest OS.

- Verify that CurrentOwner is empty or defined to the end user PC-over-IP client.

The hosted resource must be assigned properly for access:

Set Owner	Device Properties	Pool Properties
User		X
MAC	X (Enter MAC)	
User and MAC	X (Enter MAC)	X

- If there is no MAC address assigned to a host, it is available for "User and MAC" access.

- If there is a MAC address assigned, only users part of the associated Pool connecting from the specified MAC address may connect to the device.

I have two entries in my Device assignment. Does this mean that the user must meet both requirements?

No, only one of the conditions needs to be met for access to the device. For example, if your Properties page looks like the following:
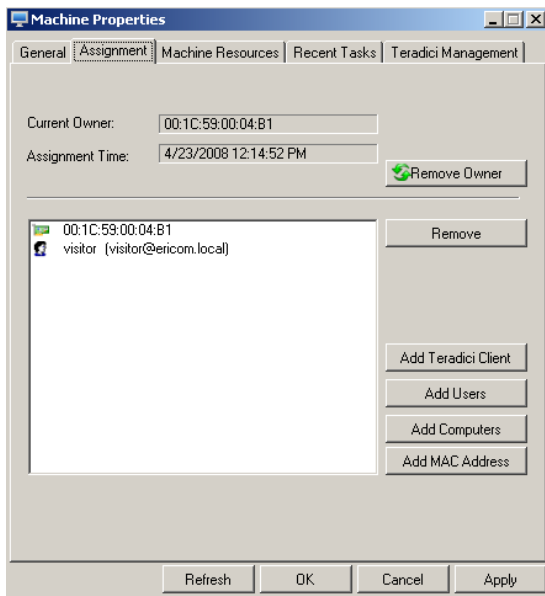
Any user can access the device from the "fixed seating" client, or, the user "visitor" can connect from any device.

20. Working with IBM Lotus Expeditor

20.1. Installation Package

PowerTerm WebConnect client for Lotus Expeditor is provided in an Update Site package. This is a ZIP archive containing the Update Site with the Eclipse features and plug-in, that comprises the PowerTerm WebConnect client.

- Extract the ZIP file, keeping the folders' structure intact.

NOTE   In Winzip, verify that the "Use folder names" option is set to TRUE.

Package structure

```
Update Site

    - plugins

          - PowerTermWebConnectClient_5.6.0.365.jar

    - features

          - com.ericom.WebConnect_5.6.0.365.jar

    - site.xml

config

    - webconnect.xml
```
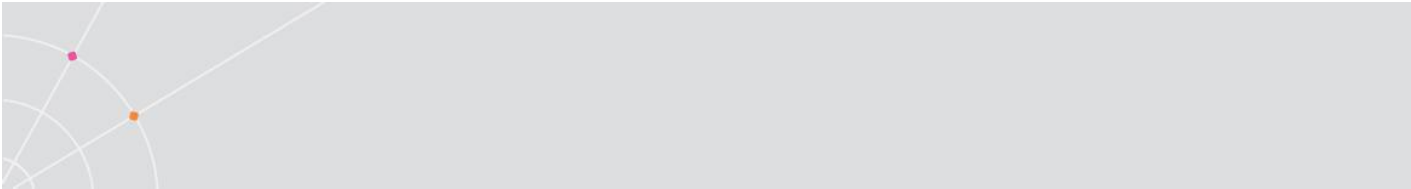
Definitions

- **webconnect.xml**, PowerTerm WebConnect client configuration file
- **com.ericom.WebConnect_5.6.0.365.jar**, PowerTerm WebConnect client feature file
- **PowerTermWebConnectClient_5.6.0.365.jar**, PowerTerm WebConnect client plugin file

20.2. Pre-installation Steps

PowerTerm WebConnect client for Lotus Expeditor does not run independently, but in conjunction with PowerTerm WebConnect Server. You can either install it and define your users, groups, and applications or use Ericom Software's Demo PowerTerm WebConnect Server.

- If you decide to install PowerTerm WebConnect Server, you will need the full installation, i.e. the PowerTerm WebConnect Server and the Web components. If

you do not have the installation CD, you can download and install a trial version from www.Ericom.com.

- If you decide to use Ericom Software's Demo PowerTerm WebConnect Server, then skip to *Installing PowerTerm WebConnect Client on Lotus Expeditor*.

20.3. Installing PowerTerm WebConnect Client on Lotus Expeditor

1. Start the Lotus Expeditor client.

2. Select **File | Application | Install**.

3. Select **Add Folder Location**, and type or select the location of the **Update site** folder from the provided package. Click **OK**.

4. Select the location you have just created, and click **Finish**.

5. In the **Select the feature to install** tree, select **PowerTerm WebConnect/Update Site**. Click **Next**.

6. Select **I accept the terms** in the license agreements and click **Next**.

7. Click **Finish**.

8. When prompted, restart the platform.

20.4. Running PowerTerm WebConnect Client for Lotus Expeditor
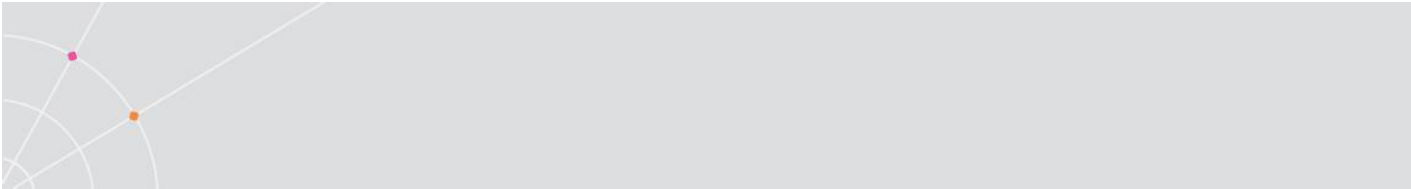
1. Click **Open**. The **PowerTerm WebConnect** option is displayed.

2. Select **PowerTerm WebConnect**. The application will automatically connect and start downloading the components from PowerTerm WebConnect Server.

IMPORTANT

If you did not install PowerTerm WebConnect Server, and are instead connecting to Ericom Software's Demo WebConnect Server then you need to open port 443 in the firewall.

20.4.1. PowerTerm WebConnect Client Workflow

PowerTerm WebConnect client reads the URL of webconnect.xml from the **preferences.ini** file and requests it.

When the webconnect.xml is successfully downloaded, the application reads the configuration, connects to the specified Web server, downloads the PowerTerm WebConnect components, and connects to the PowerTerm WebConnect Server.

The user is requested to login to the PowerTerm WebConnect Server. For testing, you can use the username `Example` and password `example`.

NOTE   This step will be skipped if Single Sign-on is set to "true".

After logging in to PowerTerm WebConnect Server, the user's applications are displayed as defined by the administrator.

To run an application, select the desired application from the list and click **Launch** or double-click the application. The application will be launched in a separate window.

20.5. Troubleshooting

When you encounter a problem, the first step is to open the log file. This file is located on the client machine, in the **Ericom** folder.

Windows:

C:\Documents and Settings\<username>\Ericom\leclient\EricomPlugin.log

Linux:

<user-home-directory>/Ericom/leclient/EricomPlugin.log

Following is a guide for diagnosing and fixing the problems in cases of error messages, and additional information:

Error message	Solution
Version file reading error	Check the **url** parameter in the **webconnect.xml** file on the Web server. the value should be:
	http://<WebServerIP>/WebConnect
	Try to run the following URL on the browser:
	Windows:
	http://<WebServerIP>/WebConnect/windows/ptagent.ver.txt
	Linux:
	http://<WebServerIP>/WebConnect/linux/ix86/qterm-wc.ver.txt
	The file contents displayed in the browser window should be in the following form:

	`5.6.0-rel.14546`
	`PowerTerm WebConnect Application Zone`
	`5.6.0 – Main Release`
	`<root>/PowerTerm WebConnect 5.6/<WebServer>`
	If the version file contents are not as shown, check:
	- Is the Web Server running?
	- Are PowerTerm WebConnect Web Components and version files in place?
	On the Web server, check **<PowerTerm WebConnect root>\web\windows\ptagent.ver.txt**. If the contents "look wrong" or not in the proper form, reinstall the PowerTerm WebConnect Web components.
	On the client machine, open the aforementioned URL in the browser. The file content should appear in the browser. If it does not it could be that the Web server is down.
Web Server is shut down	The **webconnect.xml** configuration file must be located on the Web server. The explicit URL to this file is defined in the **preferences.ini** file.
	The error message contains the IP address of the Web server. Verify that the Web server on this machine is running.
Version file does not exist on <URL>	See Version File reading error.
The configuration file is not accessible or has a wrong format	The **webconnect.xml** configuration file must be located on the Web server and the explicit URL to the configuration must be defined in the **preferences.ini** file.
	Try to open the URL specified in the error message in the browser. If it does not open then it either does not exist or it has a wrong format.
Preferences file does not exist in the application bundle	The **preferences.ini** file, containing the URL to the configuration file, was removed from the **Update site** folder.
	Uninstall the current PowerTerm WebConnect client from the client machine. Create a new customized package and reinstall it.
Configuration file URL is	The URL to the configuration file does not appear in the

not defined in the Preference file	**preferences.ini** file.
	Uninstall the current PowerTerm WebConnect client from the client machine. Create a new customized package and reinstall it.
No IP address could be found for the host	The Web server URL, specified in the **preferences.ini** file or in the **webconnect.xml** file is an unknown host.
	If the mistake is in the preferences.ini file, uninstall the current PowerTerm WebConnect client from the client machine. Create a new customized package and reinstall it.
	If the mistake is in the webconnect.xml file, correct the file and reopen the Lotus Expeditor client.
Cannot write to destination	The temporary file cannot be written to the defined destination. Check the write permissions.
Copied configuration file has wrong format	The **webconnect.xml** file, as received from the specified URL, has a wrong format. Correct the file and try again.
PowerTerm WebConnect Agent URL is malformed	The PowerTerm WebConnect Agent URL, specified in the **webconnect.xml** file does not have a proper HTTP format. Correct the file and try again.
PowerTerm WebConnect Agent URL is not defined	The PowerTerm WebConnect Agent URL parameter is not specified in the **webconnect.xml** file. Correct the file and try again.
The specified destination folder name is wrong	The destination folder name contains illegal characters:
	/ \ : * ? < >	
	Check the **dst** parameter in the **webconnect.xml** file. Correct the file and try again.
You do not have permissions to write to <path>	The PowerTerm WebConnect Agent cannot be written to the destination as defined. Check the write permissions.
	The default destination defined in the version file, should not be changed.
	A customized destination for PowerTerm WebConnect Agent downloading can be defined in the **webconnect.xml** file.
	Check the destination value, correct and try again.

21. Working with PowerTerm WebConnect Portlet

21.1. On IBM Workplace Server for Windows OS

Step 1: Install PowerTerm WebConnect Server

If PowerTerm WebConnect Server and IBM Workplace Server reside on separate machines:

- Configure PowerTerm WebConnect Server:
  Launch PowerTerm WebConnect Administration Tool.
  Open **Files | Configuration | Main**.
  In the **[Portal]** section, edit:
  `Machines=localhost;<IBM server machine>`

- Configure PowerTerm WebConnect Web components:
  Copy the **web** folder from the PowerTerm WebConnect server installation to the IBM Workplace server machine.
  Create an **Alias**, or a Virtual directory to it, named WebConnect, on the Web server, providing access to it, for the users. This is in order to enable the users to download the necessary files to run their applications

Step 2: Enable JSR Portlets

1. On IBM Workplace Server, go to
   <PortalServer>\shared\app\config\services\ConfigService.properties

2. Edit `portal.enable.jsr168=true`

3. Save and close the file

Step 3: Enable SSO

1. On IBM Workplace Server, go to
   <PortalServer>\shared\app\config\services\LoaderService.properties

2. Edit
   `command.path=com.ericom.portal.commands,com.ibm.wps.engine.commands`

3. Save and close the file.

Step 4: Copy Files

The following files need to be copied from PowerTerm WebConnect **Server/AddOns/IBM Workplace/Portlet** folder to IBM Workplace Server:

File name to copy	Destination folder
OpenSSL.dll	<AppServer>/java/jre/bin
IbmPortal.dll	<AppServer>/java/jre/bin
IbmPortal.ini	<AppServer>/java/jre/bin
WebConnectPortal.jar	<AppServer>/lib/
EricomLogin.jar	<PortletServer>/shared/app

Step 5: Portlet Configuration

1. On IBM Workplace Server, go to **<AppServer>/java/jre/bin/IbmPortal.ini**

2. You can modify the following parameters in the **[Server=WebConnect]** section:
   web.server.port=<IBM web server port>
   Specifies the Web server port for accessing the PowerTerm WebConnect clients folder.
   Default: 80
   Address
   Specifies the address of the PowerTerm WebConnect Server machine for Portlet to connect to, when PowerTerm WebConnect Server is located on a different machine than the IBM Workplace Server.
   CustomAddress
   Specifies the address of the PowerTerm WebConnect Server machine for Clients to connect to. If **CustomAddress** is the same as **Address** then this may be omitted.
   web.server.addr
   Specifies the address of the Web Server machine, when it is located on a different machine than the IBM Workplace Server.

3. Restart the IBM server:
   ```
   <PortalServer>/rootscripts/stopWorkplaceServices.bat
   <PortalServer>/rootscripts/startWorkplaceServices.bat
   ```

NOTE   This procedure may take about 20 minutes.

Step 6: Install the Portlet

1. In a Web browser open the URL **http://<IBM Workplace Server>:9081/lwp/myworkplace** to open the IBM Workplace Portal.

2. Login as administrator.

3. Go to **Administrator | Portlets | Install**.

4. Browse to the P**owerTerm WebConnect.war** file, located on PowerTerm WebConnect Server, and click **Next**.

5. Click **Install**.

Step 7: Create an Application Page

1. Login to the Workplace.

2. Go to **Portal User Interface | Manage Pages**.

3. Search for **My Work**.

4. Click the **My Work** link and select **New Page**.

5. Name the page **PowerTerm WebConnect** and click **OK**.

6. Click **OK** again. You will see the created page on the list.

7. Click the pencil icon on the new page and select the 1 square layout.

8. Click **Add Portlet** and search for PowerTerm WebConnect.

9. Select it and click **OK**.

10. Click **Done**.

11. Click **My work** at the top of the page. PowerTerm WebConnect is displayed on the list.

Step 8: Run the Portlet

1. Restart IBM Workplace Server.

2. Open IBM Workplace Portal in a browser: **http://<portal server>/lwp/myworkplace**

3. Login to IBM Workplace Server.

4. Click **My work**. PowerTerm WebConnect portlet is displayed.

5. Launch it. The user's applications, as defined on PowerTerm WebConnect Server, appear.

6. Click an application to launch it.

21.2. On IBM Workplace Server for Linux OS

Step 1: Enable JSR 168 Portlets

1. Go to
   **/opt/IBM/Workplace/PortalServer/shared/app/config/services/ConfigService.properti
   es**

2. Modify `portal.enable.jsr168 = true`.

3. Restart the server:
   ```
   cd /opt/IBM/Workplace/PortalServer/rootscripts
   run ./stopWorkplaceServices.sh
   run ./startWorkplaceServices.sh
   ```

NOTE   This procedure can take up to 20 minutes!

4. Log on to the workplace server at **http://<workplace
   server>:9081/lwp/myworkplace** using the administrator's username and
   password.

Step 2: Install the Portlet

1. Restart IBM Workplace Server.

2. In a Web browser open the URL **http://<workplace server IP>/lwp/myworkplace**.

3. Login to IBM Workplace Server as an administrator.

4. Go to **Administration | Portlets | Install**.

5. Browse to the **PowerTerm WebConnect.war** file, located on PowerTerm
   WebConnect Server, and click **Next**.

6. Click **Install**.

Step 3: Install the Application Page

1. Login to the workplace as administrator.

2. Go to **Administration | Portal user Interface | Manage Pages**.

3. Search for **My Work**.

4. Click the My Work link and select **New Page**.

5. Name the page **PowerTerm WebConnect** and click **OK**.

6. Click **OK** again. You will see the created page on the list.

7. Click the pencil icon and select the 1-square layout.

8. Click **Add Portlet** and search for PowerTerm WebConnect.
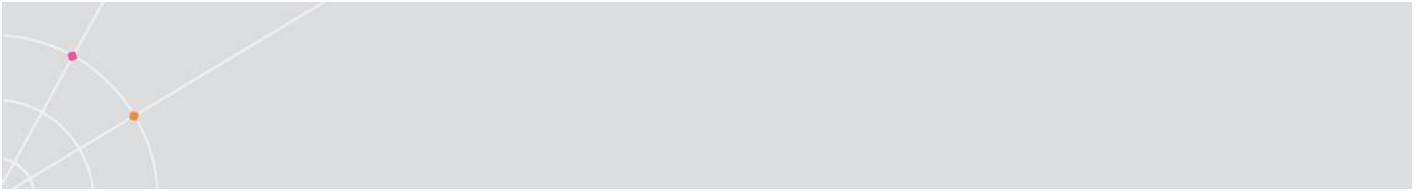
9. Select it and click **OK**.

10. Click **Done**.

11. Click **My Work** on top and PowerTerm WebConnect is displayed on the left bar.

Step 4: Run the Portlet

1. Restart IBM Workplace Server.

2. Open IBM Workplace Portal in a browser: **http://<portal server>/lwp/myworkplace**.

3. Login to IBM Workplace Server.

4. Click **My Work**. PowerTerm WebConnect Portlet is displayed.

5. Launch it. The User's applications, as defined on PowerTerm WebConnect Server, appear.

6. Click an application to launch it.

21.3. On IBM WebSphere 6.1 Server for Windows OS

Step 1: Install PowerTerm WebConnect Server

You have to configure PowerTerm WebConnect Server if it and the IBM WebSphere Server are on separate machines:

1. Launch PowerTerm WebConnect Administration Tool.

2. Open **Files | Configuration | Main**.

3. In the **[Portal]** section, edit:
   ```
   Machines=localhost;<IBM Server machine>
   ```

Step 2: Copy Files

The following files need to be copied from **WebConnect Server/AddOns/IBM WebSphere/Portlet** folder to IBM WebSphere Server:

File name to copy	Destination folder
openSSL.dll	<AppServer>/java/jre/bin/
ibmPortal.dll	<AppServer>/java/jre/bin/
ibmPortal.ini	<AppServer>/java/jre/bin/
WebConnectPortal.jar	<AppServer>/lib/

Step 3: Portlet Configuration

1. On IBM Workplace Server, go to **<AppServer>/java/jre/bin/IbmPortal.ini**.

2. You can modify the following parameters in the **[Server=WebConnect]** section:
   web.server.port=<IBM web server port>
   Specifies the Web server port for accessing the PowerTerm WebConnect clients folder.
   Default: 80
   Address
   Specifies the address of the PowerTerm WebConnect Server machine for Portlet to connect to, when PowerTerm WebConnect Server is located on a different machine than the IBM Workplace Server.
   CustomAddress
   Specifies the address of the PowerTerm WebConnect Server machine for Clients to connect to. If **CustomAddress** is the same as **Address** then this may be omitted.
   web.server.addr
   Specifies the address of the Web Server machine, when it is located on a different machine than the IBM Workplace Server.

3. Restart the IBM server:
   ```
   <AppServer>/Profiles/AppServer01/bin/stopServer.bat
   <AppServer>/Profiles/AppServer01/bin/startServer.bat
   ```

NOTE   This procedure may take about 20 minutes.

Step 4: Install the Portlet and Create and Application Page

1. In a Web browser open the URL **http://<IBM WebSphere Server>:9060/ibm/console** to open the IBM WebSphere Portal.

2. Login and go to **Applications | Install New Application**.

3. Browse to the **PowerTerm WebConnect.war** file, located on PowerTerm WebConnect Server.

4. Enter **Context root**, and click **Next**. The **Select installation options** dialog appears.

5. Optional, change options to your preference or keep the default.

6. Click **Next**.

7. Select **Ericom** in the **Module column**.

8. Click **Apply** and then **Next**.

9. Click **Finish** and then **Save**.
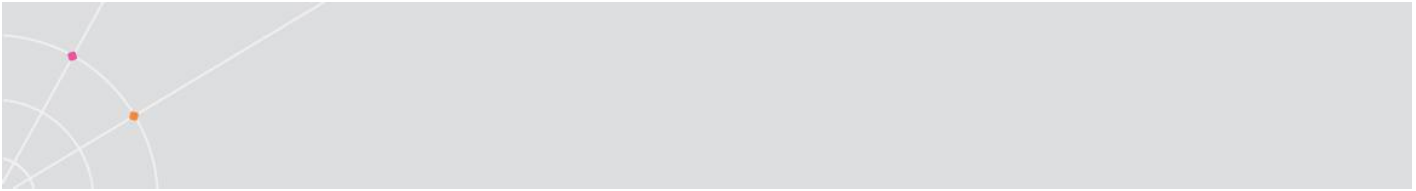
10. Select **Applications | Enterprise Applications**.

11. Select **PowerTerm WebConnect.war** checkbox and click **Start**.

12. Enter, in the Web browser, the URL **http://<IBM WebSphere Server>:9080/<Context root>/Ericom portlet**. The **Login** dialog appears.

13. Login and you will see PowerTerm WebConnect displayed on the list.

Step 5: Run the Portlet

1. Restart IBM WebSphere Server.

2. Open IBM WebSphere Portal in a browser: http://<portal server>:9080/<Context root>/Ericom portlet.

3. Login to IBM WebSphere Server.

4. Launch it. The User's applications, as defined on PowerTerm WebConnect Server, appear.

5. Click an application to launch it.

21.4. PowerTerm WebConnect Server Configuration

To enable the Lotus Expeditor to run the PowerTerm WebConnect client, the System Administrator must provide the users with accounts on PowerTerm WebConnect Server (see the PowerTerm WebConnect Administrator's Manual for detailed instruction on how to create users, groups, and connections on the PowerTerm WebConnect Server.)

To enable PowerTerm WebConnect's Single Sign-on feature, the System Administrator must create a PowerTerm WebConnect user with the same username and password as used for the Lotus Expeditor. For a managed Lotus Expeditor the credentials used are the username and password sent to the managing server. For an unmanaged Lotus Expeditor, the operation system username and the Lotus Expeditor password are used as credentials.

> NOTE   If a password is not defined then the Single Sign-on will fail and the user will be prompted with a Login dialog.

21.5. PowerTerm WebConnect Client Configuration

The PowerTerm WebConnect Client is configured in **webconnect.xml**, located in the **config** folder. The parameters are:

url	The PowerTerm WebConnect Agent url
server	The PowerTerm Server address
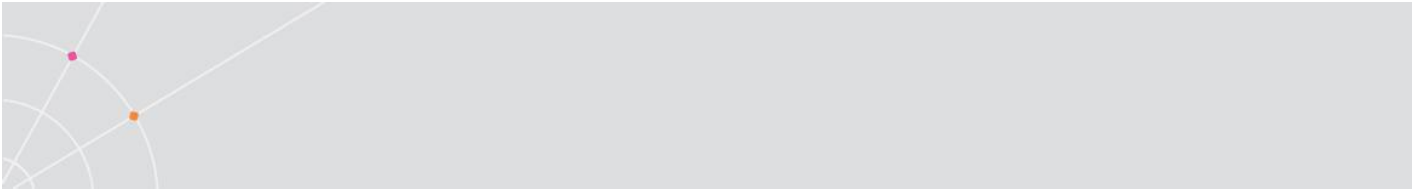
sso	The Single Sign-on feature
dst	The local destination for downloading PowerTerm WebConnect components.

url

PowerTerm WebConnect components are installed on a Web server. Their default url is:

Windows Agent:

```
http://<WebServer IP>/WebConnect/windows/ptagent.cab
```

Linux Agent:

```
http://<webServer IP>/WebConnect/linux/ix86/qterm-wc.zip
```

The url parameter must include the first part of the url (which is identical for both Windows and Linux agents.)

The PowerTerm WebConnect client will automatically append the appropriate suffix, in order to create a full accurate url.

Example:

```
<item key="url" value=http://adminserver/WebConnect/>
```

server

The computer name or IP address of the PowerTerm WebConnect Server machine.

The PowerTerm WebConnect client will log in to this PowerTerm WebConnect Server, display the applications defined on it, and run them according to t his server's configuration.

Format: `<server IP>[:<port>]`

Where default port is 4000 (can be edited)

Example:
```
<item key="server" value="admin2:4000"/>
```

sso

Determines whether Single Sign-on will be used to log in to PowerTerm WebConnect Server.
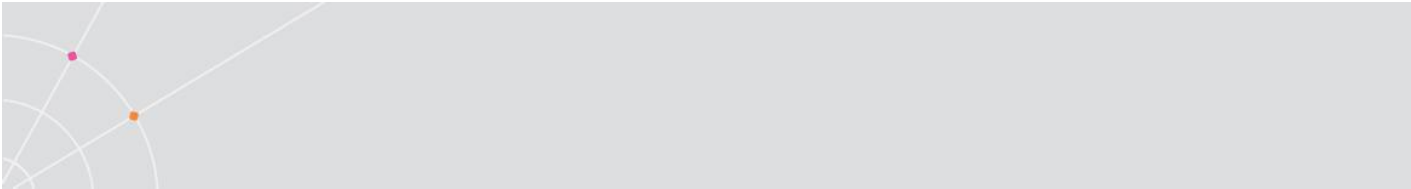
Values:

- **True** (default), the client should automatically log in to PowerTerm WebConnect Server using the same credentials as the ones used to log in to the Lotus Expeditor client.

> NOTE The System Administrator must verify that these credentials can log in to the PowerTerm WebConnect Server.

- **False**, the user will be prompted with a Login dialog, or will log in automatically using previously saved credentials.

Example:

```
<item key="sso" value="true"/>
```

Autologin mode:

If **sso** is set to **True**, the user is not prompted for credentials and the login process to PowerTerm WebConnect Server is done automatically, sending the credentials used for the Lotus Expeditor, unless the Lotus Expeditor does not have a password defined. (In the Lotus Expeditor **preferences page | Password | Prompt me for a password at start up** checkbox.)

However, if Single Sign-on is not used, there are several options regarding **Autologin** that can be defined in the PowerTerm WebConnect Preferences page.

Options:

- **Yes**

- **No**

- **Interactive**

- **First time interactive** (default) – Simplifies the login process to PowerTerm WebConnect Server. In this mode, the first time the user logs in to PowerTerm WebConnect Server, he will be prompted for his credentials with the Login dialog. These credentials will be stored in the machine, and from then on, the login process to PowerTerm WebConnect Server will be done automatically.
  1. Open **File | Preferences** from the Lotus Expeditor and select **PowerTerm WebConnect**.
  2. In the **Autologin to WebConnect Server** section, select **First Interactive** and click **OK**.
  3. Start PowerTerm WebConnect Client for Lotus Expeditor. If credentials were entered at least once, then the next time the client will connect to PowerTerm WebConnect Server without prompting for the user name and password.

> NOTE The Administrator must configure the Agent to do nothing when it exits fro the feature to work this way.

- **Allow multiple selection** – Defines whether the user can launch more than one application at a time (by using the **<Ctrl>** or **<Shift>** button while selecting applications.

dst

Defines the path to download PowerTerm WebConnet components on the client machine. The **dst** parameter can contain macros which are translated by the PowerTerm WebConnect Client for Lotus Expeditor during runtime. The macros should be placed between percent symbols (%), for example: `%WebServer%`

When such a value is defined, the PowerTerm WebConnect Client for Lotus Expeditor substitutes the entire expression for the macro's value.

> NOTE The PowerTerm WebConnect Client for Lotus Expeditor does not support the use of environment variables as macros.
>
> NOTE Macros are not case sensitive.

Macros supported by PowerTerm WebConnect Client for Lotus Expeditor

Macro name	Description
WebServer	The name of the Web server.
	It is obtained from the PowerTerm WebConnect Agent url parameter.
Name	The name of the client's CAB or ZIP file, e.g. "ptagent".
Display	The client's display name from the version file.
Root	The default root location.
	Windows: "C:"
	Linux/Unix: An empty string
OSDir	**Windows**: Windows' installation directory, e.g. "C:\Windows"
	Linux: An empty string
OSDrive	**Windows**: Windows' installation drive, e.g. "C"
	Linux: An empty string
HomePath	**Windows**: The **HOMEPATH** environment variable.
	Linux: The **HOME** environment variable.
Home	The Ericom folder in the user's home
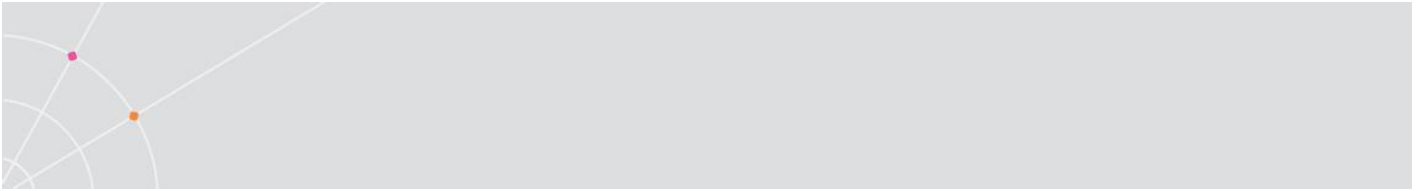
	directory:
	Windows: C:\Documents and Settings\<user>\Application Data\Ericom
	Linux: /<user>/Ericom

In addition to the predefined macros listed above, the PowerTerm WebConnect client supports the usage of Java System Properties, see Appendix B.

To Configure the PowerTerm WebConnect Client:

1. Open the **Config** folder and edit the **webconnect.xml** file. Example:
```
<?xml version ="1.0" encoding="UF-8"?>
<section name="parameters">
      <item key="url" value=http://adminserver/WebConnect5.6/>
      <item key="server" value="admin2:4000"/>
      <item key="sso" value="true"/>
      <item key="dst" value="C:/Program Files/Ericom"/>
</section>
```

2. Save the customized webconnect.xml to a Web server folder available to all users. It is recommended to use the same Web server as the PowerTerm WebConnect Agent. Example:
```
<WebConnect installation folder>\web\webconnect.xml
```

3. Test the accessibility to this file – Type the URL of webconnect.xml in the browser. Example:
```
http://<WebServer IP>/WebConnect/webconnect.xml
```
The contents of the file are displayed.

To configure the Preference file:

1. Open the **Plugins** folder, and open the **PowerTermWebConnectClient_5.6.0.365.jar** file.
You can use Winzip version 7.0 and up, or in Windows XP – Create a new file type for the jar extension, click **Advanced** and select **Compressed (zipped) folder** in the drop down list. Now you can open the JAR files in the Windows Explorer.
The default contents of the file:
configURL=http://le.ericom.com/WebConnect/webconnect.xml

2. Specify the accurate URL of the webconnect.xml file. Example:
http://<WebServer IP>/WebConnect/webconnect.xml
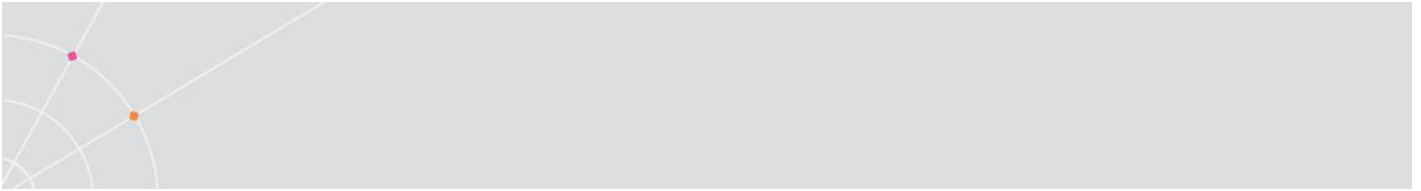
3. Save the file and close it. The WinZip will display the following dialog:

   `"File preferenes.ini has been changed since it was extracted. Update archive with this file?"`

4. Click **Yes**, and close the archive.

If you are editing the file from within the explorer, you will have to save the file elsewhere, and drag it to the explorer windows, where the JAR file is open.

22. Upgrade Instructions

You can upgrade a PowerTerm WebConnect installation to the current version, and modify your license (if necessary), without losing existing settings and configuration.

NOTE In order to follow the instructions provided in this chapter, you must have administrative privileges for the computer on which you are installing PowerTerm WebConnect, as well as being an administrator of the existing PowerTerm WebConnect installation.

NOTE If PowerTerm WebConnect Server and the Web server components are installed on separate machines, you will also need to install a new version of the Web server on the Web server machine.

22.1. Backup the Previous Installation

It is highly recommended that you backup the existing PowerTerm WebConnect installation before proceeding to install the new version. Before performing a backup of PowerTerm WebConnect files, it is recommended that the PowerTerm WebConnect server be stopped. This is in order to prevent making modifications to the database while the backup is in process. Also, some backup software requires exclusive access to the data being backed up. For instructions on stopping the PowerTerm WebConnect server see chapters 2.3 and 2.4.

The PowerTerm WebConnect **Windows** edition default installation file locations are:

- WebConnect 5.1 and higher
  All the files are located under C:\Program Files\Ericom Software\WebConnect 5.x

- WebConnect before 5.1
  Server side: C:\Program Files\Ericom Software\WebConnect 4.x
  Client side: C:\InetPub\wwwroot\Ericom\WebConnect4.x

PowerTerm WebConnect **Linux** edition Database can be backed up either manually or automatically. (For Ubuntu only manually.)

- For manual backup:
  Backup folder /opt/WebConnect5.x/DataBase/

- For automatic backup:
  The backup is done during uninstall. The Database will automatically be transferred to the folder /opt/WebConnect5.x/OldDataBase/OLD1

22.2. Upgrade PowerTerm WebConnect Windows

To install a new version without losing previous settings:
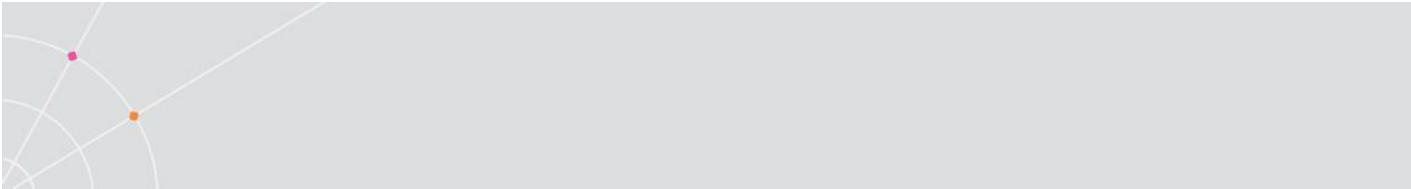
1. Follow the instructions of the installation program. You will be asked to confirm the configuration file:
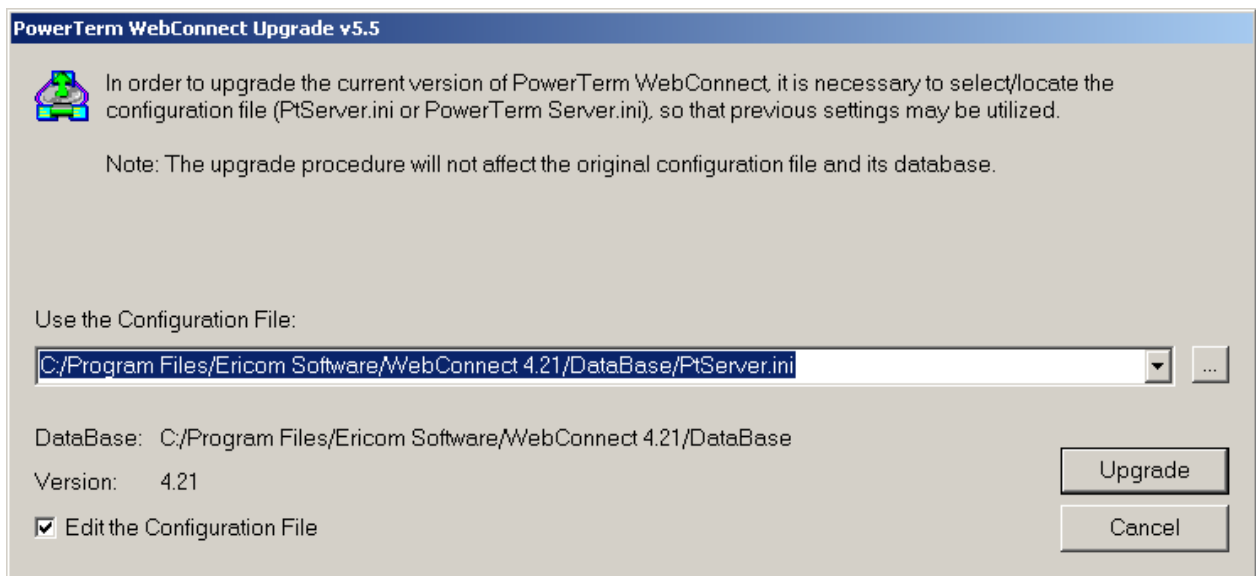
2. Verify the PtServer.ini file location.
3. Select the Edit option if you wish to edit the Configuration file.
4. Click Upgrade. The installation continues and the PowerTerm WebConnect Server icon will appear in the system tray (not available in Windows Vista).

To install from an earlier version than WebConnect 4.22:

1. Follow step 1 through 4 in the previous section.
2. Click Yes to link existing PowerTerm WebConnect Users to User Objects on the network.
3. In the Console window that appears, press <Return> to use all available Active Directory domains, or type in the path to the Active Directory Root.
4. Click Yes to use the Network Password Authentication.
5. Select the correct path if there are more than one option:

```
C:\Program Files\Ericom Software\WebConnect 5.5\bin\PtADsUser.exe                    _|□|×|
r Dray,OU=USA,OU=Domain Users,DC=ericom,DC=local                                          ▲
5727.          CN=Tami Golan                  user            LDAP://CN=Tami
 Golan,OU=USA,OU=Domain Users,DC=ericom,DC=local
5728.          CN=Tracey Ciliberti            user            LDAP://CN=Trac
ey Ciliberti,OU=USA,OU=Domain Users,DC=ericom,DC=local
5729.       OU=External Contacts          organizationalUnit  LDAP://OU=External
 Contacts,DC=ericom,DC=local
5730.       OU=External Kerberos Users    organizationalUnit  LDAP://OU=External
 Kerberos Users,DC=ericom,DC=local
5731.       CN=400.ericom.local           user            LDAP://CN=400.er
icom.local,OU=External Kerberos Users,DC=ericom,DC=local
5732.       CN=root                       user            LDAP://CN=root,O
U=External Kerberos Users,DC=ericom,DC=local
5733.   IIS:                          Namespace         IIS:

Writing to file 'ADsUser - ADs=.txt'...
5418 users found in 'ADs:'.
1. User 'Administrator' not found in AD
2. User 'Example' linked AUTOMATICALY to 'WinNT://ERICOM2K3/example'
2 users named 'Guest' were found in AD:

        1. WinNT://ERICOM2K3/Guest
        2. WinNT://TEST/Guest

Please choose the right path (0 .. 2):                                                    ▼
```

6. Click Yes when prompted to upgrade the configuration file.

7. Type Exit to proceed with the PowerTerm WebConnect Upgrade Installation, or enter an additional Activate Directory domain to be defined:

```
C:\Program Files\Ericom Software\WebConnect 5.5\bin\PtADsUser.exe                    _|□|×|
5731.       CN=400.ericom.local           user            LDAP://CN=400.er ▲
icom.local,OU=External Kerberos Users,DC=ericom,DC=local
5732.       CN=root                       user            LDAP://CN=root,O
U=External Kerberos Users,DC=ericom,DC=local
5733.   IIS:                          Namespace         IIS:

Writing to file 'ADsUser - ADs=.txt'...
5418 users found in 'ADs:'.
1. User 'Administrator' not found in AD
2. User 'Example' linked AUTOMATICALY to 'WinNT://ERICOM2K3/example'
2 users named 'Guest' were found in AD:

        1. WinNT://ERICOM2K3/Guest
        2. WinNT://TEST/Guest

Please choose the right path (0 .. 2): 1
3. User 'Guest' linked MANUALLY to 'WinNT://ERICOM2K3/Guest'

Done!

Enter another AD root
        Press <RETURN> for default,
        type FILE to use the values specified in the PtServer.ini
        type EXIT to terminate
===>                                                                                      ▼
```

The installation continues and the PowerTerm WebConnect Server icon will appear in the system tray (not available in Windows Vista).

22.3. Upgrade PowerTerm WebConnect Linux

1. Install the new PowerTerm WebConnect version (see above).

2. Run the command /opt/WebConnect5.6/bin/wcctl –upgrade

3. Press 'Y' when prompted "Do you want to upgrade from older versions?"

4. Input the path to PtServer.ini from the older version (/opt/WebConnect5.x/OldDataBase/OLD1/PtServer.ini). At the end of the process the message "Upgrade was finished successfully" is displayed.

22.4. Update Product License

License modification is typically applicable when:

- Extending demo version.

- Converting demo version to real version.

- Modifying the number of license seats.
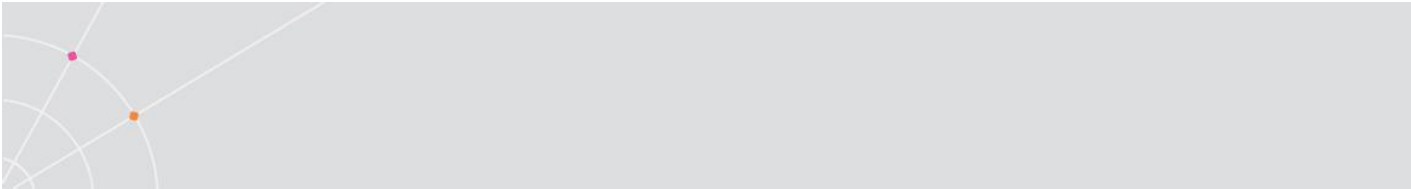
To modify the product license:

1. Browse to the PowerTerm WebConnect installation folder, select the bin folder and run PowerTerm WebConnect Server License Update.exe. Alternatively go to Start menu | Programs | Ericom Software | PowerTerm WebConnect X.xx and click PowerTerm Server License Update. The PowerTerm Server License Update dialog appears.

2. Send the contents of the Key to send to Ericom field to Ericom, specifying your request.

3. Upon receipt of the new key from Ericom, type it into the Key received from Ericom field.

4. Click Activate Key. The product license is updated.

5. Restart the PowerTerm WebConnect Server service.

22.5. HTML Files and PowerTerm WebConnect Client CAB File Locations

The new PowerTerm WebConnect 5.x HTML files are now located in the web subdirectory under the installation directory, as follows:

C:\Program Files\Ericom Software\WebConnect 5.x\web\

This directory is automatically mapped to a virtual directory on the local Web server. Files in this directory can be accessed from the browser by typing the following URL:

http://<server_name>/WebConnect5.x/ClientURLs.html

ClientURLs.html is a central location for launching the various PowerTerm WebConnect clients, and also serves as a base from which you can create your own customized HTML pages. A link to ClientsURLs.html is also created in the Start menu.

Before reviewing this example, it is important to understand that PowerTerm WebConnect's browser-based client activation mechanism has been changed significantly in version 5.1. For backward compatibility, the old client activation mechanism is still supported in version 5.1. For more details on activating clients from the browser, see chapters 8 and 11.

If you decide to continue using the old client activation method, you will still need to update your HTML files because the GUIDs (Global Unique Identifier) of the Windows clients, such as PowerTerm WebConnect HostView (formally ActiveX) have changed. The new GUIDs are listed in section 11.4.
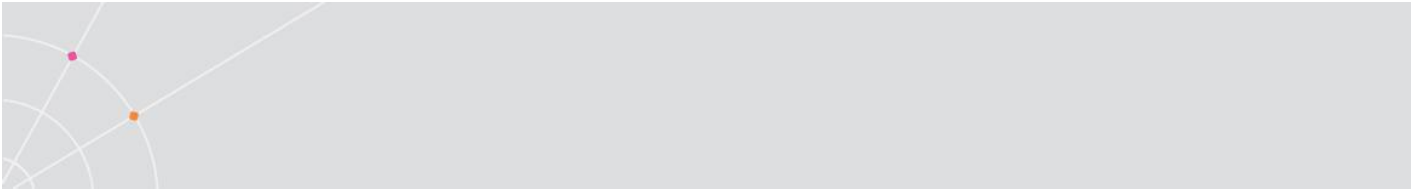
In addition, you will need to manually copy the CAB files containing the clients from the Downloads subdirectory under the WebConnect server installation directory to the web/windows directory. The installer does not place these files in the Web server's directory because the new download mechanism retrieves these files directly from the PowerTerm WebConnect server.

22.5.1. Translating Existing HTML Files to the New Format

The new client activation mechanism, as described in chapters 8 and 11, uses the Windows Downloader or Java Downloader to start the activation processes. Both of these downloaders proceed to download and launch the PowerTerm WebConnect Agent. The Agent in turn downloads and launches the desired client. This is in contrast to the previous mechanism, which used the browser's built-in support for ActiveX controls to download and launch the clients directly. See chapter 11 for the advantages of the new activation method.

The result of this change means that the HTML contains an <OBJECT> tag (or <APPLET> tag) referencing the Downloader rather than the actual client. The GUID of the Downloader is guaranteed to remain fixed in all future versions of PowerTerm WebConnect, so the HTML need not be changed in future upgrades.

Another change is that the arguments controlling the behavior of the clients are passed as command-line arguments using the Downloader's Parameter property, rather than using client methods activated by JavaScript. For the complete list of command-line arguments supported by the WebConnect clients, see chapter 8.

The following code snippet demonstrates the old method of activating clients applied to the new HostView:

```
<OBJECT ID=HostView

CLASSID="CLSID:BBC72F64-2AC3-4942-A8CD-B88857BB21C3"
CODEBASE="ptermX.CAB#Version=5,1,3,1000"

width="0" height="0" >

</OBJECT>
```

To connect this client, a method is invoked from the browser's on-load event handler:

```
function window.onload() {

    HostView.LoginDialog(location.href,

    4000,

    1,

    "username",

    "password",

    "?",

 location.href);

}
```

The new method of performing the same operation:

```
<OBJECT ID=Downloader WIDTH=0 HEIGHT=0

    CODEBASE="ptdownloader.cab#Version=5,1,3,100"

    CLASSID="CLSID:7EC816D4-6FC3-4C58-A7DA-A770EE461602">

    <PARAM NAME="Src" VALUE="ptagent.cab">

    <PARAM NAME="Parameters"

VALUE="<WebServer> /RUN=HostView /USER=username /PASS=password">

</OBJECT>
```

> NOTE Its is highly recommended that you review and become familiar with all the sample HTML files provided in the installation before attempting to convert existing HTML files to the new format.

22.5.2. Examples of some Scripts in the New Format

Old (JavaScript) Method for OsLogin:

```
<!-- CUT -->

Connector.OsLogin( window.location.href,     // server_location

                        4000,     // server_port

                           1,     // use_ssl

                         "?",     // session_id

        window.location.href );     // WEB_server_location

<!-- CON'T -->
```

New (HTML) Method for OsLogin:

```
<!-- CUT -->

<OBJECT ID=Downloader WIDTH=0 HEIGHT=0 STYLE="DISPLAY:none"

CODEBASE="ptdownloader.cab#Version=5,1,3,1000"

CLASSID="CLSID:7EC816D4-6FC3-4C58-A7DA-A770EE461602">

<PARAM NAME="Src" VALUE="ptagent.cab">

<!-- This is a modified HTML PARAM line to perform the same function of
"Connector.OsLogin" -->

<PARAM NAME="Parameters" VALUE="<WebServer>:4000 /NOSELFUPDATE
/RUN=HostView /EXTRA_PARAMS=&quot;/SSL /SID=? /USER=*?&quot;">

</OBJECT>

<!-- CON'T -->
```

NOTE In the current HTML version (5.x) there is no reference to a Web server. In
       version 4.22 and earlier all files were downloaded from the Web server, while in
       version 5.1 and later all client files (except the ptagent.cab) are located in
       <webconnect_server>/downloads. Therefore there is no need for the Web server
       address in the HTML.

---

23. Optimizing Performance

This chapter provides rules and suggestions for optimizing PowerTerm WebConnect performance. You can customize your PowerTerm WebConnect Server configuration in different ways to improve performance:

- Host PowerTerm WebConnect Server on a dedicated server.
- Ensure that PowerTerm WebConnect has sufficient resources.
- Alternate Connection Points.
- Set PowerTerm Server's Process Priority, schedule PowerTerm Server executions.
- Administration Tool Parameters: configure administrator shortcuts.
- Integration with different RTO components.

23.1. Use a Dedicated Server

For optimal performance, it is recommended to install the PowerTerm WebConnect server on a dedicated computer. It is specifically recommended not to install PowerTerm WebConnect on a computer that is already under heavy load, such as a computer that hosting the corporate Web server. Following is a list of applications that should not be installed on the same computer as the PowerTerm WebConnect server:

- Microsoft Terminal Server or Citrix Presentation Server
- Microsoft Active Directory or any other directory service
- Microsoft Exchange or any other mail server
- Corporate Web server

To host the server on a non-Web server:

1. Copy the relevant Internet folders:
If the Web server is an NT machine: Install on it the client side.
If the Web server is a non-NT machine: Copy the folder Ericom\PowerTerm WebConnectversion x.xx (installed by default under \InetPub\wwwroot) to the desired Web server.
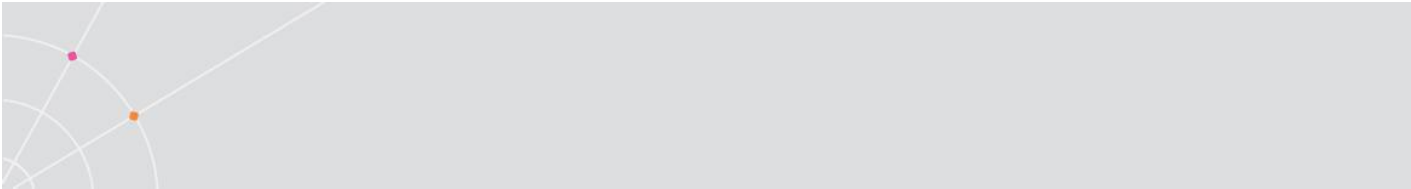
2. Set the desired value of the applet parameter server in each of its multiple occurrences in all of the relevant HTML files.
For Java Client use the following syntax:
<param name="server" value="powerterm-java-server-host-name">
For HostView, WebView, PrintView, and Agent clients, change the corresponding parameter in their respective HTML file.

3. Set the entry [Server]AttachURL to match the http address where the applet is located. This entry is found in the configuration file used by the server and is used for starting attached clients.
Example: AttachURL=http://MyWebServer/Ericom/Client/AttachClient.html

4. Set the entry [Server]WebDir to point to the client side's root folder. Default path for IIS: \Inetpub\wwwroot\Ericom\PowerTerm WebConnect <version>.

23.2. Allocate Sufficient Resources

For optimal performance it is important to ensure that the PowerTerm WebConnect components have sufficient resources. Specifically, 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. For details of the memory requirements of the PowerTerm WebConnect server see chapter 2.1.1.

You can use the Performance Monitor, part of the Microsoft Management Console, to monitor the system's performance and resource usage over time. It is particularly useful to inspect memory related statistics such as Memory\Pages/sec and Memory\Page Faults/sec. High values indicate that available RAM is insufficient, and memory is being constantly swapped to and from the disk.

You can also use the Performance Monitor to monitor network traffic. This will enable you to identify communication bottlenecks. You can use the Administration Tool to analyze network traffic at the user and group levels.

NOTE These monitors provide information about the amount of communication between the PowerTerm WebConnect server and clients. However, if the clients are connecting directly to the host then communication is not observed by these monitors.

23.3. Alternate Connection Points

The default installation defines the main connection point as 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 configuration file (default: PtServer.ini).

If necessary, you can define alternate connection points by copying an existing connection point and changing the name and other pertinent information in Server ConnectionPoints Table.

Example

*   [ConnectionPoint=LAN]

*   Address=126.1.1.177

- PortNo=7777

- SSL-Required=False

- LoginRequestTimeoutSeconds=10

- EchoTestFrequencySeconds=60

- EchoTestTimeoutSeconds=30

- KeepAlive=False

- UseConnectingMachineName=True

23.4. Set PowerTerm WebConnect Server's Process Priority

As described in chapter 2.6.5, you can control the PowerTerm WebConnect server's process priority. A process' priority determines how much CPU resources the operating system allocates to the process, relative to other processes running on the computer. Processes with a higher priority are allocated more CPU time and therefore often execute more quickly than processes with a lower priority.

To set the server's process priority:

Set the entry [Server]ProcessPriority=priority-name in the server's configuration file (default: PtServer.ini).

The supported priority-name values:

- Normal/High/Realtime are identical to those of Windows NT process priorities.

- <Default> is dependent on whether the PowerTerm WebConnect Server is running as an NT Service, in which case the process priority will be set to High, or as a regular program, in which case the process priority will remain Normal.

Under normal conditions, you should not change the server's process priority.

23.5. Administration Tool Parameters

The administrator can configure personal shortcuts to the Administration Tool adding command line parameters. The parameters are optional and their order is not of any consequence.

-user=user-name	User's account name on the PowerTerm WebConnect Server.
	If the account name is equal to a question mark (?), then the user name used to login to the operating
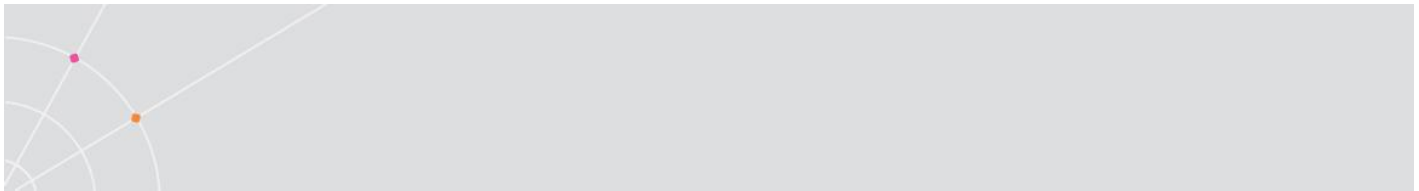
	system will be used.
	If the first character is an asterisk (*), then no login dialog box will appear.
-pass=password	User's password on the PowerTerm WebConnect Server.
-host=hostname	PowerTerm WebConnect Server's host name.
-port=port=number	PowerTerm WebConnect Server's port number.

Example: "D:\Ericom\PtAdmin.exe" –host=117.18.75.89 –port=778 –user="Lee Marshal"

23.6. Integration with RTO

PowerTerm WebConnect installation comes with the option to install different RTO components to optimize the work with PowerTerm WebConnect. The installations are bundled inside the PowerTerm WebConnect installation, in the **AddOns|RTO** folder.

The PowerTerm WebConnect licensing includes RTO licensing.

Available RTO components in different PowerTerm WebConnect editions:

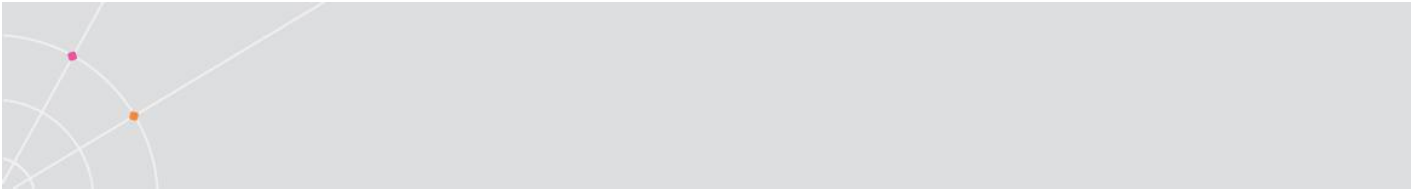|	PowerTerm WebConnect RemoteView	PowerTerm WebConnect Enterprise
RTO Discover	-	√
RTO PinPoint	-	√
RTO TScale Advanced	√	√

For more information about RTO see www.rtosoft.com.

23.6.1. RTO TScale Advanced

This feature optimizes virtual memory usage on the Terminal Server thus potentially allowing more sessions to run at the same time. It also prevents applications from making excessive use of the CPU.

The RTO TScale Advanced installation consists of two MSI files:

- **TScaleConsole_v4.0.4.msi**, the Console MSI that can be installed on any machine.

- **TScaleAgent_v4.0.4.Ericom.msi**, the RTO TScale agent MSI that needs to be installed on each Terminal Server machine.

23.6.2. RTO Discover

This tool maps the entire network with all its hard- and software, including application versions, and presents it in a graph. This real-time view makes it easy for administrators and other IT staff to find configuration discrepancies, decide about license renewals, etc.

The RTO Discover installation consists of one MSI file:

- **Discover_v1.1.1.x86.msi**, that needs to be installed on each machine that you want to collect information from.

To run RTO Discover through the Ericom license, you need to:

- Add the command prompt
  ```
  Discover_v1.1.1.x86.msi ERICOM="yes"
  ```
  to automatically install the **Ericom_lic.dll**.

- Configure **PtServer.ini** with
  ```
  RTOListenPort=<your choice of port>
  ```

NOTE You need to restart the server to initiate the port.

To launch RTO Discover:

1. Select, from the Start menu, the RTO Discover application. The Ericom WebConnect Server dialog opens.

2. Enter <server IP>:< defined port> and click OK.

23.6.3. RTO PinPoint

This tool monitors network and application performances in real time, thus allowing alerts and early discovery of system failures. It also tracks user experience, from the client to the server.

The RTO PinPoint installation consists of three MSI files:

- **Agent_v3.1.12.msi**, theTSagent MSI that needs to be installed on each machine that you want to track.

- **Console_v3.1.12.msi**, the Console MSI that can be installed on any machine.

- **ClientMonitor_v3.1.12.msi**, the client MSI that needs to be installed on each client machine.

To run RTO PinPoint through the Ericom license, you need to:

- Add the command prompt
  `Console_v3.1.12.msi ERICOM="yes"`
  to automatically install the **Ericom_lic.dll**.

- Configure **PtServer.ini** with
  `RTOListenPort=<your choice of port>`

NOTE   You need to restart the server to initiate the port.

To launch RTO PinPoint:

1. Select, from the Start menu, the RTO PinPoint application. The **Ericom WebConnect Server** dialog opens.

2. Enter `<server IP>:< defined port>` and click **OK**.

24. Useful scripts

This chapter provides a collection of useful PowerTerm Scripting Language scripts for use with the emulation clients – HostView (for Windows and Linux) and WebView.

24.1. Limiting Number of Emulation Sessions per User

In order to limit your users by to only one (1) session of PowerTerm WebConnect HostView at a time, copy and paste the script below at the beginning of the connection's login script (in the Administration Tool).
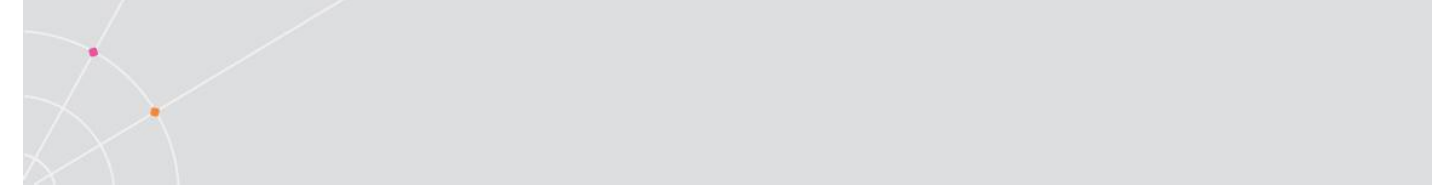
```
max_sessions = 1

if { [get session-count] > $max_sessions } {

message "There are too many sessions open.\n Please close all open emulation
windows."

session close

activate-menu-item Exit

return }

remove-menu-item NewTerminalWindow
```

This script verifies the number of currently open HostView sessions. If the current number exceeds the maximum number of allowed sessions, this session is terminated. Otherwise, the session is allowed to continue, but the option to open a new Terminal Window is removed from the menu and toolbar. It then proceeds with the session.

24.2. Distributing Users between Hosts

In some cases it may be useful to distribute users between two or more hosts. This can be accomplished by defining two connections - one for each host. One of these connections will be defined as the primary - and will be the first one the user activates. The login script of the primary connection will transfer half of the user (chosen at random) to the secondary connection.

```
if {[expr [time] % 2] == 1} {

    w2h-select-connection "alternate"

}
```

In this example, the secondary connection is named "alternate".

NOTE   Do not place this script in the secondary connection, otherwise the connections will "ping-pong" between each other.
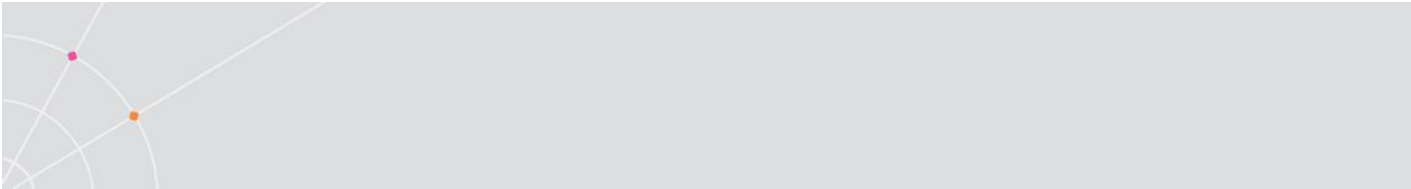
24.3. Using Microsoft COM from PSL

PSL provides direct access to COM components. The following script demonstrates how to send an email from script using Microsoft Outlook COM Automation interfaces:

```
to = [input-line Name Mail]
if {[string length $to] == 0} {
    return
}
outlook = [com create Outlook.Application]
com with [com call $outlook CreateItem 0] {
    recipients = [com get Recipients]
    com with [com call $recipients Add $to] {
            com put Type 1
    }

    com foreach recip $recipients {
            com call $recip Resolve
    }

    com put Subject "Sample email"
    com put Body "This is an example of PSL COM using Outlook"

    com call Send
}
```

NOTE   PSL COM support is available only on the Windows platform. The PSL "com"
command is not supported by PowerTerm HostView for Linux.
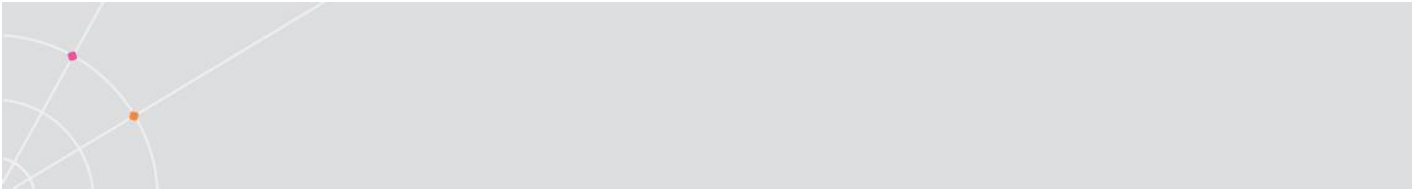
Appendix A – PowerTerm WebConnect Ports

Most PowerTerm WebConnect components (server, starter, Administration Tool, and some clients such as the JAVA and HostView clients) use port 4000 as default. This port can be modified to avoid conflicts with other applications, as well as with firewalls or proxies (see also chapter 23.3).

To modify the server's TCP/IP port:

1. Open the configuration file used by the server and starter. The default configuration file name is PtServer.ini.

2. Set the entry [ConnectionPoint=<name>]PortNo=new-port-number

3. Set the desired value of the applet parameter port in all of the relevant HTML files.

4. For Java Clients use the following syntax:

5. var sParamPort = '<param name="port" value="port-number "> ';

6. For HostView, WebView, PrintView, and Agent Clients, change the corresponding parameter in their respective HTML file.

7. Perform the necessary modification in the HTML that uses the HostView component.

8. You can pass the port number to the Administration Tool as a command line parameter, using the following syntax:

9. -port=port-number

10. This allows you to create a shortcut to the Administration Tool, or modify an existing one, adding your specific port number as a parameter in the Target field of the Shortcut property page.

11. Example: "C:\Program Files\Ericom Software\PowerTerm WebConnect\bin\PtAdmin.exe" –port=778

PowerTerm WebConnect ports

Port #	Listening to
389	LDAP
636	SSL LDAP

515	LPD/LPR
1812	RSA SecureID or Radius two-factor-authentication protocol
4000	Default PowerTerm WebConnect components
4001	PowerTerm WebConnect Administration Tool
4080	Broadcast port for Automatic Server Discovery

About Ericom

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

For more information on our products and services, contact us at the location nearest to you. And visit our web site: http://www.ericom.com

North America
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