Atrust

Topics Covered:

Setup and Maintenance
Basics as an Endpoint Device in VDI
Atrust Client Setup Console

Mobile Thin Client Solution
Atrust mt182L

User's manual

Version 0.01
Copyright © 2019-20 Atrust Computer Corp.

Copyright and Trademark Statements

Copyright © 2019-20 Atrust Computer Corp. All rights reserved.

This document contains proprietary information that is protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of Atrust Computer Corp.

Disclaimer

Atrust Computer Corp. (“Atrust”) makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Atrust is not liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

Trademark Statements

Atrust is a trademark of Atrust Computer Corp.

Intel is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Windows, Windows Server, RemoteFX, and MultiPoint are trademarks or registered trademarks of the Microsoft group of companies.

Citrix, ICA, XenApp, XenDesktop, VDI-in-a-Box, Virtual Apps and Desktops, are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware, VMware View, and VMware Horizon View are trademarks or registered trademarks of the VMware, Inc.

PCoIP is a registered trademark of Teradici Corporation in the United States and/or other countries.

Other product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

About This User's Manual

This manual provides detailed instructions on how to set up, use, and maintain Atrust mt182L mobile thin clients.

Manual Structure and Subjects

Chapter	Subject
1	Provides an overview of Atrust mt182L mobile thin clients.
2	Provides detailed instructions on how to set up Atrust mt182L mobile thin clients.
3	Provides the basics of how to use Atrust mt182L mobile thin clients.
4	Provides instructions on how to configure client settings and customize Atrust mt182L mobile thin clients with the Atrust Client Setup console.
Appendices	Provides supplementary instructions on advanced settings, maintenance, and upgrade for Atrust mt182L mobile thin clients.
Specifications	Provides detailed information on key components of Atrust mt182L mobile thin clients.

Notes, Tips, and Warnings

Throughout this manual, the notes, tips, and warnings in the following formats are used to provide important information, useful advice, and prevent injuries to you, damage to your devices, or loss of data on your system.

NOTE

- A note provides important information for a specific situation.

TIP

- A tip gives a piece of useful advice to perform a task more efficiently.

WARNING

- A warning provides crucial information that must be followed to prevent injuries to you, damage to your devices, or loss of data on your system.

Style Conventions

The following styles are used throughout this manual while referring to operational items on input devices, hardware panels, or application interfaces.

Item	Style	Example
Keys on the keyboard	bold	**Ctrl + F2**, **Alt + F9**, **Alt + Tab**
Application windows or entry lists	first letter capitalized	Confirm Dialog window, RDP Connection list, ICA Connection list, View Connection list
Buttons or tabs on a window, toolbars, taskbar, or menu	bold	**OK**, **Next**, **Save**, **Applications** tab
Options on a window, screen, list, or menu	bold	**Add**, **Domain**, **Connection Type**, **High Quality**
Selecting a series of options	bold	**Applications** > **Citrix ICA**, **Applications** > **Remote Desktop**, **Applications** > **VMware View**, **Network** > **Wireless**, **Devices** > **Printer**, **System** > **Time Zone**

Safety and Regulatory Information

Regulatory Statement

Federal Communications Commission Interference Statement
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Regulatory Information

WEEE (Waste Electrical and Electronic Equipment) Directive

In the European Union, this symbol indicates that this product should not be disposed of with household waste. It should be deposited at an appropriate facility to enable recovery and recycling. For proper disposal, please contact your local recycling or hazardous waste center.

Safety Information

WARNING

- Use only power supplies listed in the user instructions.

WARNING

- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.

WARNING

- For safety, do not make mechanical or electrical modifications to the equipment.
- Do not remove equipment covers and access any of the components inside the equipment. Any access inside the equipment without an authorized or certified technician may cause serious injuries and damage. For any problem, contact your dealer for assistance.
- You should only make repairs as authorized by the product documentation. Repairs, replacement, expansion, and upgrades not performed by a certified service technician may cause injuries to you, damage your system, and void your warranty.

Table of Contents

Copyright and Trademark Statements i

Disclaimer i
Trademark Statements i

About This User's Manual ii

Manual Structure and Subjects ii
Notes, Tips, and Warnings ii
Style Conventions iii

Safety and Regulatory Information iv

Regulatory Statement iv
Regulatory Information v
Safety Information v

1 Overview 1

1.1 Introduction 3

1.2 Features 3

1.3 Package Contents 4

1.4 Exterior Components 5

1.5 Before Getting Started 9

2 Getting Started 11

2.1 Learning the Basics 13

3 Configuring Client Settings 41

3.1 Atrust Client Setup 43

3.1.1 Interface Overview 43
3.1.2 Client Settings at a Glance 44

3.2 Configuring System Settings 45

3.2.1 System Tab Overview 45
3.2.2 Available Settings at a Glance 46
3.2.3 Configuring Time Zone and Time Server 47
3.2.4 Configuring the Access Privileges and Passwords of Atrust Client Setup 48
3.2.5 Configuring the Login Password for the Local Desktop 52
3.2.6 Configuring Shadow Settings for Remote Assistance 54
3.2.7 Updating Firmware from the Management Computer 56
3.2.8 Enabling or Disabling the Appliance Mode 58
3.2.9 Enabling or Disabling Auto Setup 62
3.2.10 Configuring the Quick Connection Mode 62
3.2.11 Configuring Advanced Quick Connection Settings 64
3.2.12 Managing the Use of Power 68
3.2.13 Enabling or Disabling the Command-line Functions 69
3.2.14 Collecting Event Logs and Capturing Related Screens 70
3.2.15 Uploading Files for Error Reporting 72
3.2.16 Importing Certificates for Remote Computers 73
3.2.17 Enabling or Disabling Auto Registration 77
3.2.18 Viewing System and Network Information 78

3.3 Configuring User Interface Settings 79

3.3.1 User Interface Tab Overview 79
3.3.2 Available Settings at a Glance 80

3.3.3 Configuring Display Settings 80
3.3.4 Customizing Desktop and System Language Settings 83
3.3.5 Hiding or Showing Quick Access Shortcuts 86
3.3.6 Using a Custom Wallpaper 87
3.3.7 Adjusting Keyboard Settings 88
3.3.8 Adjusting Mouse Settings 90
3.3.9 Configuring Screensaver Settings 91

3.4 Configuring External Device Settings 93

3.4.1 Devices Tab Overview 93
3.4.2 Available Settings at a Glance 94
3.4.3 Configuring Settings for USB Storage Devices 94
3.4.4 Manually Mount and Eject Attached USB Storage Devices 95
3.4.5 Disabling or Enabling Attached Audio Devices 96
3.4.6 Using Audio Devices 97
3.4.7 Muting or Unmuting the Sound 98
3.4.8 Adding a Local Printer 99
3.4.9 Adding a Network Printer 102

3.5 Configuring Network Settings 103

3.5.1 Network Tab Overview 103
3.5.2 Available Settings at a Glance 104
3.5.3 Configuring Wired Network Settings 105
3.5.4 Configuring IEEE 802.1X Authentication 108
3.5.5 Establishing and Stopping a VPN connection 109
3.5.6 Configuring Virtual Private Network Settings 113
3.5.7 Creating the Mapping of IP Addresses to Names of Hosts 114
3.5.8 Configuring the Failover Cluster List 116
3.5.9 Changing the Host Name of Your Thin Client 118
3.5.10 Enabling or Disabling the Wireless Interface 119
3.5.11 Configuring the Trigger Threshold for Roaming 120
3.5.12 Establishing and Stopping a Wireless Connection 121
3.5.13 Configuring Wireless Connection Settings 124
3.5.14 Configuring Proxy Settings for Web-based Access to Services 125

3.6 Configuring Service Access Settings 127

3.6.1 Applications Tab Overview 127
3.6.2 Available Settings at a Glance 128
3.6.3 Configuring Basic RDP Connection Settings 129
3.6.4 Accessing Remote Desktop Services 138
3.6.5 Configuring Advanced RDP Connection Settings 144
3.6.6 Configuring Basic ICA Connection Settings 159
3.6.7 Switching the Citrix Receiver Version 172
3.6.8 Enabling or Disabling Esc to Quit on the Web Logon Screen 173
3.6.9 Configuring Keyboard Layout and Type for Citrix ICA Sessions 174
3.6.10 Accessing Citrix Services 175
3.6.11 Configuring Advanced ICA Connection Settings 182
3.6.12 Configuring Basic VMware View Connection Settings 212
3.6.13 Accessing VMware View or Horizon View Services 214
3.6.14 Configuring Advanced View Connection Settings 216
3.6.15 Configuring SSH Connection Settings 221
3.6.16 Launching SSH and Telnet Sessions 223
3.6.17 Configuring Basic Settings for Browser Sessions 224
3.6.18 Launching Browser Sessions 226
3.6.19 Configuring Advanced Settings for Browser Sessions 227
3.6.20 Configuring Basic RAS / RDP Connection Settings 228
3.6.21 Accessing Remote Desktops or Applications 233
3.6.22 Configuring Advanced RAS / RDP Connection Settings 235

Appendices 247

A.1 Resetting Your mt182L to the Factory Default 249

A.2 Updating Firmware for Your mt182L 250

A.3 Using SECUREMATRIX Authentication for VMware Connections 252

A.4 Auto Setup Flowchart 259

Specifications 261

1

Overview

This chapter provides an overview of Atrust mt182L.

1.1 Introduction
Desktop virtualization and simple endpoint devices 3

1.2 Features
Key features of Atrust mt182L 3

1.3 Package Contents
Check your package contents 4

1.4 Exterior Components
Exterior components of Atrust mt182L 5

1.5 Before Getting Started
About the Battery Sleep Mode 9

1.1 Introduction

Desktop virtualization provides a new perspective to reconsider the design and implementation of an IT infrastructure. In a desktop virtualization infrastructure, a station is no longer a cumbersome desktop, but simply an endpoint device for users to access delivery services from the server(s).

With the introduction of the desktop virtualization technologies, you can considerably benefit from:

- On-demand applications/desktops
- Centralized management of work environments
- Drastically reduced endpoint software/hardware issues
- Simplified system maintenance and improved system security
- More scalability with low-cost endpoint devices

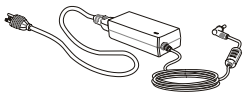
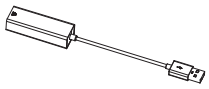
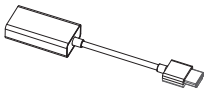
1.2 Features

The key features of Atrust mt182L mobile thin clients are:

- Built-in Wireless 802.11 ac/a/b/g/n, Bluetooth 4.2, and Ethernet network interface
- Support for a wide range of desktop virtualization solutions from industry-leading companies:
  - Microsoft® Remote Desktop
  - Citrix® XenApp™, XenDesktop®, Virtual Apps and Desktops™, VDI-in-a-Box™
  - VMware® View™ and Horizon View™
- Support for high-definition technologies
  - Microsoft® RemoteFX®
  - Citrix® HDX™
  - VMware® View™ PCoIP®
- Simple click-access to various applications/desktops
- Support for both local and remote management

1.3 Package Contents

Please check your package contents. Ensure that all of the items are present in your package. If any items are missing or damaged, please contact your dealer immediately.

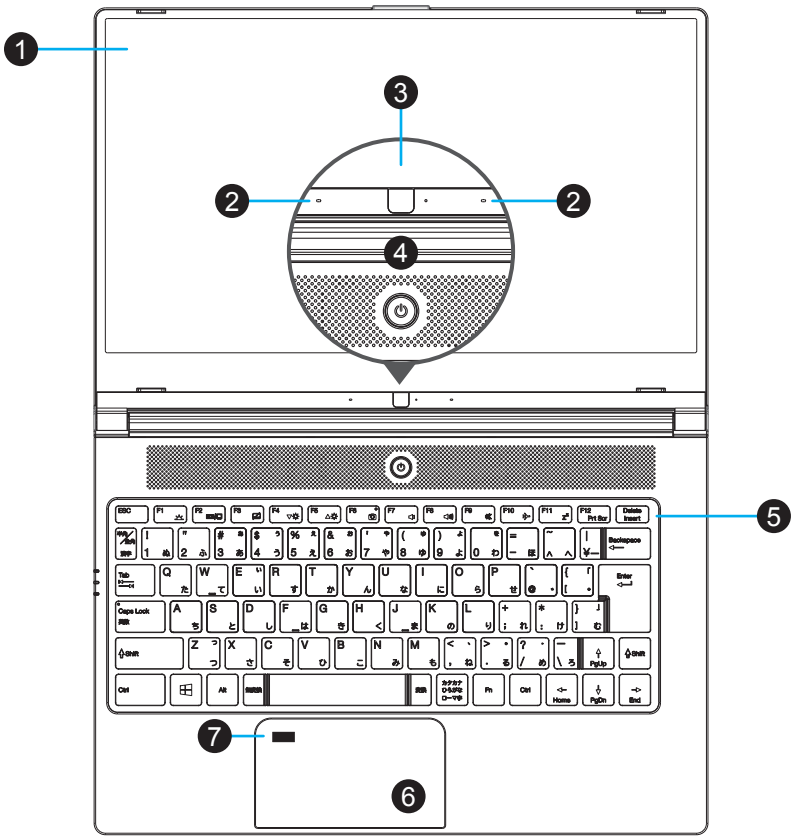
Atrust mt182L	AC adapter	Quick Start Guide
		
USB-to-RJ45 Adapter	**HDMI-to-VGA Adapter**	
	(*Optional*)	
		

NOTE

- Your package may not contain a hard copy of the Quick Start Guide. In this case, a soft copy in PDF format will be provided.

1.4 Exterior Components

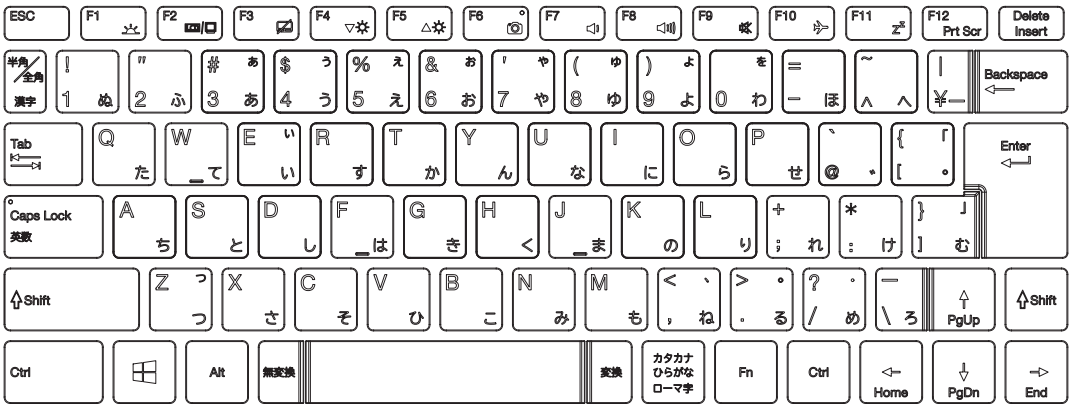
Display and Base Components



No.	Sign	Component	Description
1		LCD display	Built-in display for visual output.
2		Microphone	Built-in microphone for audio input.
3		Webcam	Built-in video camera for real-time video.
4	⏻	Power button	• Press to power on your mt182L. • Press to shut down when your mt182L is on.
5		Keyboard	Built-in keyboard for control and input.
6		Touchpad	Built-in pointing device for control and input.
7		Fingerprint Sensor	Built-in reader for fingerprint sign-in.

Fn Key Combinations

With the combination of **Fn** [Fn] plus another specific key (most with one printed symbol on it), you can quickly adjust hardware settings to suit your needs.

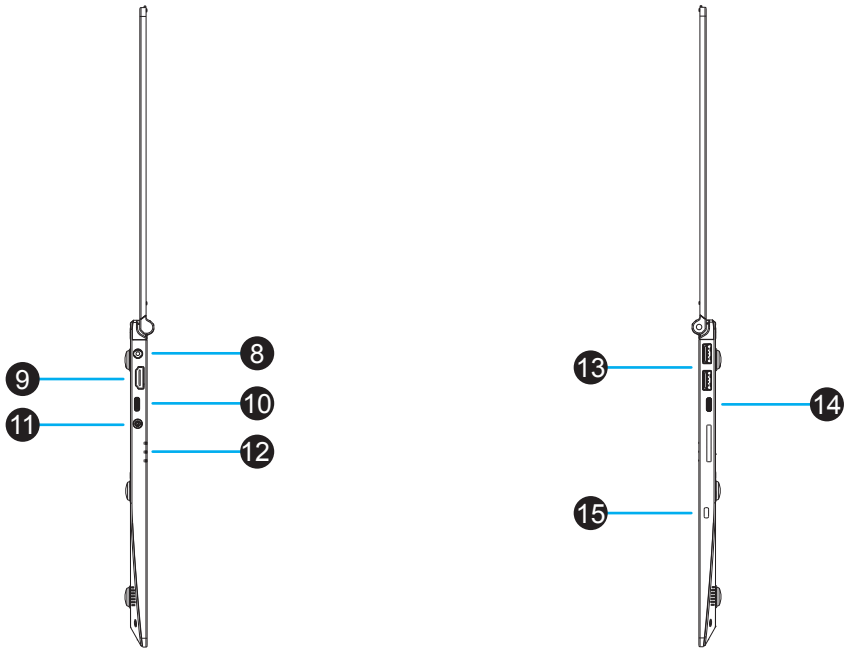


NOTE

- To use an Fn key combination, press and hold **Fn**, and then press another key.

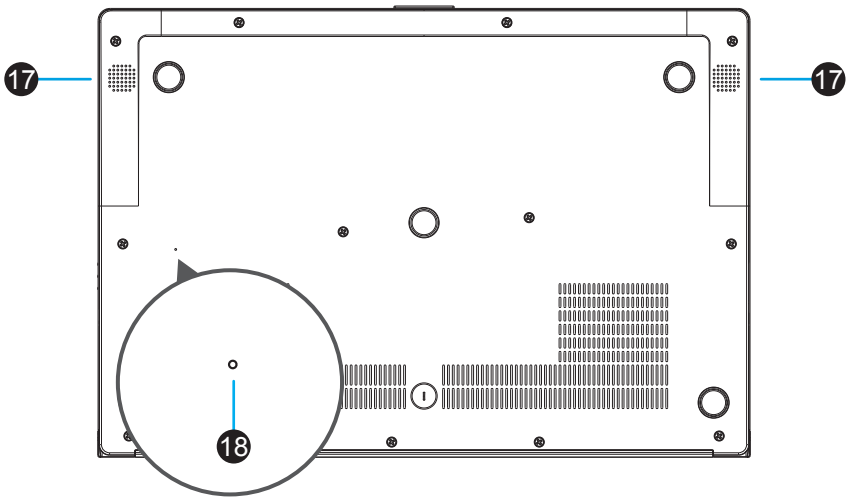
Combination	Description	Combination	Description
Fn + F1	**Fn + F1** Use to switch the brightness of the keyboard backlight.	Fn + F9	**Fn + F9** Use to mute / unmute the sound.
Fn + F2	**Fn + F2** Use to switch the use of displays.	Fn + F10	**Fn + F10** Use to enable / disable the Airplane mode.
Fn + F3	**Fn + F3** Use to enable / disable the touchpad.	Fn + F11	**Fn + F11** Use to enter the System Sleep mode. Press the Power button or any key to exit.
Fn + F4	**Fn + F4** Use to decrease the brightness of the LCD display.	Fn + F12 Prt Scr	**Fn + F12** Use to work as **Pri Scr** key.
Fn + F5	**Fn + F5** Use to increase the brightness of the LCD display.	Fn + PgUp	Use to work as **PgUp** key.
Fn + F6	**Fn + F6** Use to enable / disable the Webcam.	Fn + PgDn	Use to work as **PgDn** key.
Fn + F7	**Fn + F7** Use to decrease the volume of the built-in speakers.	Fn + Home	Use to work as **Home** key.
Fn + F8	**Fn + F8** Use to increase the volume of the built-in speakers.	Fn + End	Use to work as **End** key.

Left and Right Side Components



No.	Sign	Component	Description
8	⎓	DC IN	Connects to an AC adapter.
9	HDMI	HDMI port	Connects to a high quality digital audiovisual device.
10		USB-C port (USB 3.1 Gen 1)	Connects to a USB-C device.
11		Audio combo jack	Connects to a set of headphones.
12		Power LED	• Glows blue when the system is on. • Goes off when the system is off. • Glows orange when the system is in Sleep mode.
		Battery LED	• Glows orange when the battery is being charged. • Glows blue when the battery is fully charged.
		Wireless LED	• Glows blue when wireless network is enabled. • Goes off when Airplane mode is enabled. **Airplane mode:** disabled wireless network
13	SS	USB-A port (USB 3.1 Gen 1)	Connects to a USB-A device.
14		USB-C port (USB 3.1 Gen 1)	Connects to a USB-C device.
15		Kensington security slot	Connects a Kensington cable to secure the mobile thin client.

Bottom Components



No.	Sign	Component	Description
17		Speaker	Built-in speakers for audio output.
18		Battery Off hole	Used to press the button inside to enter the Battery Sleep mode. Please see “About the Battery Sleep Mode” on page 9 for details.

1.5 Before Getting Started

About the Battery Sleep Mode

For first time use, you must connect your mt182L to a power outlet using the supplied AC adapter for the built-in battery to exit the Sleep mode.

To enter the Battery Sleep mode when needed, please do the following:

1. Shut down and unplug your mt182L.
2. Use the tip of an unfolded paper clip (or a similar object without a sharp tip) to gently press the button inside the Battery Off hole.

NOTE

- Please note that, to exit the Battery Sleep mode and power on your mt182L, you will need to plug it in first using the supplied AC adapter.

2

Getting Started

This chapter provides the basics of how to use your mt182L.

2.1 Learning the Basics

Topic 1: Atrust Quick Connection 14
Topic 2: Setting Up a Wireless Connection 16
Topic 3: Configuring the Time Zone 18
Topic 4: Accessing Desktops or Applications 19
Topic 5: Using Built-in Applications 36
Topic 6: Viewing and Managing the Use of Power 38

2.1 Learning the Basics

The following topics will guide you through the basics of using your mt182L:

Topic 1: Atrust Quick Connection

Topic 2: Setting Up a Wireless Connection

Topic 3: Configuring the Time Zone

Topic 4: Accessing Desktops or Applications

- Microsoft Remote Desktop Services (RDP sessions)
- Citrix Services (ICA sessions)
- VMware View or Horizon View Services (View sessions)

Topic 5: Using Built-in Applications

Topic 6: Viewing and Managing the Use of Power

NOTE

- In case that ***by default*** your mt182L is Auto Setup enabled, its user environment might be different from here and will vary with preset configurations. See section 3.2.9 and appendix A.4, and consult your IT administrator for details.

NOTE

- Three client modes are available for your mt182L:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: (n/a to Web browser) • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client
3	Quick Connection	The client will enter Atrust Quick Connection screen after system startup.

- In Quick Connection mode, you can access Microsoft Remote Desktop / Citrix / VMware View or Horizon View services ***quickly*** without much client configuration required. The main purpose of this chapter is to guide you through the use of your mt182L under the Quick Connection mode. The ***default*** of your mt182L is ***NOT*** the Quick Connection mode (after restart it will enter the local Linux desktop rather than Atrust Quick Connection screen).
- To understand other modes, configure advanced settings, and customize your mt182L, please refer to chapter 3 "Configuring Client Settings" on page 41.

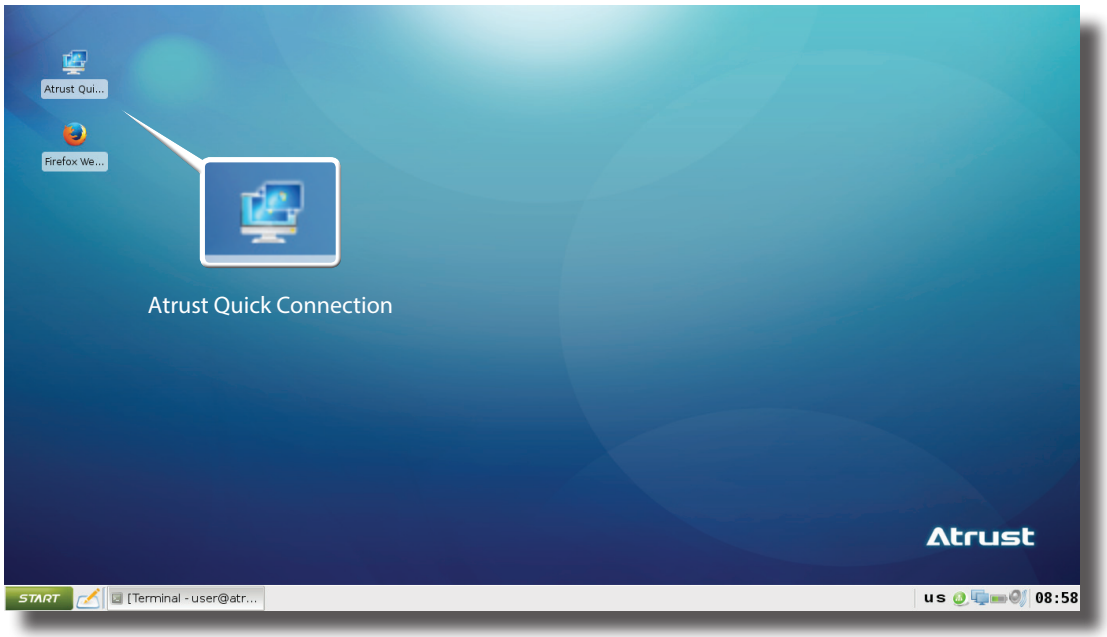
Topic 1: Atrust Quick Connection

To start using your mt182L, please do the following:

1. Press the Power button to turn on the client. Wait a moment for the system to enter the local Linux desktop.

Local Linux Desktop

2. Click **Atrust Quick Connection** on the desktop to enter ***Atrust Quick Connection screen***.



TIP

- If you don't see that shortcut, click **START** > **Settings** > **Atrust Client Setup** > **System** > **Quick Connection** to enable Quick Connection.

3. (a) Go to **Topic 2** to set up a wireless connection if needed.
   (b) Go to **Topic 3** to set the time zone for the ***first time*** use.
   (c) Go to **Topic 4** for service access if the time zone had been set.

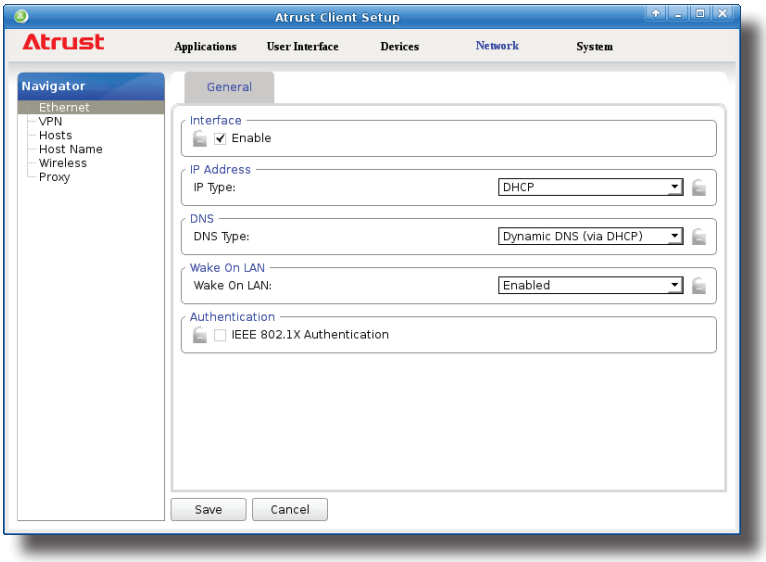
Atrust Quick Connection Screen

No.	Icon	Description
1	Power Off	Click to shut down, suspend, or restart the system.
2	Local Desktop	Click to return to the local Linux desktop.
3	Setup	Click to launch Atrust Client Setup.
4	Mixer	Click to configure audio settings.
5	Power	Indicates the power source (adapter, battery, or both) and status. Click to launch Power Management for details. **NOTE:** Power Management enables you to configure power-saving settings for your mt182L. You can choose appropriate options to suit your needs. See "Topic 6: Viewing and Managing the Use of Power" on page 38 for details. **NOTE:** When your mt182L enters ***System Sleep mode*** manually (**Fn** + **F12** or > **Suspend**) or automatically (configured in Atrust Client Setup through **System** > **Power Management**), it still requires a certain amount of power. You can use **Shut down** option instead to save the power to a greater degree. **NOTE:** When using only the battery as the power source, ensure that it has enough power to prevent data loss.
6	Network	Indicates the network type (wired or wireless) and status. Click to configure network settings. **NOTE:** To set up a wireless connection, please see "Topic 2: Setting Up a Wireless Connection" on page 16.

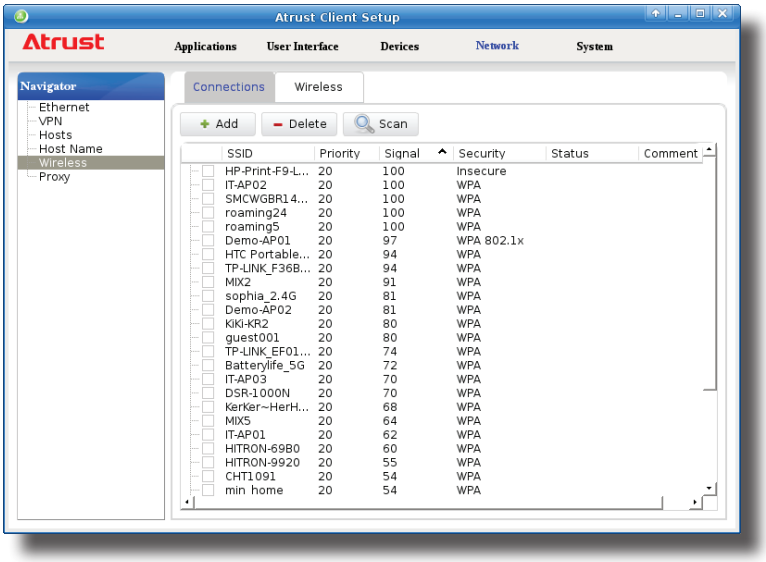
Topic 2: Setting Up a Wireless Connection

To set up a wireless connection, please do the following:

1. On Atrust Quick Connection screen, click the Network icon. Atrust Client Setup is launched.



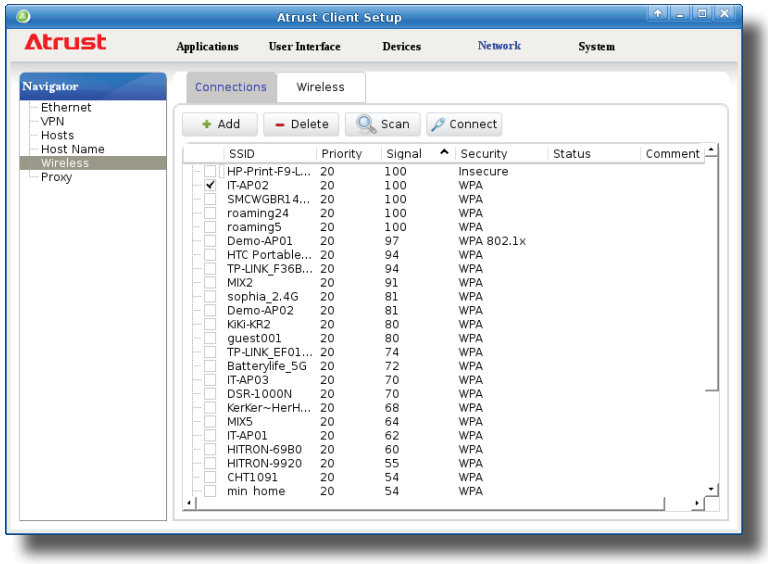
2. Click **Wireless**. The Wireless Network list will be shown under the Connections sub-tab.



NOTE

- Your mt182L will perform network discovery ***once*** and specify all available wireless networks in the Wireless Network list under the Connections sub-tab. To refresh this Wireless Network list, click Scan on the top of the list.

3. Click to check the desired wireless network. The Connect button Connect then appears on the top of the Wireless Network list.

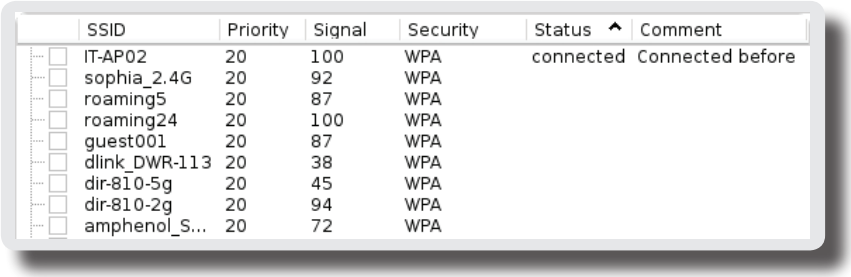


4. Click Connect to create a wireless network connection through the selected wireless network.
5. A window appears prompting for confirmation or authentication.

NOTE

- If you ever accessed this wireless network before, the password will be automatically recorded for future access. In this case, you don't need to provide the password again; you only need to confirm the establishment of a wireless connection.
- Consult your network administrator for required information on authentication.

6. Type in the required password, and then click **Connect** to continue. Or, click **OK** to confirm the establishment of a wireless connection.
7. Upon completion, the Status column of the wireless network will show **connected**.



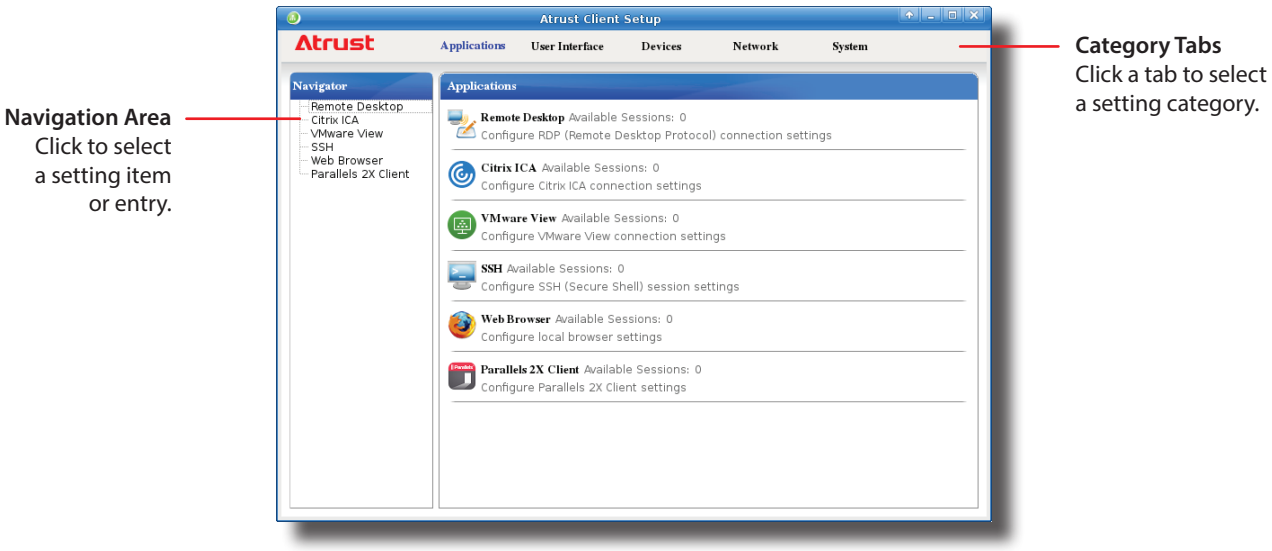
8. Close Atrust Client Setup.

Topic 3: Configuring the Time Zone

To set the time zone for your mt182L, please do the following:

1. Click the **Setup** icon to launch Atrust Client Setup.

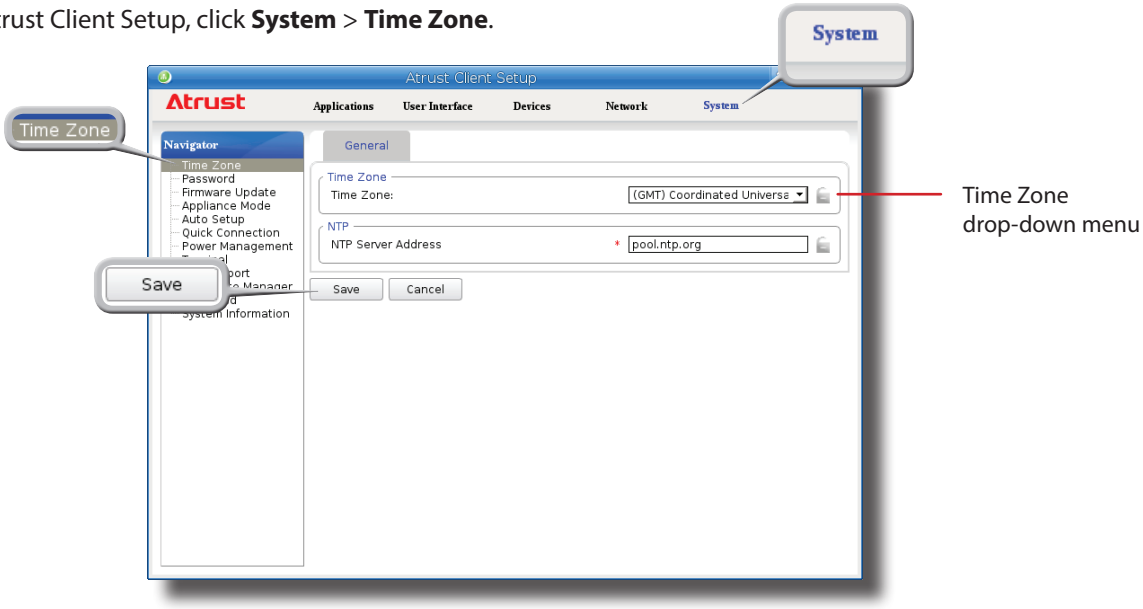
Atrust Client Setup



NOTE

- For detailed instructions on how to configure client settings and customize your mt182L with Atrust Client Setup, please refer to chapter 3 "Configuring Client Settings" on page 41.

2. On Atrust Client Setup, click **System** > **Time Zone**.



3. Click the Time Zone drop-down menu to select the desired time zone.
4. Click **Save** to apply, and then close Atrust Client Setup.

Topic 4: Accessing Desktops or Applications

Through Atrust Quick Connection screen, you can access three types of desktop virtualization services: **Remote Desktop**, **Citrix**, and **VMware View**.

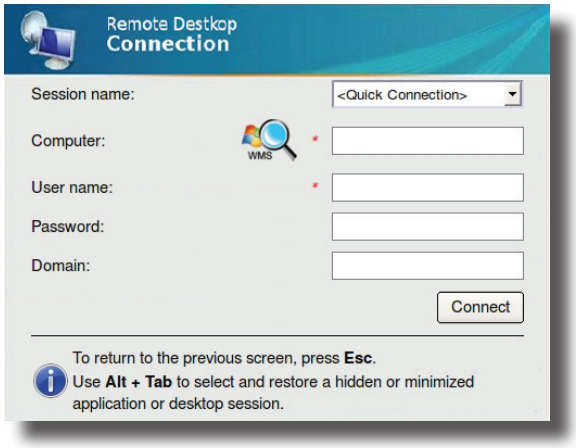
Atrust Quick Connection Screen

Icon	Description	Page
Remote Desktop	Click to access Microsoft Remote Desktop services.	20
Citrix	Click to access Citrix XenApp, XenDesktop, or VDI-in-a-Box services.	21
VMware View	Click to access VMware View or Horizon View services.	33

Accessing Microsoft Remote Desktop Services

To access Microsoft Remote Desktop services, please do the following:

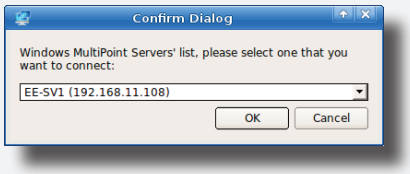
1. Click Remote Desktop on Atrust Quick Connection screen (see the screen in Topic 4).
2. On the appeared window, type in the computer name or IP address of the server, user name, password, and domain (if any), and then click **Connect**.



NOTE

- To discover available Windows MultiPoint Server systems over your network, please do the following:

  1. Click WMS on the left of the Computer field.
  2. Upon completion, a window appears with the search result.



  3. Click the drop-down menu to select the desired system, and then click **OK**.
  4. The IP address of the selected system will appear in the Computer field.

- To return to ***Atrust Quick Connection screen*** (see the screen in Topic 4), press **Esc**.

3. The remote desktop will be displayed on the screen.

Accessing Citrix Services

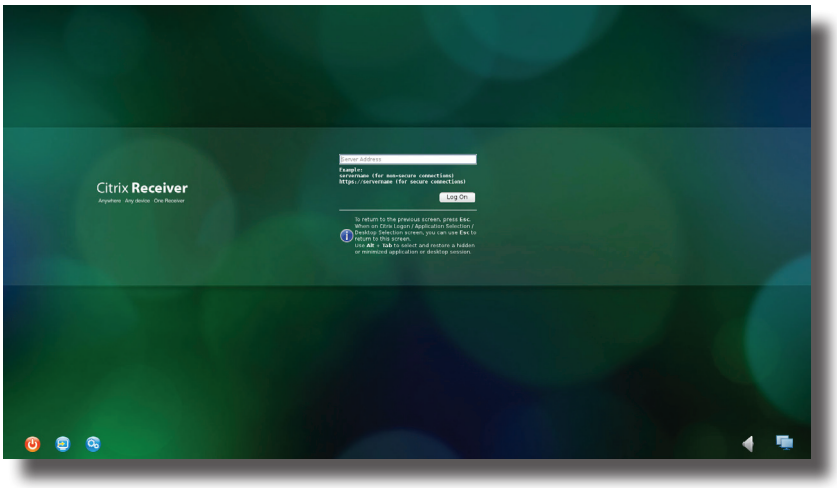
Connecting to the Server

To connect to the server through which Citrix services are accessible, please do the following:

1. Click

on Atrust Quick Connection screen (see the screen in Topic 4).
2. On the appeared ***Atrust Citrix Connection screen***, enter the appropriate IP address / URL / FQDN of the server, and then click **Log On**.

Atrust Citrix Connection Screen



NOTE

- For newer versions of XenDesktop and XenApp, you may need to further specify the sub-path of the server. Refer to the following table for details:

Citrix Product	Component to Connect	Connection Address
XenApp 6.5 or earlier	Web Interface	IP / URL / FQDN
XenDesktop 5.6 or earlier	Web Interface	IP / URL / FQDN
Virtual Apps and Desktops (XenApp and XenDesktop 7.5 or later)	StoreFront	IP / URL / FQDN **plus** *sub-path* **For example —** **FQDN:** X75.CTX.poc **Sub-path:** /Citrix/StoreWeb (default) **Connection Address:** X75.CTX.poc/Citrix/StoreWeb

- FQDN is the acronym of Fully Qualified Domain Name.
- To return to ***Atrust Quick Connection screen*** (see the screen in Topic 4), press **Esc**.

Logging On to Citrix Services

When connected to the server, the ***Citrix Logon screen*** appears. The appeared screen and required credentials for Citrix services may vary with the service type and version.

NOTE

- A warning message "This Connection is Untrusted" might appear. Consult the IT administrator for details and ensure the connection is secure ***first***. To import a security certificate, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73. To bypass, click **I Understand the Risks** > **Add Exception** > **Confirm Security Exception**.

The following are some examples of Citrix Logon screens.

XenDesktop 5.6 Platinum:

Citrix Logon Screen

Type the required user name, password, and then click **Log On** to access virtual desktops.

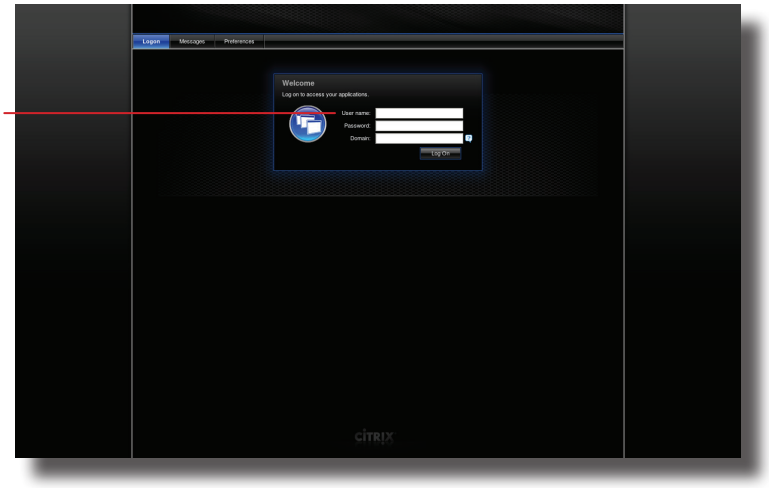
NOTE

- To return to Atrust Quick Connection screen, press **Esc**.

XenApp 6.0 Fundamentals:

Citrix Logon Screen

Type the required user name, password, domain, and then click **Log On** to access virtual applications.



NOTE

- To return to Atrust Quick Connection screen, press **Esc**.
- If your XenApp server doesn't belong to any domain, type the computer name of the server in the Domain field.

XenApp 6.5 Platinum:

Citrix Logon Screen

Type the required user name, password, domain, and then click **Log On** to access virtual applications.

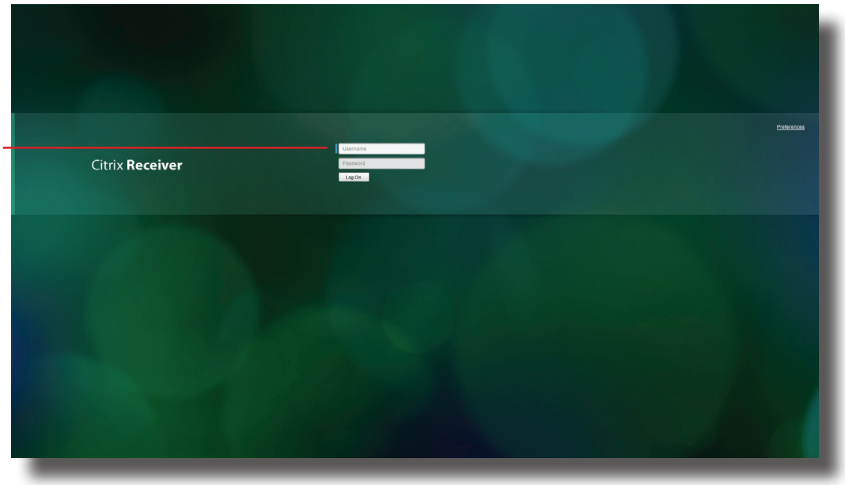
NOTE

- To return to Atrust Quick Connection screen, press **Esc**.
- If your XenApp server doesn't belong to any domain, type the computer name of the server in the Domain field.

VDI-in-a-Box:

Citrix Logon Screen

Type the required user name, password, and then click **Log On** to access virtual desktops.



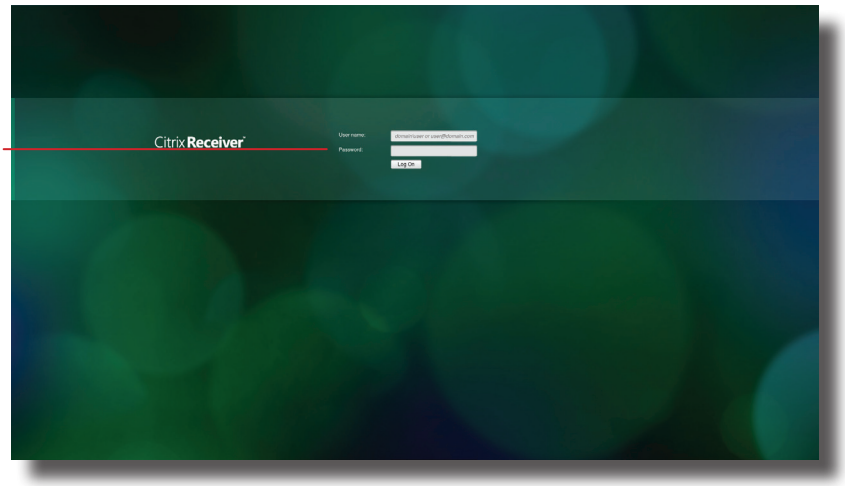
NOTE

- To return to Atrust Quick Connection screen, press **Esc**.

XenApp and XenDesktop 7.5 Platinum:

Citrix Logon Screen

Type the required user name, password, and then click **Log On** to access virtual desktops.



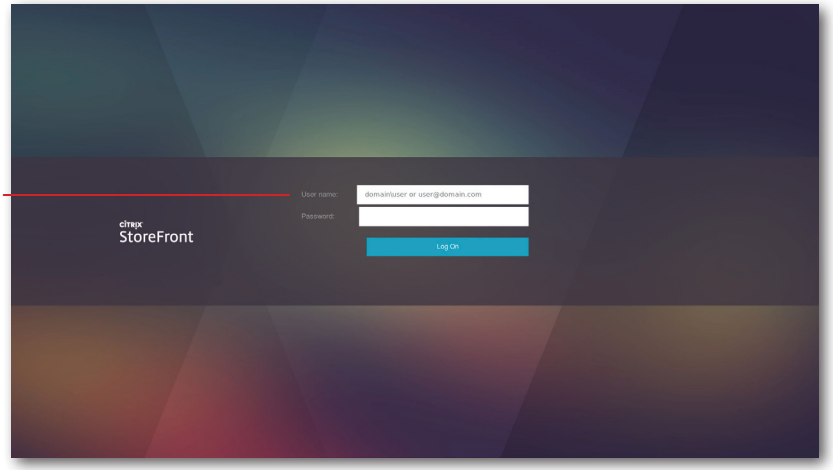
NOTE

- To return to Atrust Quick Connection screen, press **Esc**.

Virtual Apps and Desktops 7 1808.2:

Citrix Logon Screen

Type the required user name, password, and then click **Log On** to access virtual applications and desktops.



NOTE

- To return to the Quick Connection screen, press **Esc**.

Accessing Virtual Desktops and Applications

You will enter the ***Desktop Selection*** or ***Application Selection screen*** after logon. On the screen you can click to select the desired desktop or application(s).

NOTE

- You might enter the virtual desktop directly if only one type of virtual desktop is assigned to the provided credentials.

TIP

- Use **Alt + Tab** to select and restore a hidden or minimized application or desktop.

The following are some examples of Selection screens and delivered desktops and applications.

XenDesktop 5.6 Platinum:

1. The ***Desktop Selection screen*** appears after logon.

Desktop Selection Screen

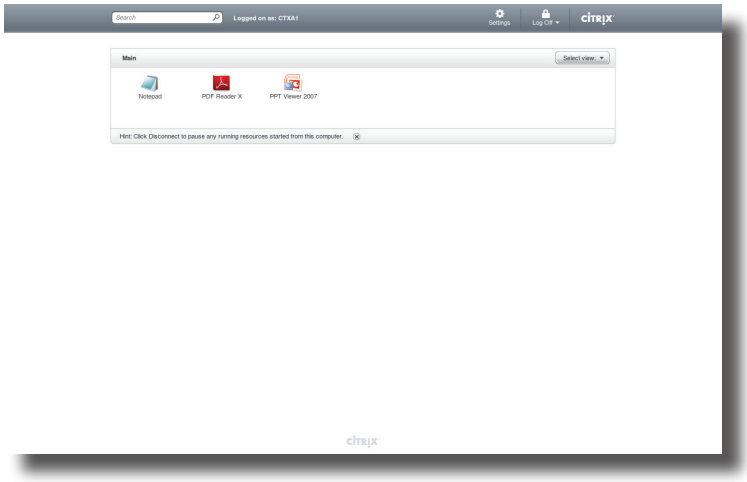
2. Click to select the desired desktop.
3. The selected virtual desktop will be displayed on the screen.

Virtual Desktop Example: Windows 7 Ultimate

XenApp 6.5 Platinum:

1. The ***Application Selection screen*** appears after logon.

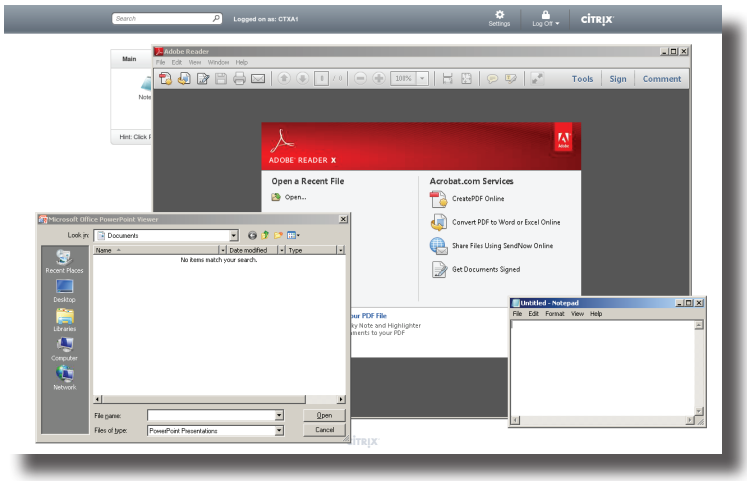
Application Selection Screen



2. Click to select the desired application(s).
3. The selected application(s) will be displayed on the screen.

Virtual Application Examples

PowerPoint Viewer, Adobe Reader, and Notepad



NOTE

- Clicking on Application Selection screen will bring the screen to the front and leave all launched application windows hidden behind. Use **Alt + Tab** to select and restore a hidden or minimized application window.
- Exiting a virtual desktop or application will return to the ***Desktop Selection*** or ***Application Selection screen***. On the screen, you can:
  - ✧ Click to launch another virtual desktop if any or to launch other applications.
  - ✧ Click **Log Off** on the top of the screen to return to the ***Citrix Logon screen***.
  - ✧ Press **Esc** to return to ***Atrust Quick Connection screen*** directly.

XenApp and XenDesktop 7.5 Platinum:

1. The ***Application Selection*** / ***Desktop Selection screen*** appears after logon.

Application Selection Screen

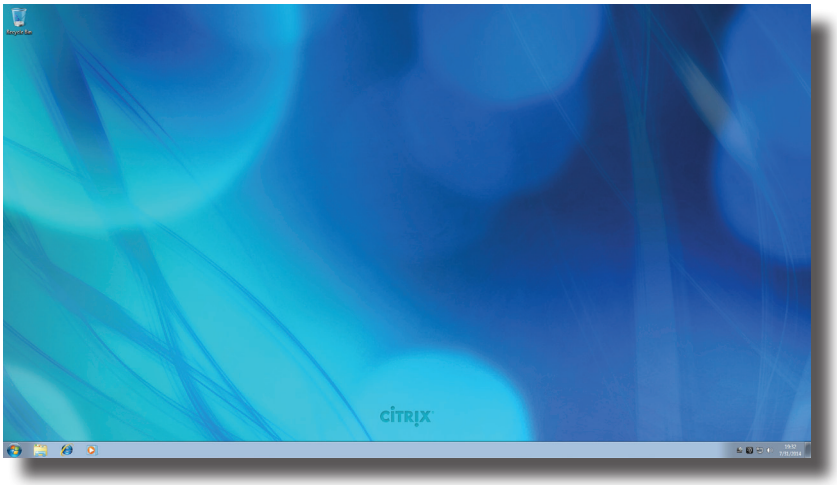
You might see this screen when you log in to XenApp 7.5 for first time. Just click to add your favorite apps from a list.

Two buttons may be available for your to switch between ***Application*** and ***Desktop Selection screen***, depending on your server-side deployment.

Desktop Selection Screen

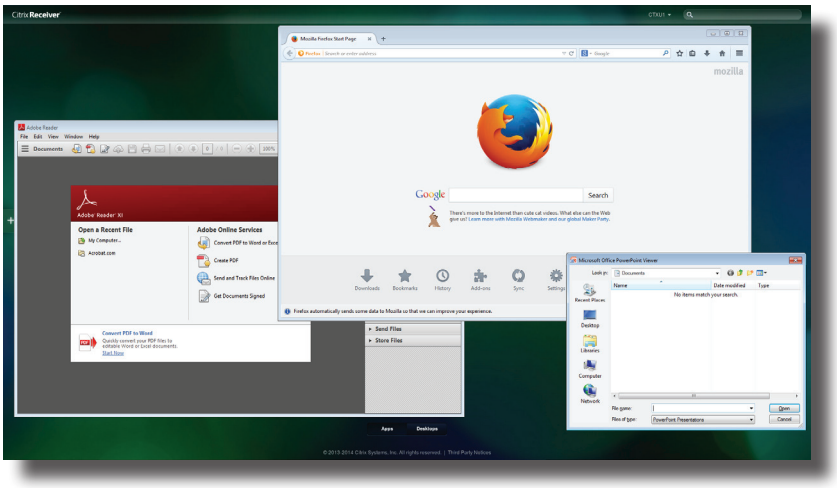
2. Click to select the desired application(s) or desktop.
3. The selected application(s) or desktop will be displayed on the screen.

Virtual Desktop Example: Windows Server 2008 R2



Virtual Application Examples

Adobe Reader, Mozilla Firefox, and PowerPoint Viewer



NOTE

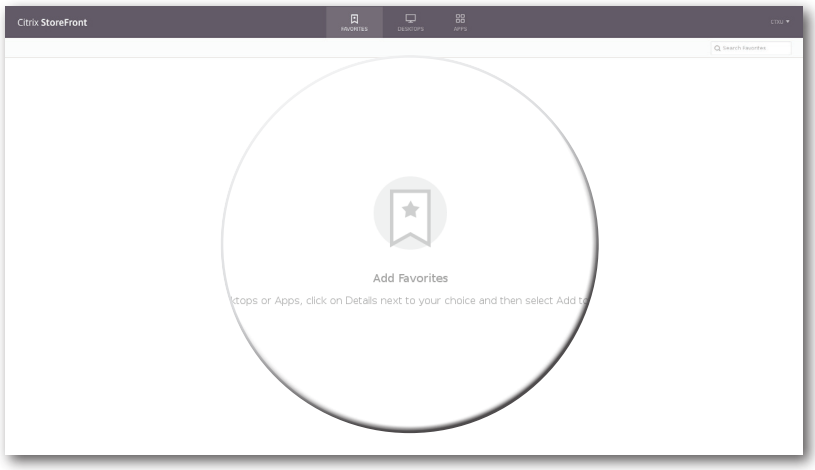
- Clicking on Application Selection screen will bring the screen to the front and leave all launched application windows hidden behind. Use **Alt + Tab** to select and restore a hidden or minimized application window.
- Exiting a virtual desktop or application will return to the ***Desktop Selection*** or ***Application Selection screen***. On the screen, you can:
  - ✧ Click to launch another virtual desktop if any or to launch other applications.
  - ✧ Click **Log Off** on the top of the screen to return to the ***Citrix Logon screen***.
  - ✧ Press **Esc** to return to ***Atrust Quick Connection screen*** directly.

Virtual Apps and Desktops 7 1808.2:

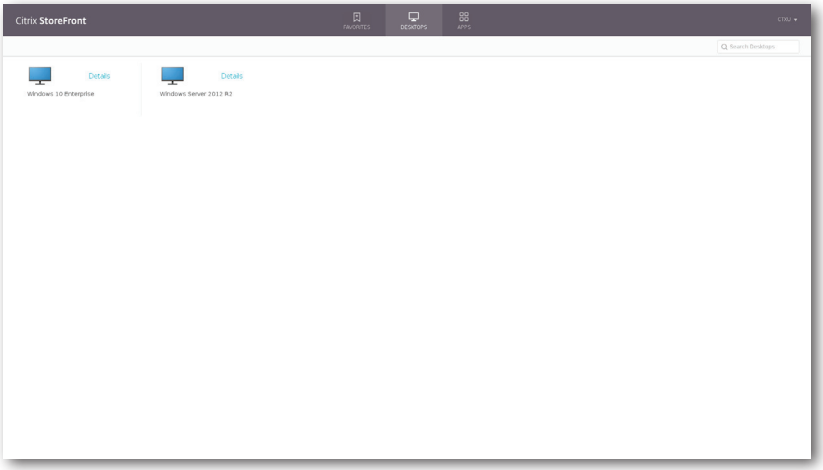
1. The ***Favorites*** / ***Application Selection*** / ***Desktop Selection screen*** appears after logon.

Favorites Screen

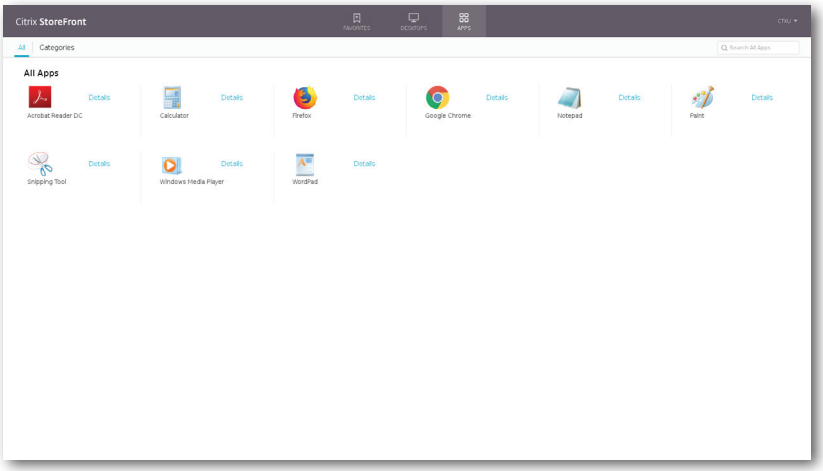
You might see this screen when you log in. To add favorites, just follow the on-screen instructions.



Desktop Selection Screen



Application Selection Screen

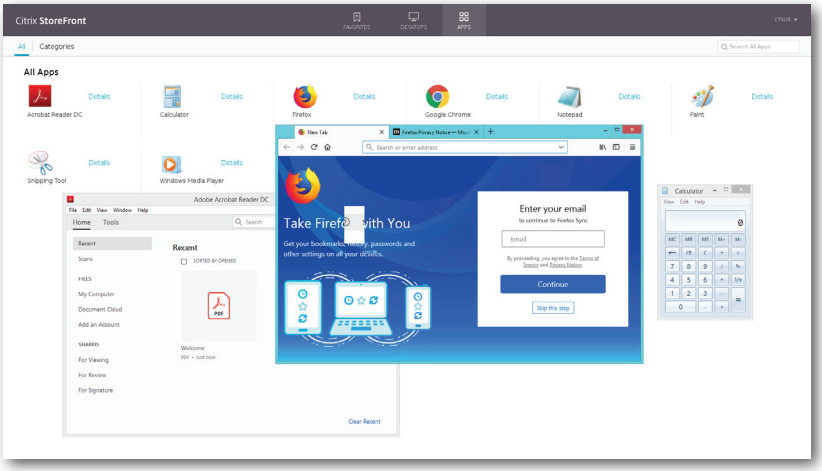


2. Click to select the desired application or desktop.
3. The selected application or desktop will be displayed on the screen.

Virtual Desktop Example: Windows 10 Enterprise

Virtual Application Examples

Launched Adobe Reader DC, Mozilla Firefox, and Calculator



NOTE

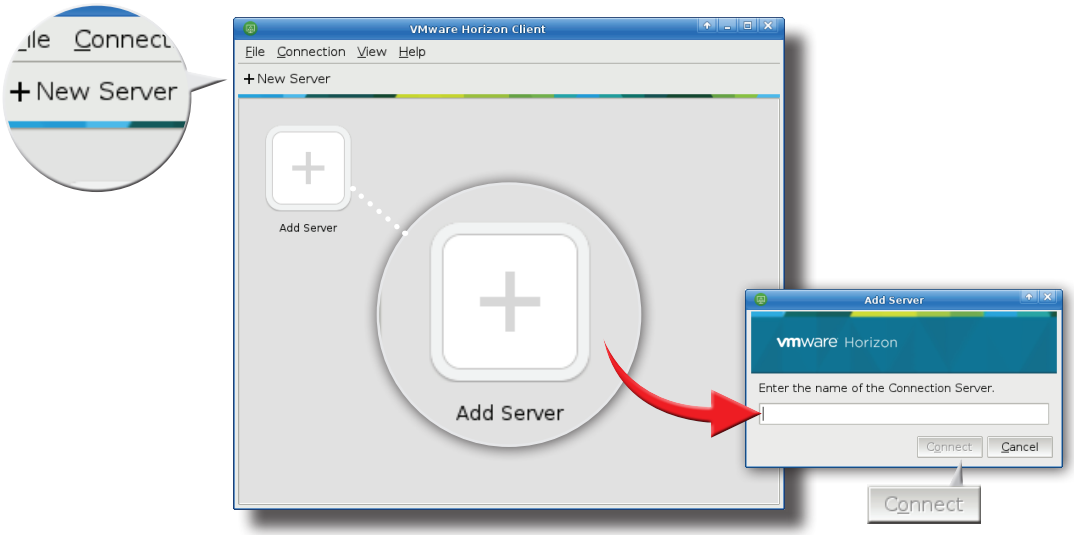
- Clicking on Application Selection screen will bring the screen to the front and leave all launched application windows hidden behind. Use **Alt + Tab** to select and restore a hidden or minimized application window.
- Exiting a virtual desktop or application will return to the ***Favorites*** / ***Desktop Selection*** / ***Application Selection screen***. On the screen, you can:
  - ✧ Click to launch another virtual desktop if any or to launch other applications.
  - ✧ Click **Log Off** on the top of the screen to return to the ***Citrix Logon screen***.
  - ✧ Press **Esc** to return to the ***Quick Connection screen*** directly.

Accessing VMware View or Horizon View Services

To access VMware View or Horizon View services, please do the following:

1. Click

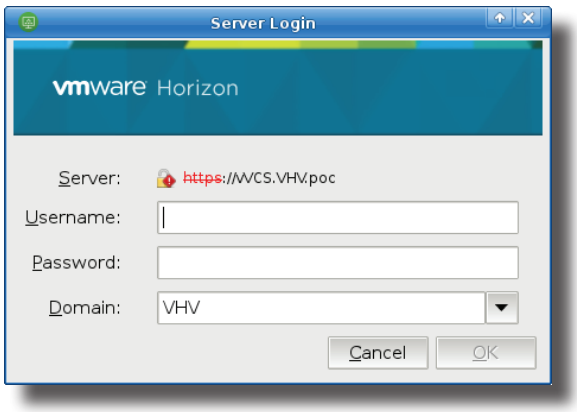
on Atrust Quick Connection screen (see the screen in Topic 4).
2. On the opened window, double-click **Add Server** icon or click **New Server** in the top-left corner. A window appears prompting for the name or IP address of the VMware View Connection Server.
3. Enter the required information, and then click **Connect**.



NOTE

- To return to ***Atrust Quick Connection screen*** (see the screen in Topic 4), close the opened window.

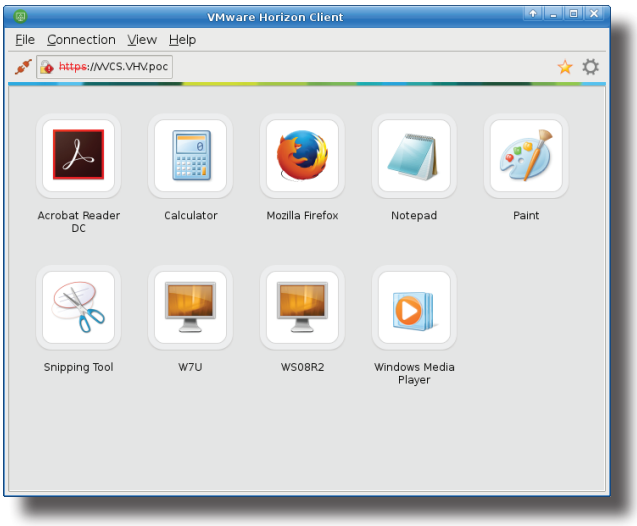
4. A Welcome window might appear, click **OK** to continue.
5. A window appears prompting for the credentials. Enter your user name, password, click the Domain drop-down menu to select the domain, and then click **OK**.



NOTE

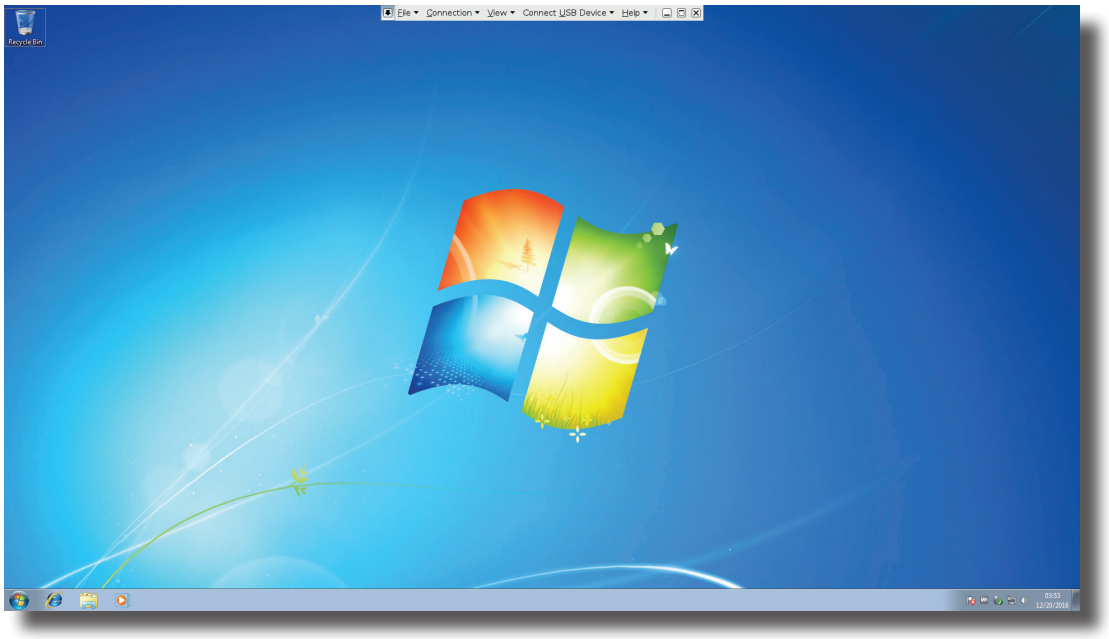
- A window might appear with a certificate message about the remote server. Consult the IT administrator for details and ensure the connection is secure ***first***. To import a security certificate, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73. To bypass, click **Connect Insecurely**.

6. The Desktop and Application list appears with available desktops and/or applications for the provided credentials. Double click to select the desired desktop or application.



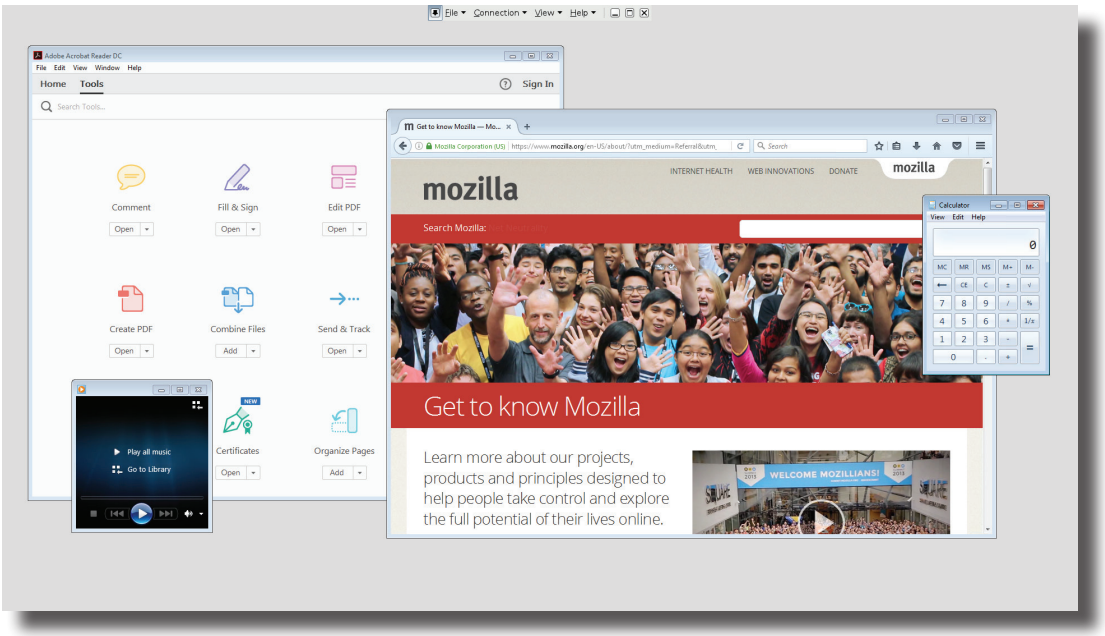
7. The virtual desktop or application will be displayed on the screen.

Virtual Desktop Example
Windows 7 Ultimate



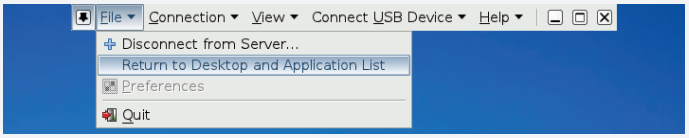
Virtual Application Examples (VMware Horizon 6 with View)

Adobe Reader, Windows Media Player, Mozilla Firefox, and Calculator

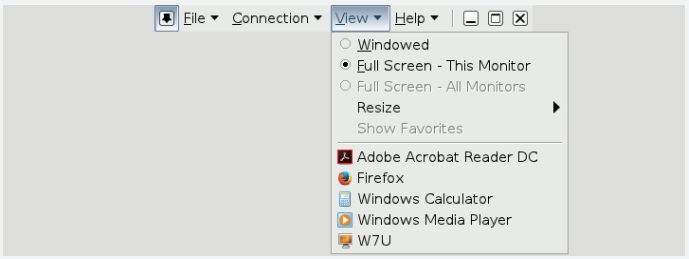


NOTE

- Your desktop or application will be displayed in full screen. You can:
  - ✧ Click **File** > **Return to Desktop and Application List** on the top tool bar to recall the Desktop and Application list.



  - ✧ Click **View** on the top tool bar to switch to a virtual desktop or application.

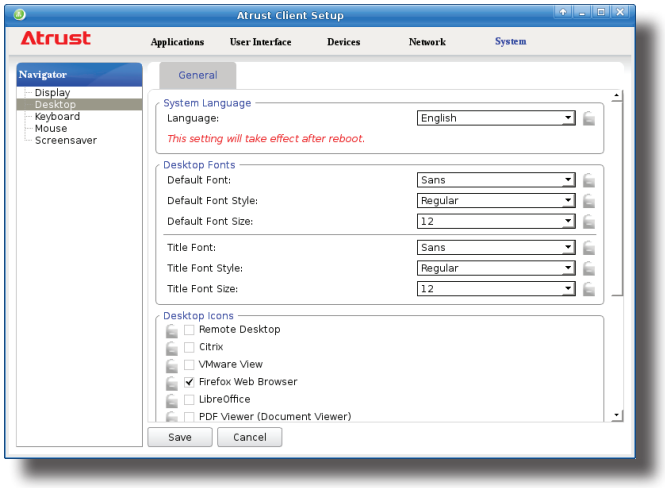


Topic 5: Using Built-in Applications

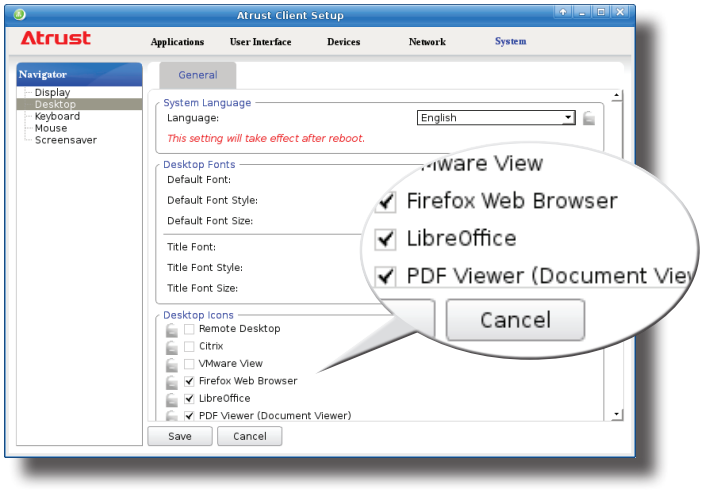
To use built-in applications (Web browser, PDF viewer, LibreOffice, etc), please do the following:

> **NOTE**
>
> - The access shortcuts for built-in applications may be hidden by default. You need to enable the display of those shortcuts on the desktop and START menu ***first***.

1. Enable the display of application shortcuts on the local desktop and START menu.
   1) On the local desktop, click **START** > **Settings** > **Atrust Client Setup** to launch Atrust Client Setup.
   2) On Atrust Client Setup, click **User Interface** > **Desktop**.

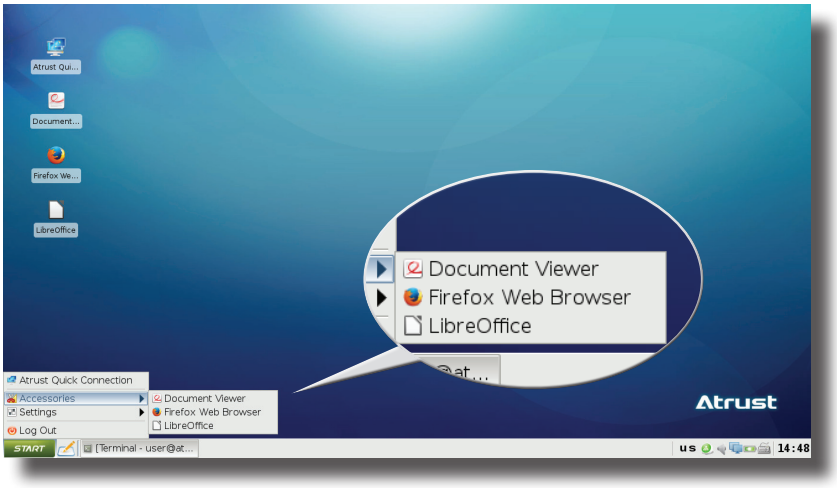


   3) Click to check **LibreOffice** and **PDF Viewer**, and then click **Save** to apply.



   4) Close Atrust Client Setup.

2. The shortcuts appear on the local desktop and START menu.

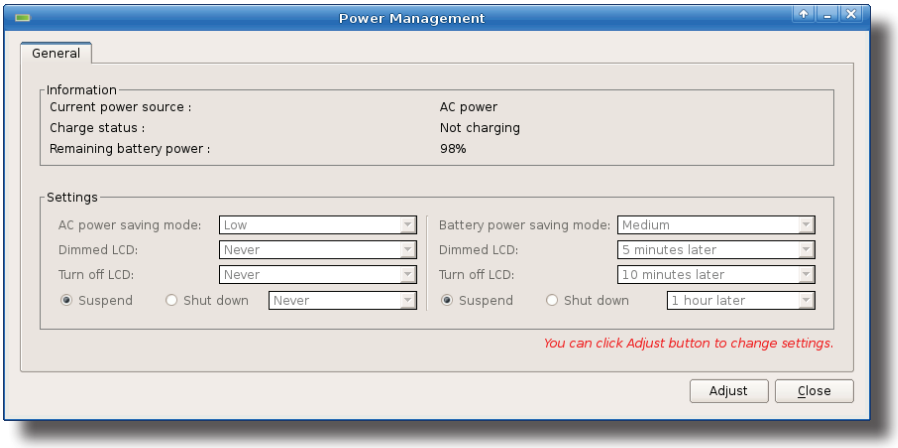


3. Click shortcuts on the desktop or START menu to launch applications.

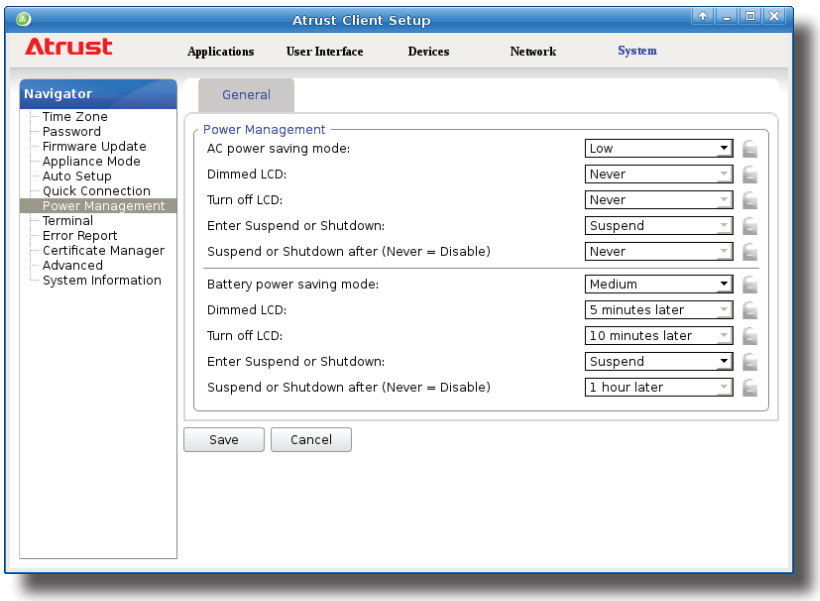
Topic 6: Viewing and Managing the Use of Power

To view and manage the use of power for your mt182L, please do the following:

1. On Atrust Quick Connection screen or on the local Linux desktop, click the **Power** icon in the bottom-right corner to launch Power Management. Here you can view the use and settings of power.



2. If needed, click **Adjust** to launch Atrust Client Setup to configure the settings of power.



3. Choose the desired power-saving mode for your AC power and battery, or choose **Custom** to customize individual settings, and then click **Save** to apply.

NOTE

- When your mt182L enters ***System Sleep mode*** manually (**Fn** + **F12** or > **Suspend**) or automatically (configured in Atrust Client Setup through **System** > **Power Management**), it still requires a certain amount of power. You can use **Shut down** option instead to save the power to a greater degree.

WARNING

- When using only the battery as the power source, ensure that it has enough power to prevent data loss.

3

Configuring Client Settings

This chapter provides instructions on how to configure advanced settings and customize your mt182L with Atrust Client Setup.

3.1 Atrust Client Setup

Interface overview 43
Available settings at glance 44

3.2 Configuring System Settings

System tab overview 45
Available settings at a glance 46

3.3 Configuring User Interface Settings

User Interface tab overview 79
Available settings at a glance 80

3.4 Configuring External Device Settings

Devices tab overview 93
Available settings at a glance 94

3.5 Configuring Network Settings

Network tab overview 103
Available settings at a glance 104

3.6 Configuring Service Access Settings

Applications tab overview 127
Available settings at a glance 128

3.1 Atrust Client Setup

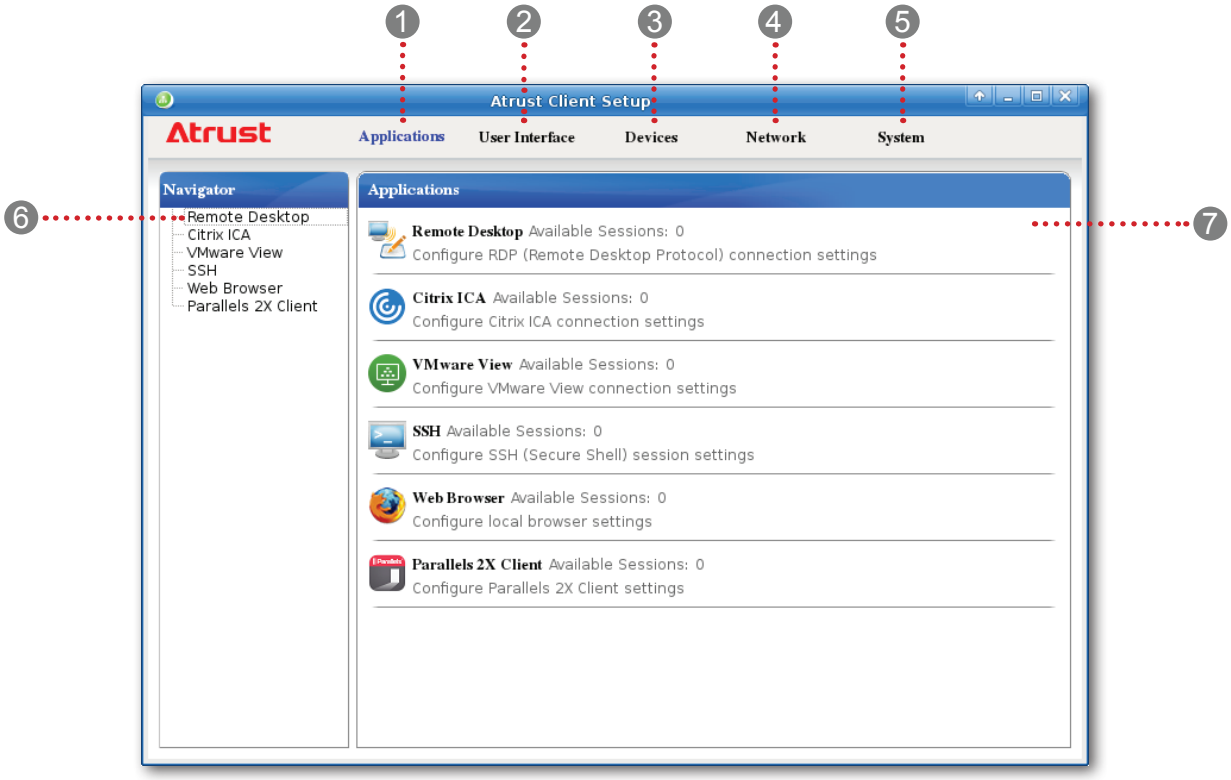
Your mt182L comes with Atrust Client Setup, the built-in local client management console to help you configure client settings and customize your mt182L.

3.1.1 Interface Overview

To access Atrust Client Setup on your mt182L, please do the following:

1. On Atrust Quick Connection screen, click the **Setup** icon to launch Atrust Client Setup.
2. The Atrust Client Setup window appears.

Interface Overview



Interface Elements		
No.	**Name**	**Description**
1	Applications tab	Click to configure settings for service access through the client.
2	User Interface tab	Click to configure settings for the user interface of the client.
3	Devices tab	Click to configure settings for external devices of the client.
4	Network tab	Click to configure settings for the connectivity of the client to networks and servers.
5	System tab	Click to configure settings for the operation and maintenance of the client.
6	Navigation area	Click to select a setting item under a selected tab or to select a setting entry under a selected setting item.
7	Configuration area	Configures setting values when a setting item or entry is selected.

3.1.2 Client Settings at a Glance

The following table provides a brief description of each setting item under five main setting categories.

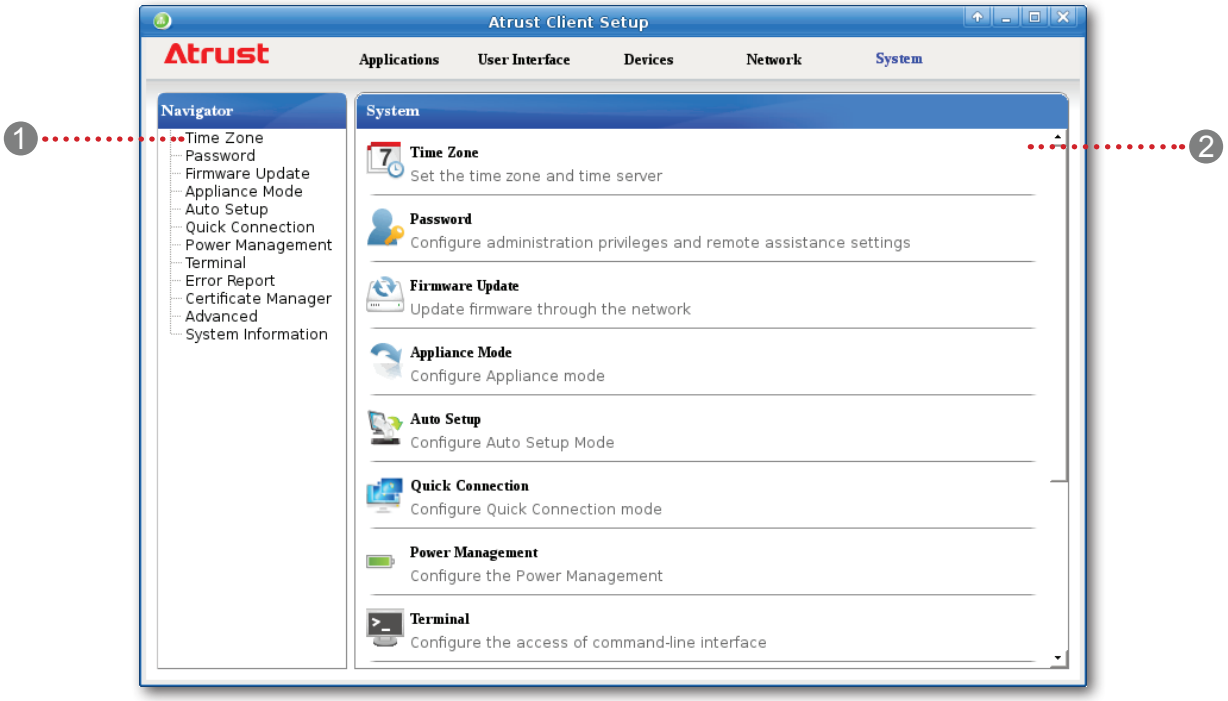
Tab	Setting Item	Section	Page
System	• Configuring time zone and time server • Configuring passwords • Configuring remote assistance settings • Updating firmware • Enabling/Disabling the Appliance mode • Enabling Auto Setup • Configuring Quick Connection • Managing the use of power • Enabling/Disabling the execution of the text-based (command-line) functions • Collecting event logs, capturing related screens, and upload files for error reporting • Importing certificates for remote computers • Enabling/Disabling Auto Registration • Viewing system and network information	3.2 Configuring System Settings	45
User Interface	• Configuring display settings • Customizing desktop and system language • Hiding/Showing Quick Access shortcuts • Using a custom wallpaper • Adjusting keyboard settings • Adjusting mouse settings • Configuring screensaver settings	3.3 Configuring User Interface Settings	79
Devices	• Configuring settings for USB storage devices • Configuring settings for audio devices • Configuring settings for local/network printers	3.4 Configuring External Device Settings	93
Network	• Configuring wired network settings • Configuring VPN settings • Creating the mapping of IP addresses to the names or aliases of hosts • Creating the Failover Cluster list • Changing the host name of your client • Configuring wireless network settings • Configuring proxy settings for Web-based access to services	3.5 Configuring Network Settings	103
Applications	• Configuring Microsoft RDP connection settings • Configuring Citrix ICA connection settings • Configuring VMware View connection settings • Configuring SSH connection settings • Configuring local Web browser settings • Configuring Parallels 2X connection settings	3.6 Configuring Service Access Settings	127

3.2 Configuring System Settings

3.2.1 System Tab Overview

System tab enables you to configure settings for the operation and maintenance of clients. To access available settings of **System** tab, click the tab on Atrust Client Setup.

System Tab Overview



Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **System** tab.
2	Configuration area	Configures setting values when a setting item or entry is selected.

3.2.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
System	Time Zone		Click to configure the time zone and time server for your mt182L.	3.2.3	47
	Password		Click to configure the access privileges of Atrust Client Setup for mt182L users. Click to set the login password for the local desktop. Click to configure settings for remote assistance.	3.2.4 3.2.5 3.2.6	48 52 54
	Firmware Update		Click to update firmware through the network. This feature is applicable to the client only when the client is managed by the remote Atrust Device Manager console.	3.2.7	56
	Appliance Mode		Click to enable/disable the Appliance mode to allow / disallow the automatic RDP / ICA / View / Web / 2X sessions. In Appliance mode, the client starts up directly with the desired RDP / ICA / View / Web / 2X session and performs the configured action after exiting the session.	3.2.8	58
	Auto Setup		Click to enable Auto Setup to allow the client to get its preset configurations on startup and enter the desired user environment automatically.	3.2.9	62
	Quick Connection		Click to configure the Quick Connection mode.	3.2.10 3.2.11	62 64
	Power Management		Click to manage the use of power.	3.2.12	68
	Terminal		Click to enable/disable the execution of the text-based (command-line) functions.	3.2.13	69
	Error Report		Click to collect error log and launch the screen capturing program for error reporting. Click to upload files to a specified FTP server for error reporting.	3.2.14 3.2.15	70 72
	Certificate Manager		Click to import or manage certificates for remote computers.	3.2.16	73
	Advanced		Click to configure advanced settings such as Auto Registration.	3.2.17	77
	System Information		Click to view detailed system and network information.	3.2.18	78

NOTE

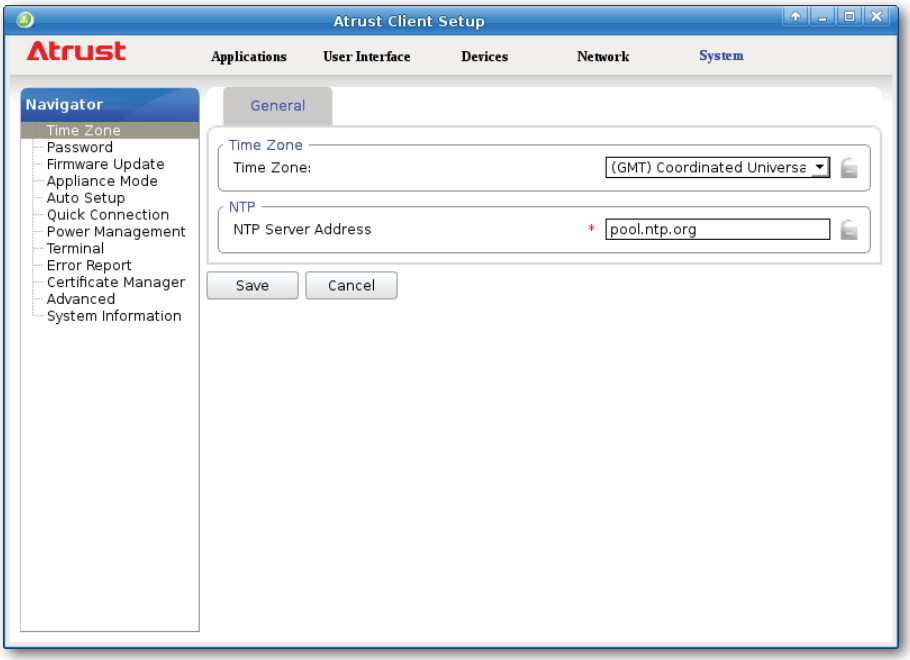
- Atrust Device Manager is a remote and mass client management console, helping you remotely manage a large number of endpoint devices in a desktop virtualization infrastructure. For more information about Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

3.2.3 Configuring Time Zone and Time Server

The Time Zone setting allows you to configure the desired time zone and time server to get the accurate system time for your mt182L.

To set the desired time zone and time server, please do the following:

1. On Atrust Client Setup, click **System** > **Time Zone**.



2. Under the Time Zone section, click the drop-down menu to select the desired time zone.
3. Under the NTP (Network Time Protocol) section, use the default or type in the desired time server.

> **NOTE**
>
> - The IP address of the default time server is **pool.ntp.org**. For more information on the default, please refer to the website for the NTP Pool Project at www.pool.ntp.org.
> - Ensure the connectivity of your mt182L to the network or Internet in order to get accurate time from the time server.

4. Click **Save** to apply.

3.2.4 Configuring the Access Privileges and Passwords of Atrust Client Setup

You can configure the access privileges of Atrust Client Setup for mt182L users by the Password setting.

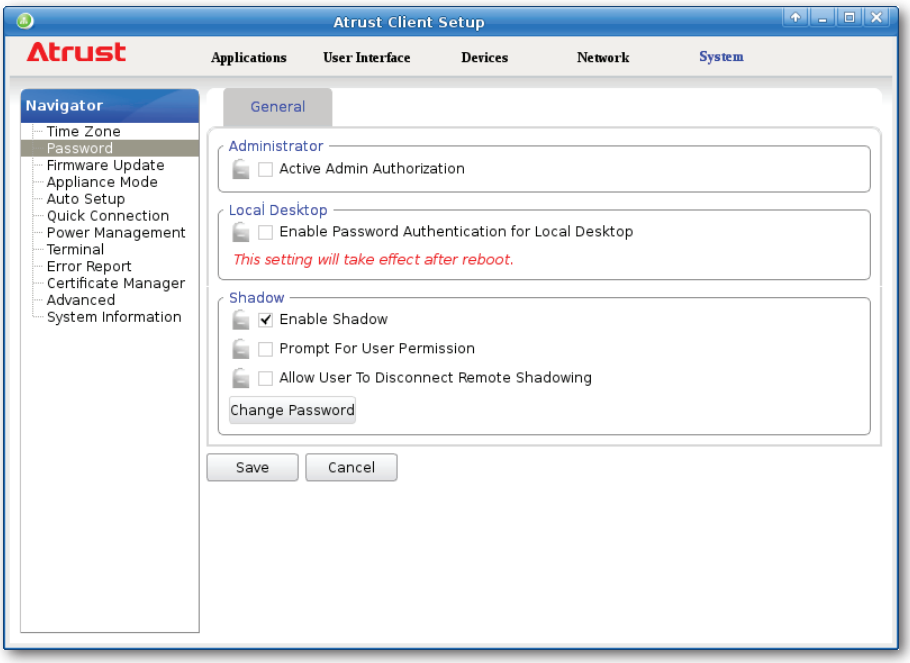
NOTE

- All mt182L users are allowed to access Atrust Client Setup by factory default. You can make changes as desired using this setting.

Setting Access Privileges and Password Only for Administrators

To set access privileges and password only for administrators, please do the following:

1. On Atrust Client Setup, click **System** > **Password**.



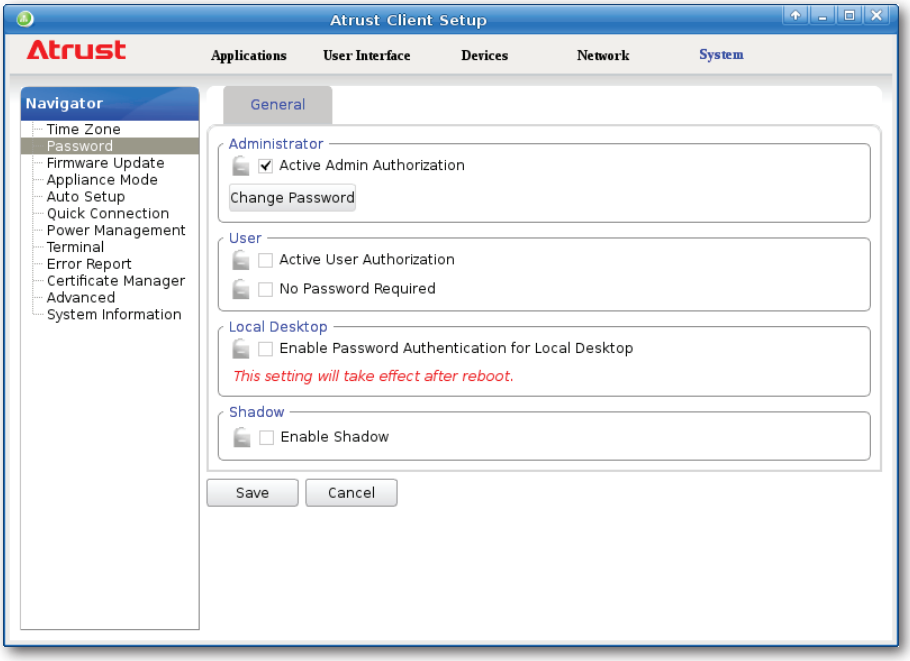
2. Under the Administrator section, click to check **Active Admin Authorization**.
3. The access privileges for administrators are granted and a window appears for you to set the password.

4. Type in the desired password, and then click **OK** to confirm.
5. Click **Save** to save all the changes.

Setting Access Privileges and Password Also for Standard Users

To set access privileges and password also for standard users, please do the following:

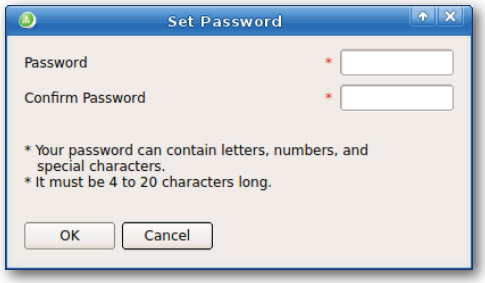
1. On Atrust Client Setup, click **System** > **Password**.
2. Under the User section, click to check **Active User Authorization**.



NOTE

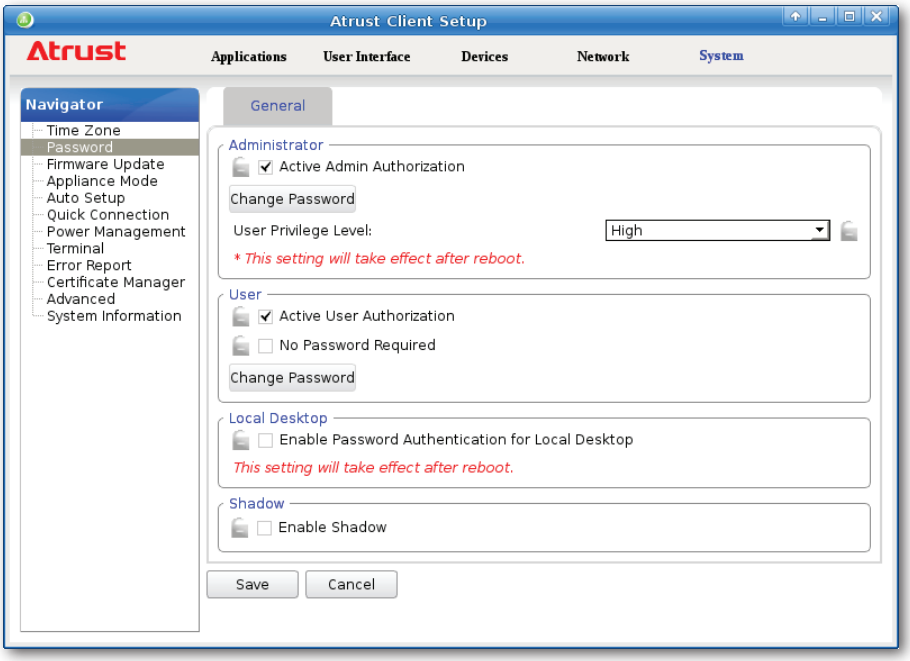
- The User section appears only when **Active Admin Authorization** is checked.

3. The access privileges for standard users are granted and a window appears for you to set the password.



4. Type in the desired password, and then click **OK** to confirm.

5. After the access privileges for standard users were granted, the **User Privilege Level** drop-down menu will appear in the Administrator section for you to set the privilege level for standard users. You can use this setting item to set the scope of settings available to a standard user.



NOTE

- You need to restart your system for the change to take effect.

User Privilege Level	Available Settings
High	Applications tab • Remote Desktop • Citrix ICA • VMware View • SSH • Web Browser • Parallels 2X Client User Interface tab • Display • Desktop • Keyboard • Mouse • Screensaver Devices tab • USB Storage • Audio • Printer Network tab • Ethernet • VPN • Hosts • Host Name • Wireless • Proxy System tab • Time Zone • Password • Firmware Update • Appliance Mode • Auto Setup • Quick Connection • Power Management • Terminal • Error Report • Certificate Manager • Advanced • System Information

Medium	User Interface tab • Display • Desktop • Keyboard • Mouse • Screensaver	Network tab • Ethernet • Wireless System tab • Time Zone • Password • Error Report
Low	User Interface tab • Display • Desktop • Keyboard • Mouse • Screensaver	System tab • Time Zone • Password • Error Report
None	System tab • Password • Error Report	

6. Additionally, **No Password Required** will appear in the User section to allow you to disable authentication for standard users.
7. After the configuration is done, click **Save** to store the changes.
8. Restart your system to apply the changes.

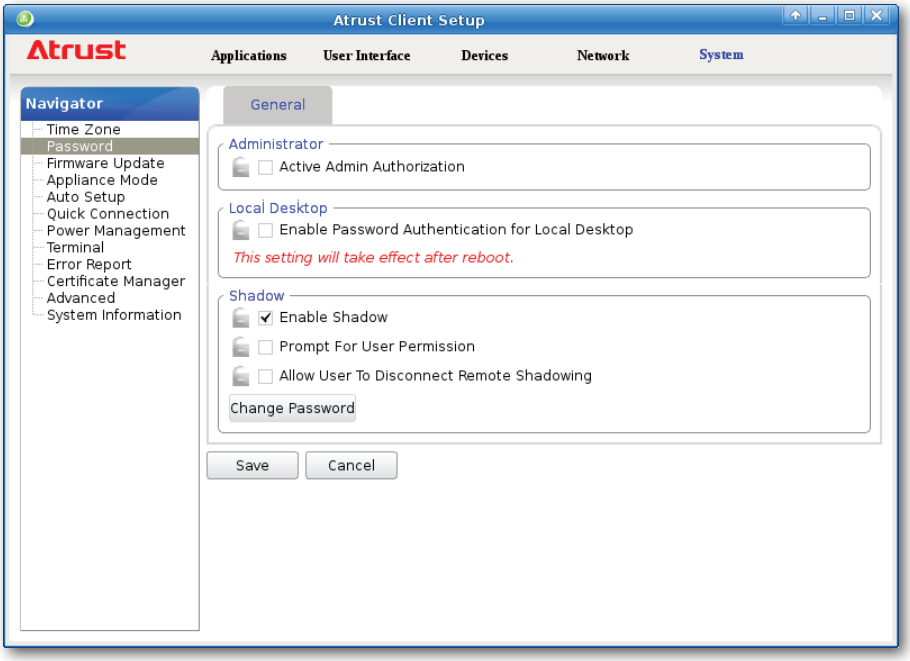
3.2.5 Configuring the Login Password for the Local Desktop

To enable and set the login password for the local desktop, please do the following:

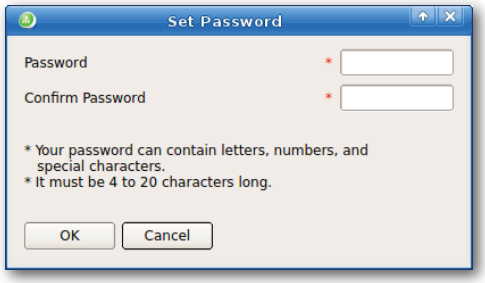
NOTE

- The default behavior is to enter the local desktop without any login password.

1. On Atrust Client Setup, click **System** > **Password**.



2. Under the Local Desktop section, click to check **Enable Password Authentication for Local Desktop**. A window appears for you to set the password.

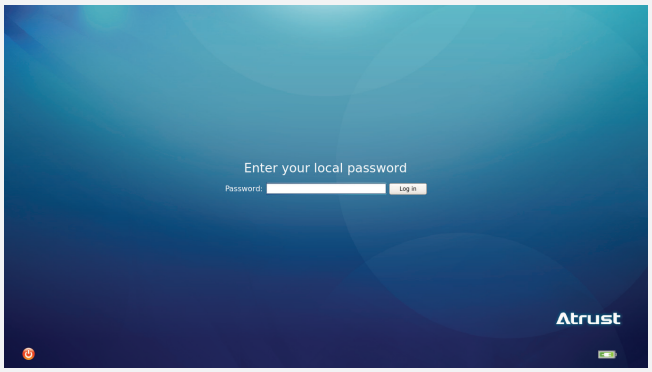


3. Type in the desired password, and then click **OK** to confirm.
4. Click **Save** to apply.

NOTE

- When this feature is enabled, each time when you start or restart your mt182L, you will be prompted to provide the Login password for the local desktop. The Login screen is shown as below.

Login Screen of Local Desktop



3.2.6 Configuring Shadow Settings for Remote Assistance

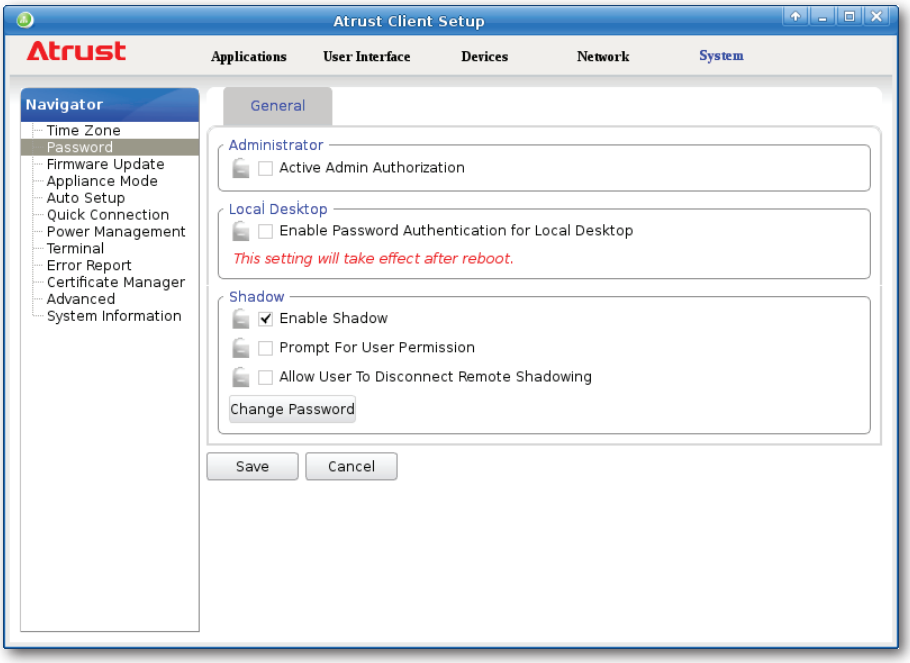
The Shadow feature allows an administrator to remotely assist client users in resolving problems or configuring local settings. When this feature is enabled, an administrator can monitor and control a client from a remote computer just like a local user.

NOTE

- To use the Shadow feature on a remote computer, you need to install the Atrust Device Manager console on that computer, and add your mt182L into a managed group under Atrust Device Manager. For details, please refer to the User's Manual for Atrust Device Manager.

To enable the Shadow feature and set the password for remote assistance, please do the following:

1. On Atrust Client Setup, click **System** > **Password**.



2. Under the Shadow section, click to check **Enable Shadow** if it's not checked.

NOTE

- By default, the Shadow feature is enabled. Click **Change Password**, and then follow the next step to set your password.

3. The Shadow feature is enabled and a window appears for you to set the password for remote assistance.

NOTE

- On a remote computer, an administrator will need this password to use the Shadow feature (remote assistance) with the Atrust Device Manager console. For more information, please refer to the User's Manual of Atrust Device Manager.

4. Type in the desired password, and then click **OK** to confirm.
5. To get user permission while shadowing, please check **Prompt for User Permission**.
6. To allow the user to stop remote shadowing, please check **Allow User to Disconnect Remote Shadowing**.
7. Click **Save** to save all the changes.

NOTE

- When the Shadow feature is performed from a remote Atrust Device Manager, on the target client, an icon appears on the Taskbar of the local Linux desktop and a notification pops up in the bottom-right corner. If you are under the Quick Connection mode, a notification would pop up in the bottom-right corner on Atrust Quick Connection screen.

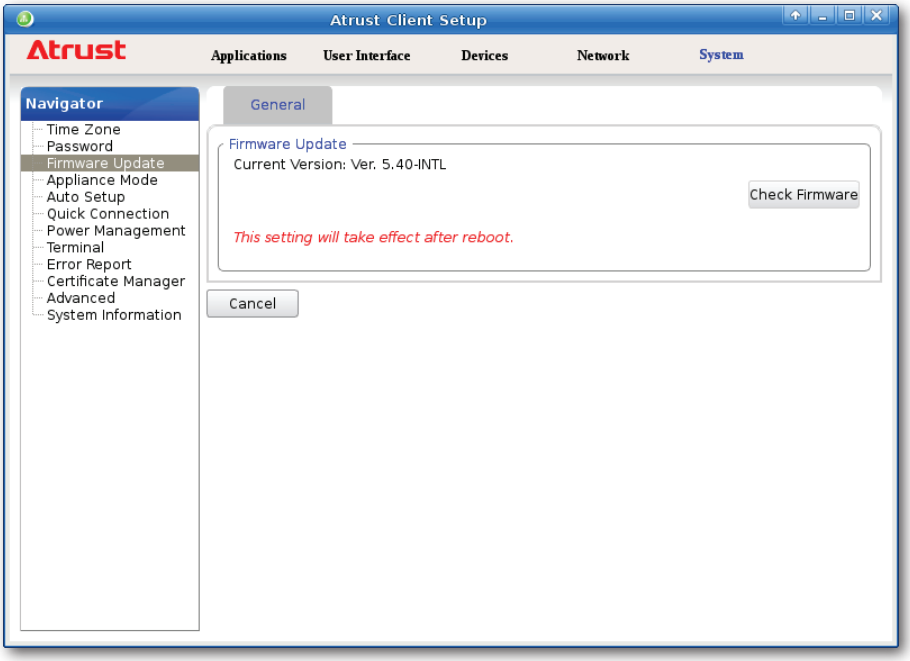
3.2.7 Updating Firmware from the Management Computer

Update Firmware allows client users to update firmware from its management computer.

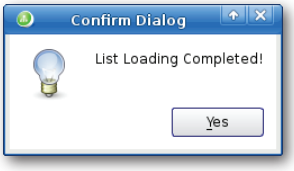
> **NOTE**
>
> - Ensure that your mt182L has been added into a managed group under Atrust Device Manager installed on a remote computer, and that you have imported client firmware files into Atrust Device Manager. These are prerequisites of this feature.
> - For more information on firmware update and Atrust Device Manager, please refer to the User Manual for Atrust Device Manager.

To update firmware from the management computer, please do the following:

1. On Atrust Client Setup, click **System** > **Firmware Update**.

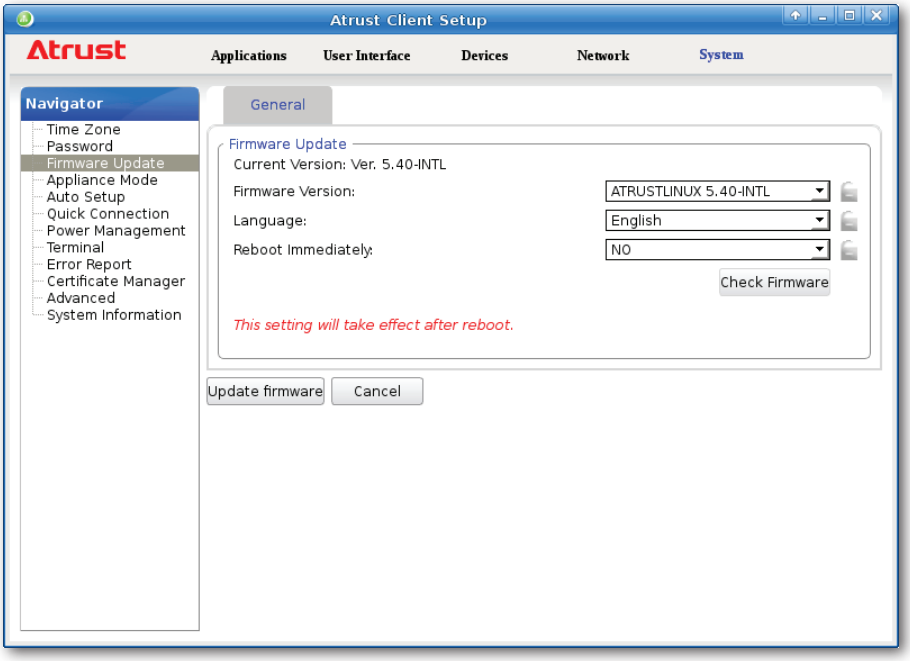


2. Under the Firmware Update section, click **Check Firmware**.
3. Upon completion, a window appears notifying you that the Firmware list has been loaded.



4. Click **Yes** to continue.

5. Click the drop-down menus to select the desired firmware version and other update options.



Firmware Update Options	
Item	**Description**
Firmware Version	Click to select the desired firmware version.
Language	Click to select the interface language of the system, including the Atrust Client Setup console. **NOTE:** Available languages may vary with the selected firmware version.
Reboot Immediately	Click to choose whether to restart the system immediately for firmware update or manually restart the system later.

6. Click **Update firmware** to confirm your selections. The system will start updating its firmware after restart.

3.2.8 Enabling or Disabling the Appliance Mode

The Appliance mode allows your mt182L to start up directly with the desired Microsoft Remote Desktop, Citrix ICA, VMware (Horizon) View, Web, or 2X session. Under this mode, users will feel as if they were using a standalone desktop computer; the underlying client operating system, Atrust Linux, is hidden from the very beginning.

NOTE

- There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: (n/a to Web browser) • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client
3	Quick Connection	The client will enter Atrust Quick Connection screen after system startup.

- For more information on these modes, please refer to sections:
  - ✧ 3.2.10 on page 62 and 2.1 on page 13 (Quick Connection mode)
  - ✧ 3.2.8 on page 58 (Appliance mode)
  - ✧ 3.6.5 on page 144 (Autostart mode for RDP sessions)
  - ✧ 3.6.11 on page 182 (Autostart mode for ICA sessions)
  - ✧ 3.6.14 on page 216 (Autostart mode for View sessions)
  - ✧ 3.6.19 on page 227 (Autostart mode for Web sessions)
  - ✧ 3.6.22 on page 235 (Autostart mode for 2X sessions)

Enabling the Appliance Mode

To enable the Appliance mode, please do the following:

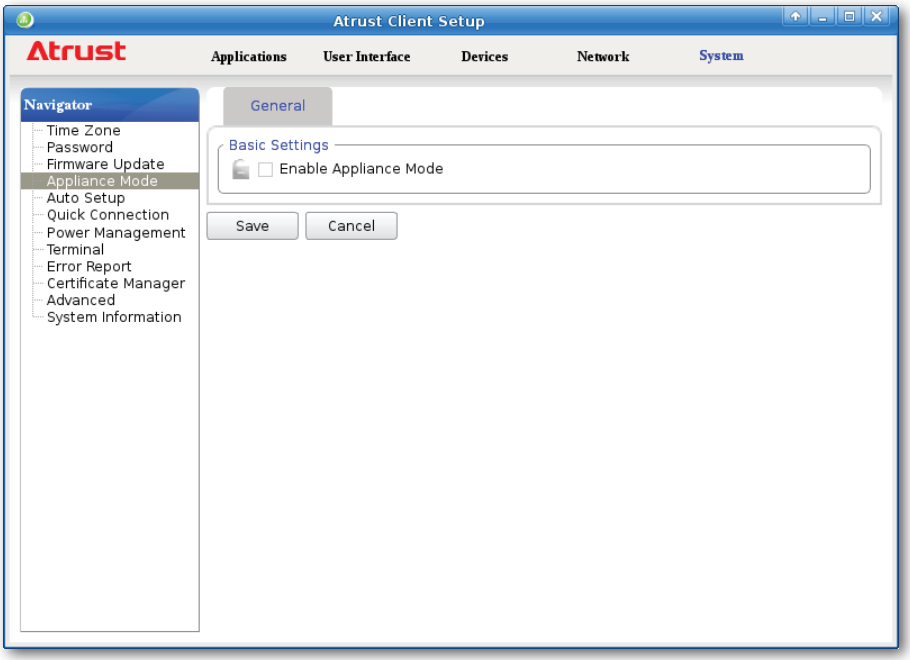
NOTE

- Ensure that you have configured the connection settings for the desired Microsoft Remote Desktop, Citrix ICA, VMware (Horizon) View, Web, or 2X session under **Applications** tab. You need to specify which service type and connection settings entry will be used under the Appliance mode. For detailed instructions, please see sections:
  - "3.6.3 Configuring Basic RDP Connection Settings" on page 129
  - "3.6.6 Configuring Basic ICA Connection Settings" on page 159
  - "3.6.12 Configuring Basic VMware View Connection Settings" on page 212
  - "3.6.17 Configuring Basic Settings for Browser Sessions" on page 224
  - "3.6.20 Configuring Basic RAS / RDP Connection Settings" on page 228

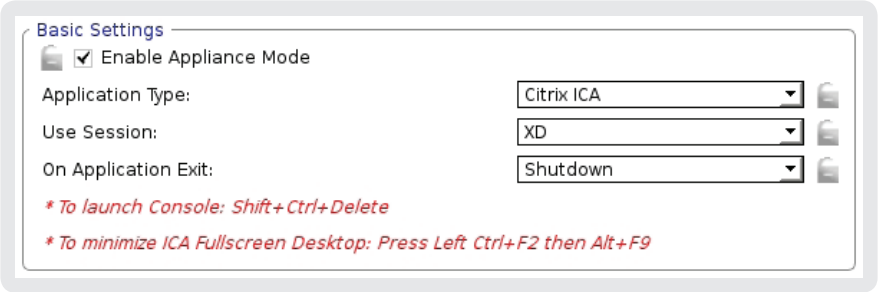
NOTE

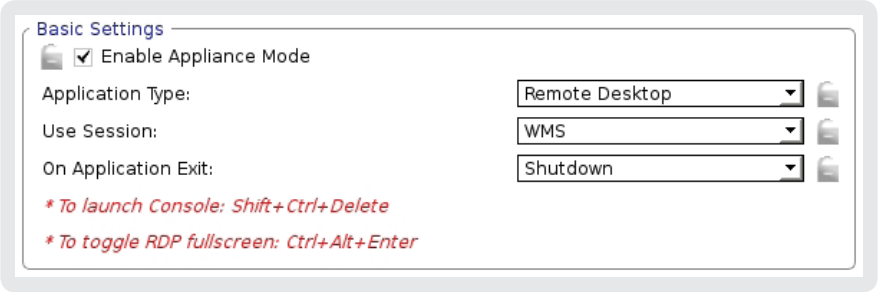
- Please note that the Autostart mode also enables the client to start up directly with an RDP / ICA / View session and provides more configuration flexibility than the Appliance mode. For detailed information on the Autostart mode, please refer to the following sections:
  - "3.6.5 Configuring Advanced RDP Connection Settings" on page 144
  - "3.6.11 Configuring Advanced ICA Connection Settings" on page 182
  - "3.6.14 Configuring Advanced View Connection Settings" on page 216
  - "3.6.19 Configuring Advanced Settings for Browser Sessions" on page 227
  - "3.6.22 Configuring Advanced RAS / RDP Connection Settings" on page 235

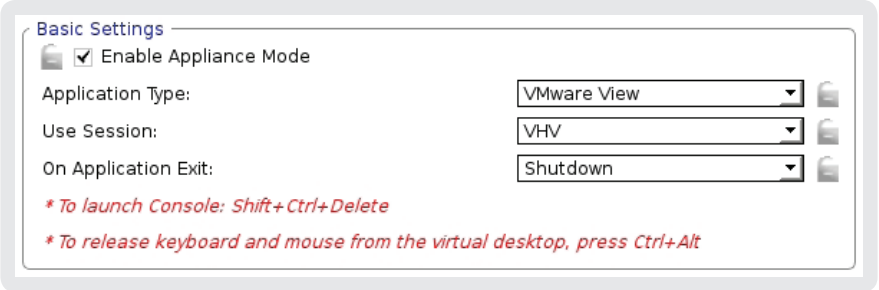
1. On Atrust Client Setup, click **System** > **Appliance Mode**.

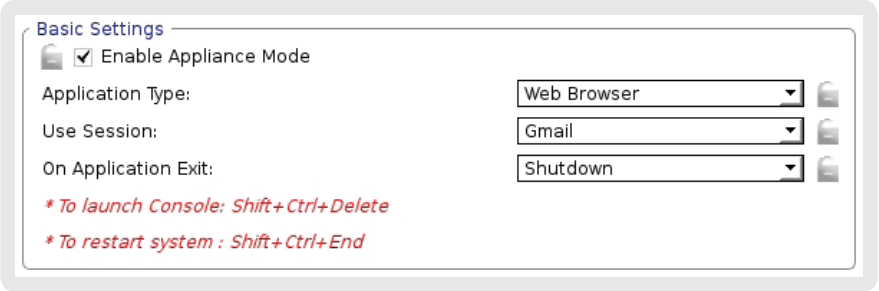


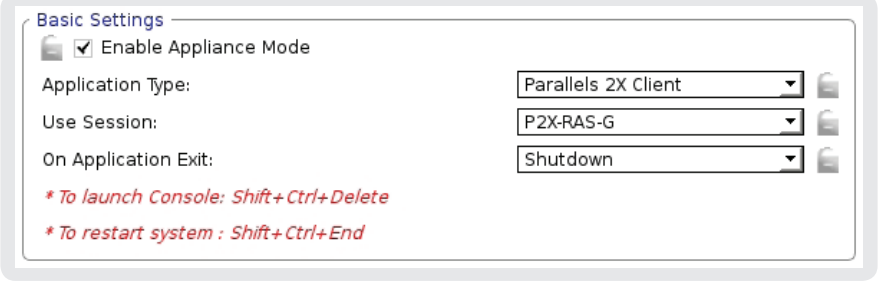
2. Click to check **Enable Appliance Mode**.
3. Other settings of the Appliance mode appear. Click drop-down menus to select the application (or service) type: **Citrix ICA**, **Remote Desktop**, **VMware View**, **Web Browser**, or **Parallels 2X Client**, the specific service available in that type, and the desired action after exiting a session.











NOTE

- No matter which Resolution option you choose for the selected RDP / ICA / View service, RDP / ICA / View sessions under the Appliance mode will always use the Full Screen mode to display the remote/virtual desktop.

4. Click **Save** to confirm your selections.
5. The system will enter the Appliance mode after restart.

NOTE

- To disable the Appliance mode or to access Atrust Client Setup under the Appliance mode, please refer to "Disabling the Appliance Mode" on page 61.

Disabling the Appliance Mode

To disable the Appliance mode, please do the following:

1. Under the Appliance mode, exit the Full Screen mode of the RDP / ICA / 2X session, minimize the Web browser window, or release the keyboard and mouse from the View session (virtual desktop):

   - To exit the Full Screen mode of the RDP session, press **Ctrl + Alt + Enter**, and then minimize the session window.
   - To exit the Full Screen mode of the ICA session, press **Ctrl + F2**, and then **Alt + F9**.
   - To exit the Full Screen mode of the 2X session, log out from the remote desktop.
   - To release the keyboard and mouse from the View session (virtual desktop), press **Ctrl + Alt**.

NOTE

- Please note that the View session (virtual desktop) will remain on the background after you release the keyboard and mouse from the View session (virtual desktop).

2. Click **Ctrl + Shift + Del** to launch Atrust Client Setup.

NOTE

- You cannot access the Taskbar of the client operating system (Atrust Linux) under the Appliance mode.

3. On Atrust Client Setup, click **System** > **Appliance Mode**.
4. Click to uncheck **Enable Appliance Mode**, and then click **Save** to apply the change.
5. Return to the current RDP / ICA / View / Web / 2X session:

   - To return to the current RDP / ICA / Web / 2X session, use **Alt + Tab** (press and hold **Alt**, and then press **Tab** to switch between different items) to select and restore the current session.

- To return to the current View session, click any place of the View session (virtual desktop) on the background.

6. End or log off from the current RDP / ICA / View / Web / 2X session.
7. The client might shut down then. Restart your client manually.

3.2.9 Enabling or Disabling Auto Setup

Auto Setup allows your thin client to get its preset configurations on startup and enter the desired user environment automatically. Its operation requires Auto Setup environment and network connectivity, except for Auto Setup on the client side. For details, please refer to "A.4 Auto Setup Flowchart" on page 259 and User's Guide for Auto Setup.

NOTE

- To disable Auto Setup after your thin client got its preset configurations, reset your client. Please refer to "A.1 Resetting Your mt182L to the Factory Default" on page 249.

3.2.10 Configuring the Quick Connection Mode

The Quick Connection mode enables you to enter the Atrust Quick Connection screen after system startup. This setting is disabled by default for mobile thin clients.

NOTE

- For detailed instructions on how to use your mt182L under the Quick Connection mode, please refer to section "2.1 Learning the Basics" on page 13.
- There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

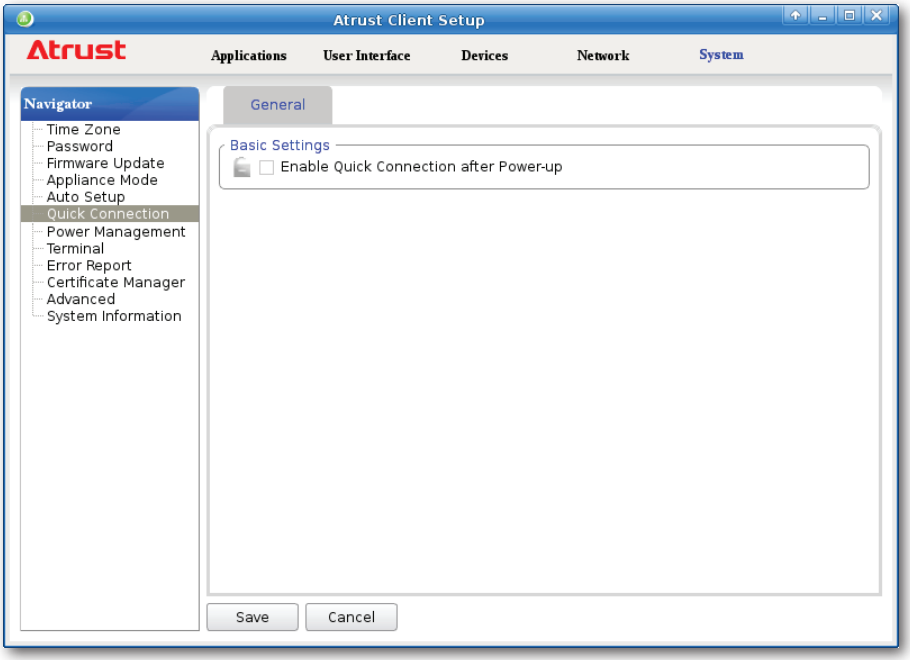
No.	Mode	Description
1	Appliance	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session. Available actions include: (n/a to Web browser) • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client
3	Quick Connection	The client will enter Atrust Quick Connection screen after system startup.

NOTE

- To use the Quick Connection mode, ensure that both the Appliance and Autostart modes are disabled. If either of two modes are enabled, the Quick Connection mode will fail to work.
- For more information on the Appliance mode, please refer to section "3.2.8 Enabling or Disabling the Appliance Mode" on page 58.
- For more information on the Autostart mode, please refer to the following sections:
  - "3.6.5 Configuring Advanced RDP Connection Settings" on page 144
  - "3.6.11 Configuring Advanced ICA Connection Settings" on page 182
  - "3.6.14 Configuring Advanced View Connection Settings" on page 216
  - "3.6.19 Configuring Advanced Settings for Browser Sessions" on page 227
  - "3.6.22 Configuring Advanced RAS / RDP Connection Settings" on page 235

To enable/disable the Quick Connection mode, please do the following:

1. On Atrust Client Setup, click **System** > **Quick Connection**.



2. Click to check/uncheck **Enable Quick Connection after Power-up** to enable/disable the Quick Connection mode, and then click **Save** to apply the changes.

NOTE

- For advanced Quick Connection settings, please refer to the next section (3.2.11).

3.2.11 Configuring Advanced Quick Connection Settings

You are allowed to configure advanced Quick Connection settings for Remote Desktop, Citrix ICA, and VMware View sessions through **System** > **Quick Connections** on Atrust Client Setup.

Advanced Quick Connection Settings for Remote Desktop Sessions

To configure advanced Quick Connection settings for Remote Desktop sessions, please refer to the table below:

Remote Desktop Option	
Item	**Description**
Multimedia Redirection	Check/Uncheck to enable/disable multimedia redirection. When enabled, the client receives original compressed multimedia streams and decodes locally for display. This feature increases the load on the client, but saves server resources, decreases the bandwidth usage, and improves audio and video playback experiences. It's enabled by default (when Quick Connection mode is enabled).

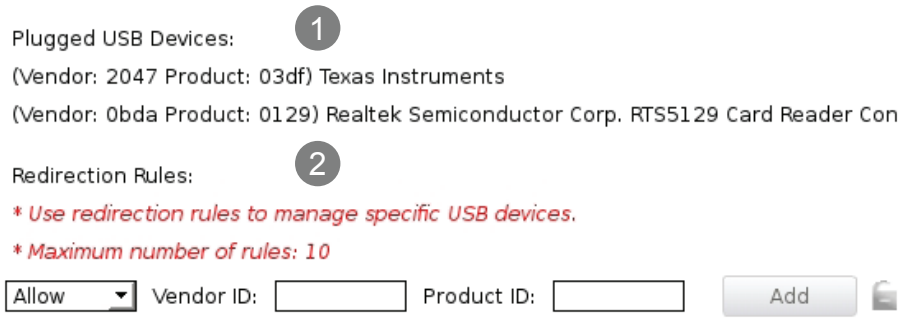
Advanced Quick Connection Settings for Citrix ICA Sessions

To configure advanced Quick Connection settings for Citrix ICA sessions, please refer to the tables below:

Citrix ICA Option	
Item	**Description**
Default Server Address	To provide a default server address, type in the desired address in this field.
Connect to the Default Server Directly	Check to connect to the default sever directly.
Client Rendering	Check/Uncheck to enable/disable client rendering. When **Client Rendering** is disabled, **Server Rendering** is used.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Check to enable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.

Citrix ICA Option	
Item	**Description**
Redirect Connected USB Devices	Check to enable redirection for connected USB devices in Quick Connection mode. All connected USB devices will be redirected unless more specific settings are specified below.

Citrix ICA Option	
Item	**Description**
Use of USB Storage Devices	Click to select how to use USB storage devices in ICA sessions. Three options are available: **Mapping**, **Redirection**, and **Disabled**.
Use of USB Printers	Click to select how to use USB printers in ICA sessions. Three options are available: **Mapping**, **Redirection**, and **Disabled**.



Citrix ICA Option	
Item	**Description**
Redirection Rules	Create redirection rules on 2 to manage specific USB devices with information on 1.

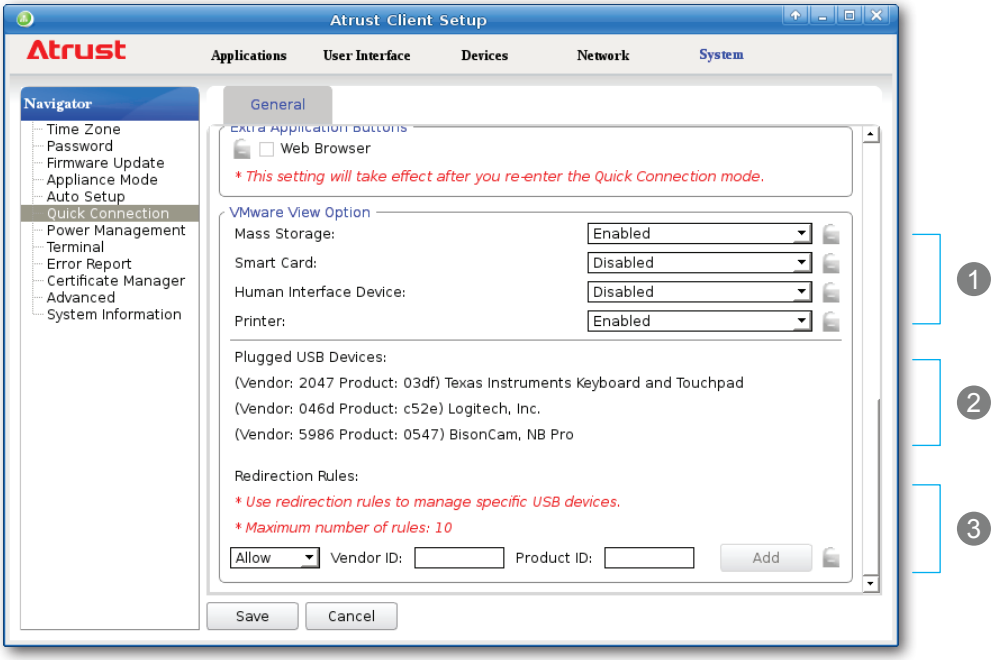
NOTE

- All attached USB devices will be listed under ***Plugged USB Devices*** (1) with vender and product information needed for creating rules.

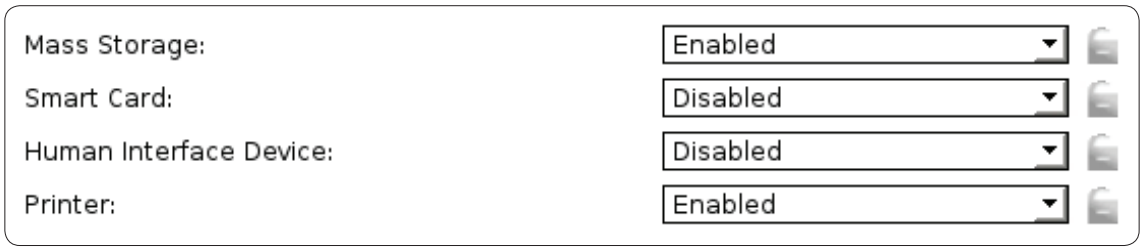
Advanced Quick Connection Settings for VMware View Sessions

To configure advanced Quick Connection settings for VMware View sessions, please do the following:

1. On Atrust Client Setup, click **System** > **Quick Connection**.



2. Click drop-down menus to configure ***Generic Settings*** (1) for mass storage devices, smart cards, and human interface devices. Two options are available: **Enabled** or **Disabled**.



3. Use ***Redirection Rules*** (3) to manage specific USB devices:

- Refer to (2) to fill in the Vender and Product IDs for a specific device, click the drop-down menu to select **Allow** or **Deny**.
- Click **Add** on the right to add a rule on (3).

NOTE

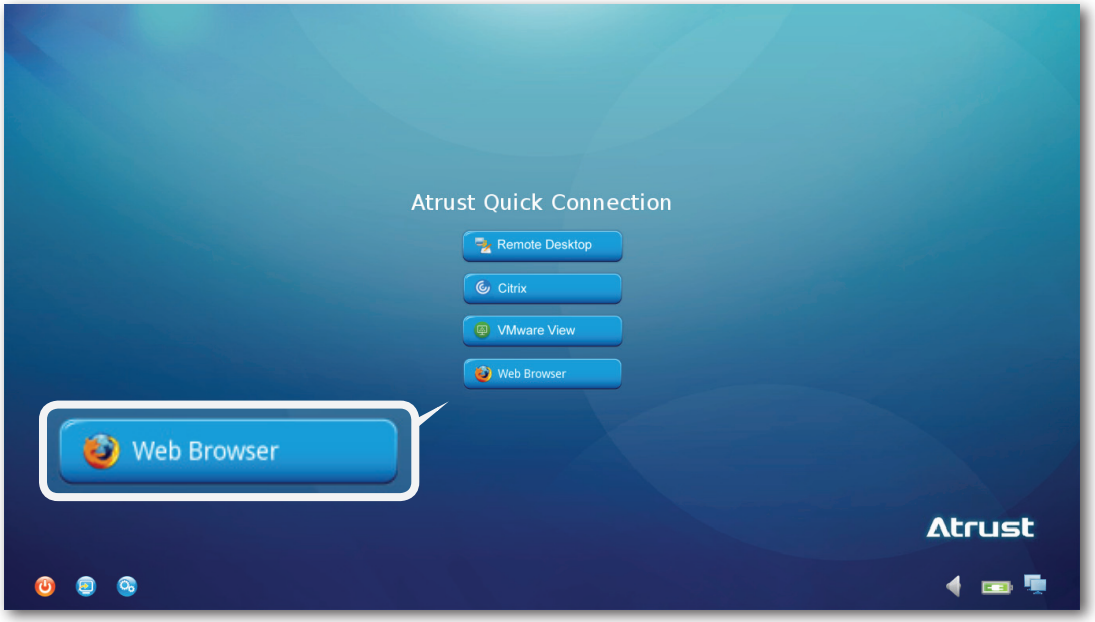
- All attached USB devices will be listed under ***Plugged USB Devices*** (2) with vender and product information needed for creating rules.
- ***Redirection Rules*** (3) have priority over ***Generic Settings*** (1).

4. Click **Save** to apply.

Accessing the Internet Locally in Quick Connection Mode

To access the Internet locally in Quick Connection mode, you can configure to show the Web Browser button on Atrust Quick Connection screen:

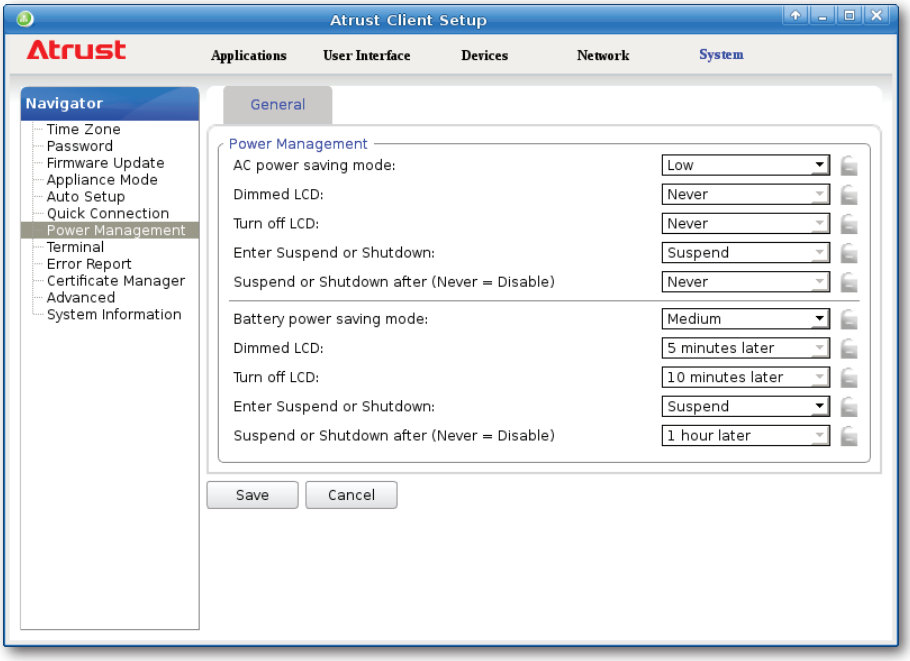
Atrust Quick Connection Screen



3.2.12 Managing the Use of Power

To manage the use of power for your mobile thin client, please do the following:

1. On Atrust Client Setup, click **System** > **Power Management**.



2. Choose the desired power-saving mode for your AC power and battery, or choose **Custom** to customize individual settings, and then click **Save** to apply.

NOTE

- When your mt182L enters ***System Sleep mode*** manually (**Fn** + **F12** or > **Suspend**) or automatically (configured in Atrust Client Setup through **System** > **Power Management**), it still requires a certain amount of power. You can use **Shut down** option instead to save the power to a greater degree.

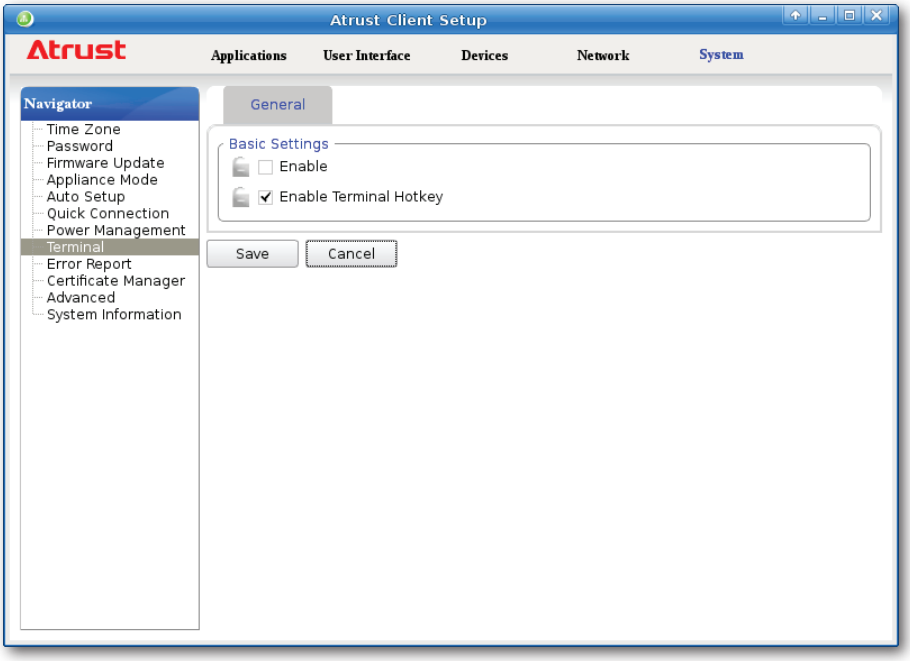
WARNING

- When using only the battery as the power source, ensure that it has enough power to prevent data loss.

3.2.13 Enabling or Disabling the Command-line Functions

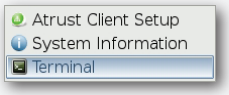
To enable/disable the execution of the text-based (command-line) functions, please do the following:

1. On Atrust Client Setup, click **System** > **Terminal**.



2. Click to configure your settings:

   - To allow the execution of command-line functions via a shortcut on Start menu, check **Enable**.
   - To allow the execution of command-line functions via a hotkey, check **Enable Terminal Hotkey**.
   - To completely disable **Terminal**, uncheck both.

> **NOTE**
>
> - To open **Terminal** via the shortcut, click **START** > **Settings** > **Terminal** on the local Linux desktop.
>
> 
>
>
> - To open **Terminal** via the hotkey, press **Ctrl** + **Alt** + **T**.

3. Click **Save** to apply your change.

3.2.14 Collecting Event Logs and Capturing Related Screens

The **Error Report** feature allows you to collect event logs and capture related screens for error reporting.

Collecting Event Logs

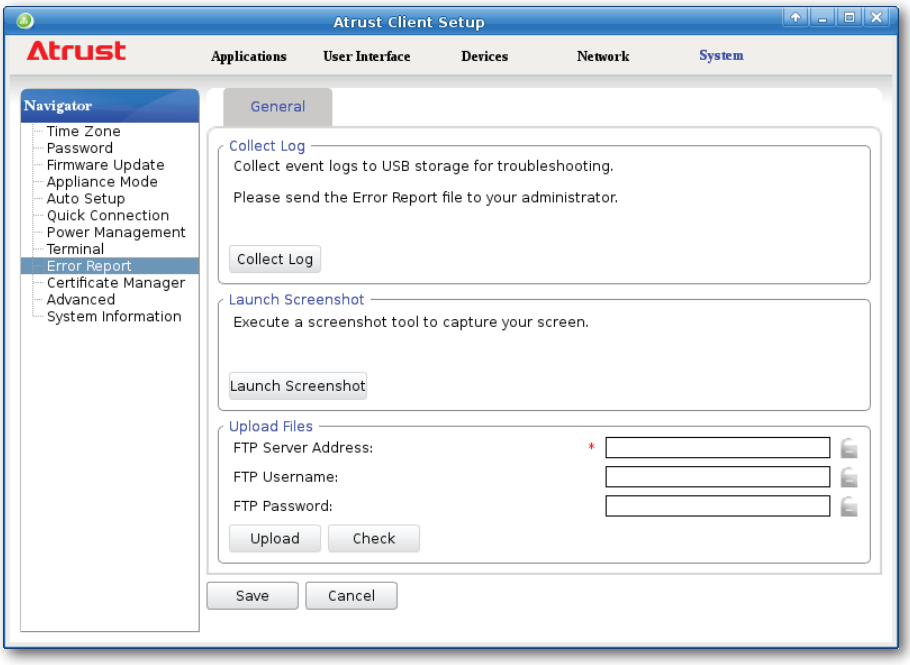
To collect event logs of your mt182L, please do the following:

1. Plug a USB flash drive into your mt182L.

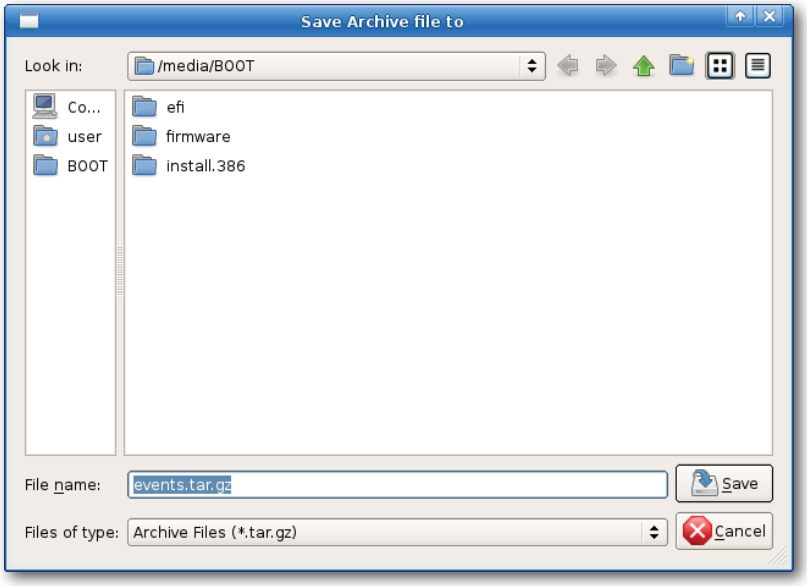
> **NOTE**
>
> - This USB flash drive will be used for storing the event logs of your mt182L.
> - Ensure that you have enabled the access and automount of USB storage devices. For detailed instructions, please refer to section "3.4.3 Configuring Settings for USB Storage Devices" on page 94.

> **NOTE**
>
> - Please note that files saved on the local desktop will be deleted after restart.

2. On **Atrust Client Setup**, click **System** > **Error Report**.



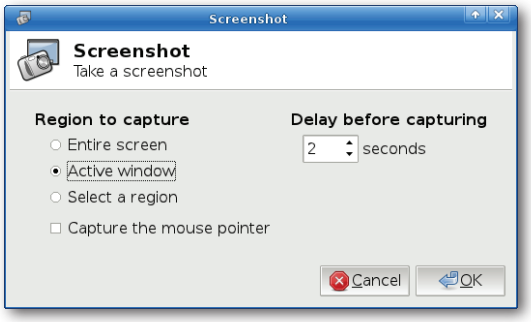
3. Click **Collect Log**. A window appears prompting you to choose where to save the log file set (named **events.tar.gz**). The attached USB flash drive is the default location if attached. Click **Save** to apply.



Capturing Error-Related Screens

To capture error-related screens of your mt182L, please do the following:

1. On Atrust Client Setup, click **System** > **Error Report**.
2. Click **Launch Snapshot** to open the screen capturing program.



3. Configure screen capturing settings directly on the opened window if needed, and then click **OK** to capture the desired screen.

TIP

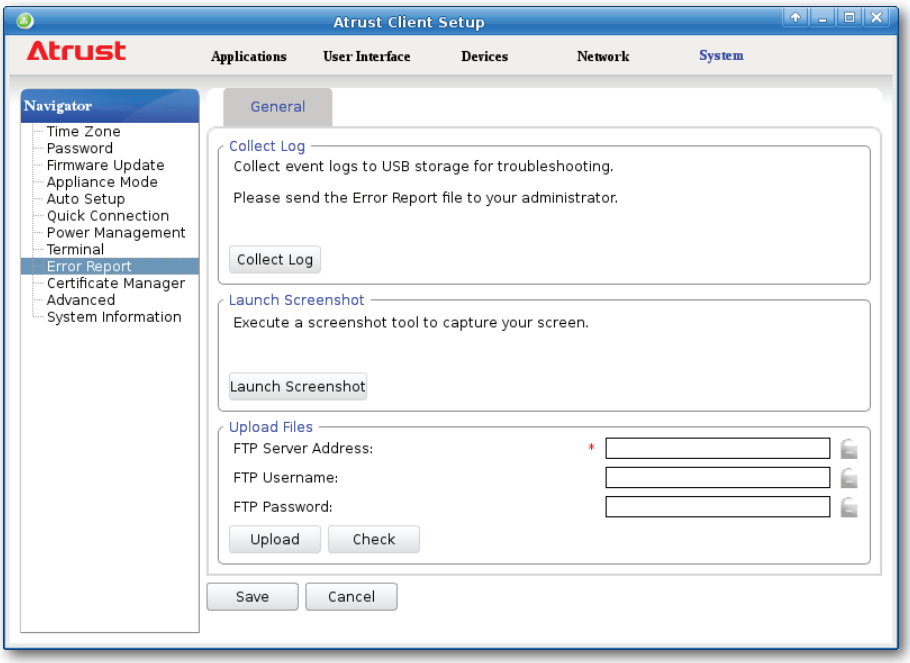
- It's recommended to set the delay time before capturing to at least 2 seconds to reserve time for switching to the desired screen or window.
- It's recommended to save the captured screens in the same USB flash drive where the event logs were saved.
- Please note that files saved on the local desktop will be deleted after restart.

3.2.15 Uploading Files for Error Reporting

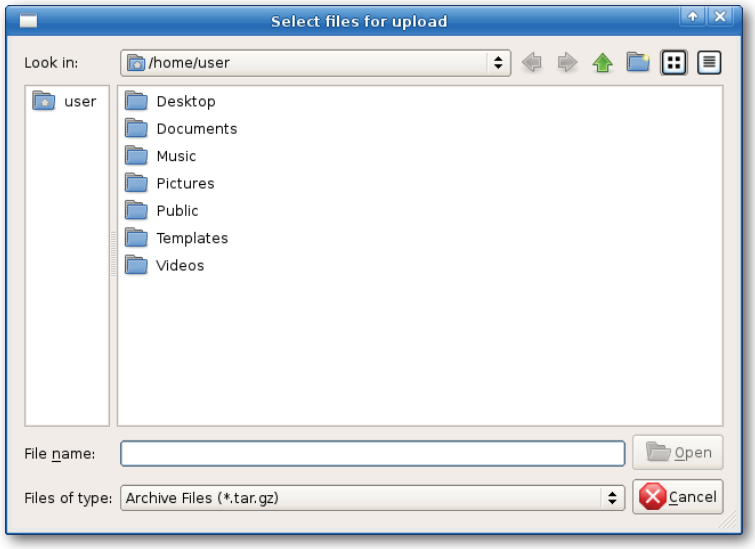
You can upload files to a specified FTP server for error reporting.

To upload files to an FTP server, please do the following:

1. On Atrust Client Setup, click **System** > **Error Report**.



2. Under the Upload Files section, type the IP address of the FTP server and credentials, click **Upload** to select and upload files to that FTP server.



TIP

- You can check the validity of the IP address and credentials first through the **Check** button.

3.2.16 Importing Certificates for Remote Computers

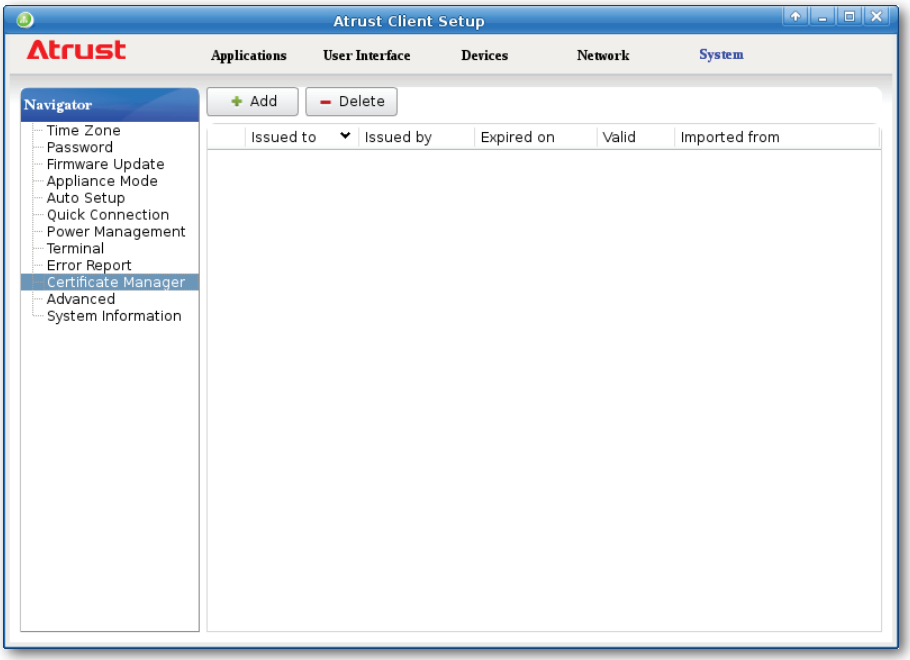
You can import certificates for remote computers through:

- A local device (from a USB storage device)
- The network (from a remote computer or the management console)

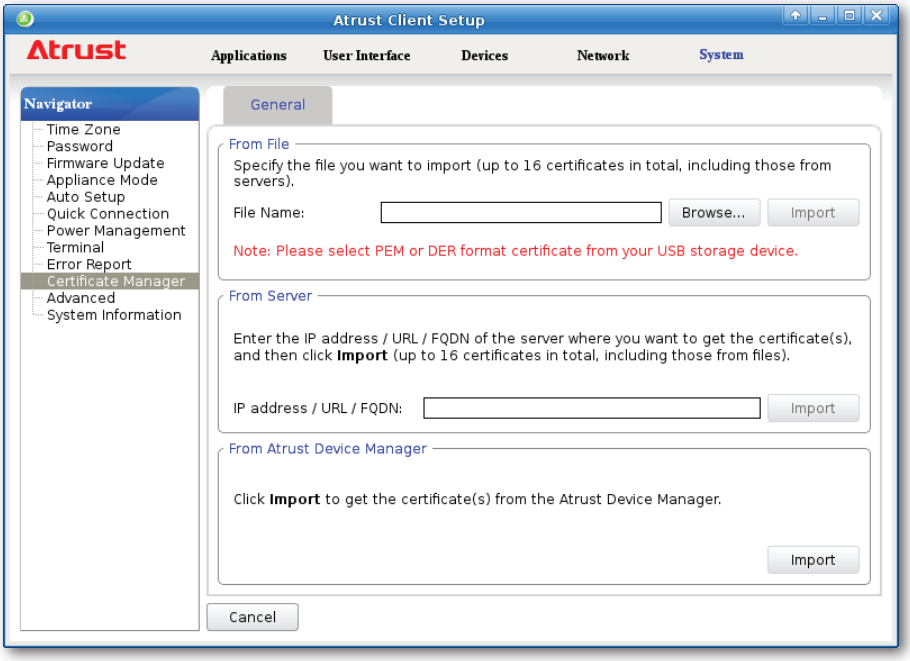
> **NOTE**
>
> - The available management console for mt182L is Atrust Device Manager, a remote and group management console for multiple thin clients. For more information, please refer to the User's Manual for Atrust Device Manager.

Importing certificates through a USB storage device
To import certificates for remote computers through a USB storage device, please do the following:

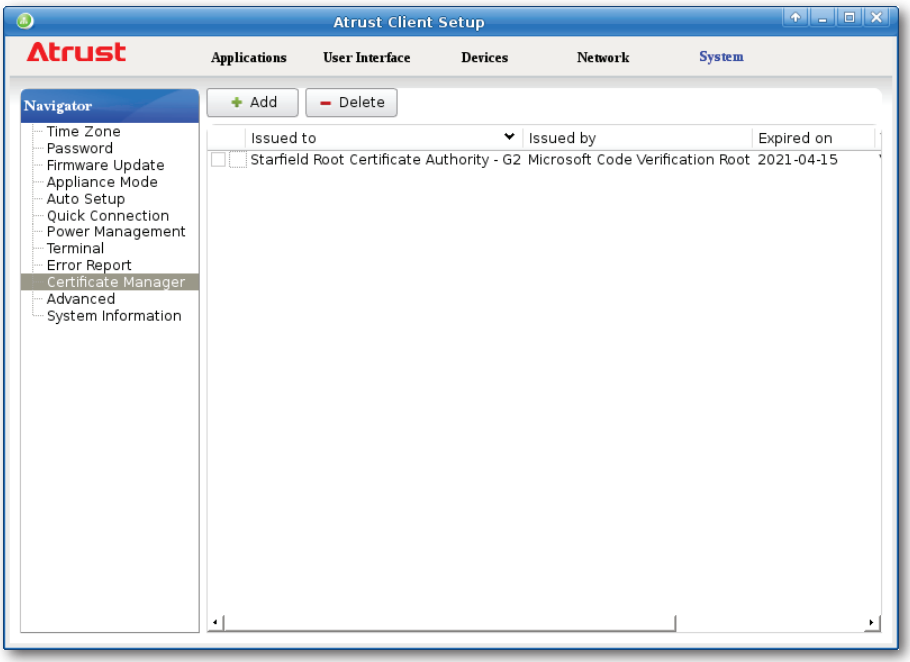
1. Copy your certificates to a USB storage device, and then connect this storage device to your mt182L.
2. On Atrust Client Setup, click **System** > **Certificate Manager**.
3. Click **Add** on the top of the Certificate list.



4. In the From File section, click **Browse** to locate the desired certificate file, and then click **Open** to confirm.

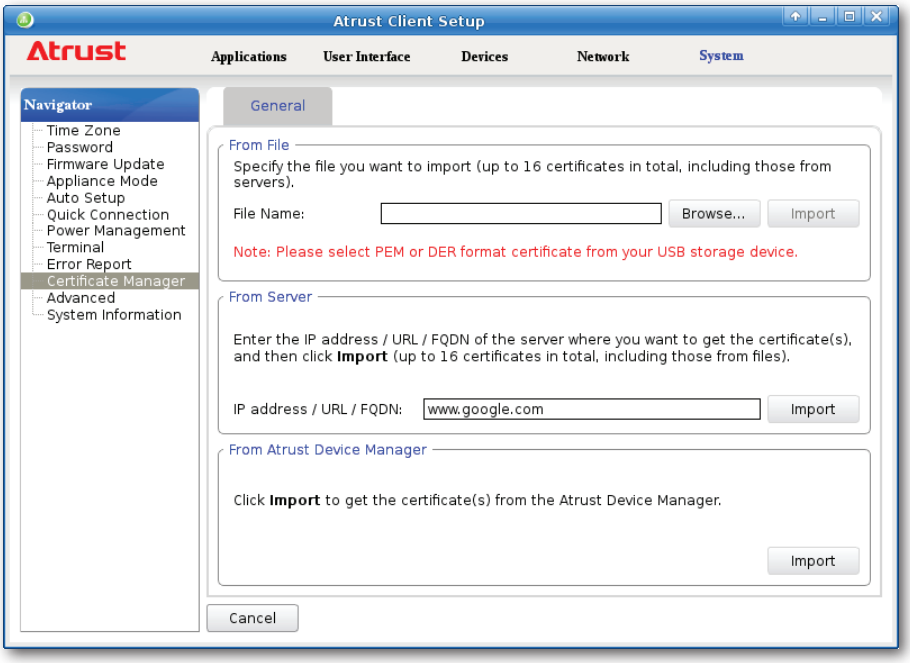


5. Click **Import** to start importing the certificate.
6. On completion, the certificate is shown in the Certificate list.

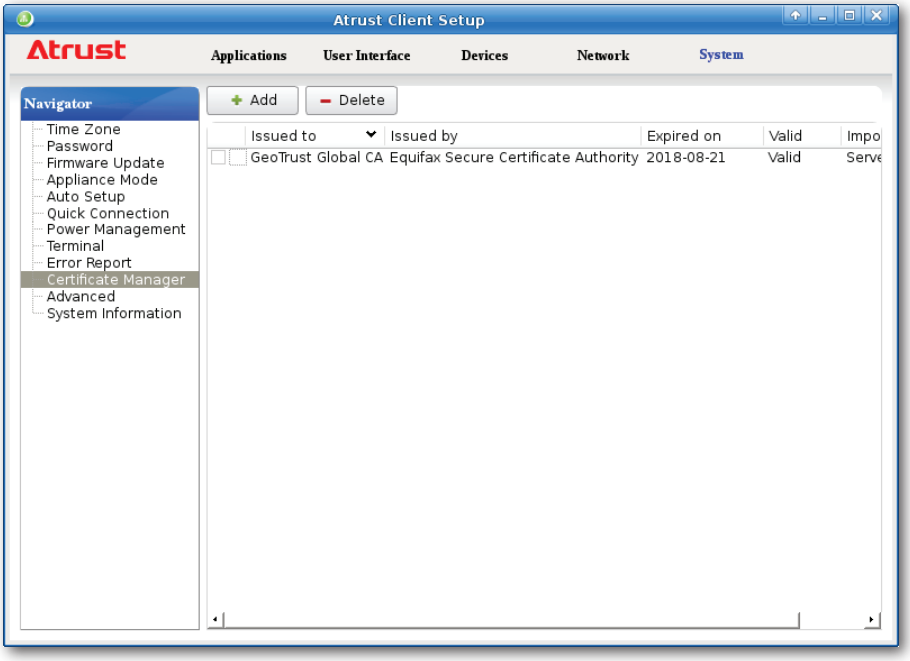


Importing certificates from remote computers through the network
To import the certificate from a remote computer through the network, please do the following:

1. On Atrust Client Setup, click **System** > **Certificate Manager**.
2. Click **Add** on the top of the Certificate list.
3. In the From Server section, type the IP address / URL / FQDN of the remote computer, and then click **Import**.



4. On completion, the certificate is shown in the Certificate list.

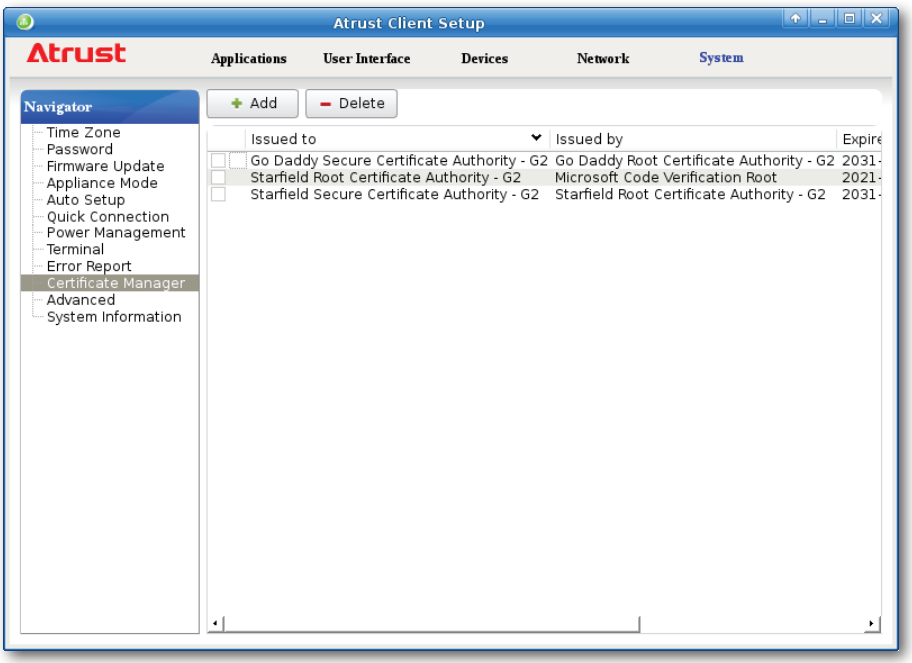


Importing certificates from Atrust Device Manager through the network

To import certificates from Atrust Device Manager through the network, please do the following:

> **NOTE**
>
> - Before proceeding, ensure that (1) your thin client has been added into a managed group in the management console, that is, Atrust Device Manager, and that (2) you have imported certificates into the management console.

1. On Atrust Client Setup, click **System** > **Certificate Manager**.
2. Click **Add** on the top of the Certificate list.
3. In the From Atrust Device Manager section, click **Import** to start importing all certificates available in Atrust Device Manager.
4. On completion, the certificates are shown in the Certificate list.



3.2.17 Enabling or Disabling Auto Registration

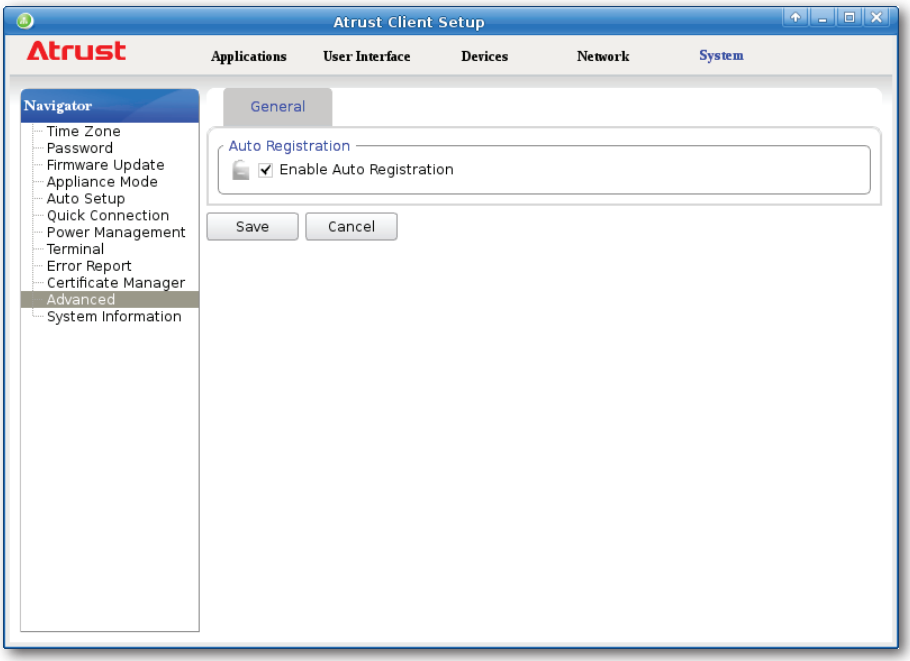
Auto Registration allows that thin clients automatically register with Atrust Device Manager when they are online and then become managed by Atrust Device Manager.

NOTE

- For this feature to work, Auto Registration must be enabled on both sides: thin clients and target Atrust Device Manager. In addition, some configurations on DHCP or DNS server over your network are required. For details, please refer to the User's Manual for Atrust Device Manager.
- By default, Auto Registration is enabled on thin client side, disabled Atrust Device Manger.

To enable or disable Auto Registration on your thin client, please do the following:

1. On Atrust Client Setup, click **System** > **Advanced**.
2. Check / Uncheck to **Enable Auto Registration** to enable / disable Auto Registration.



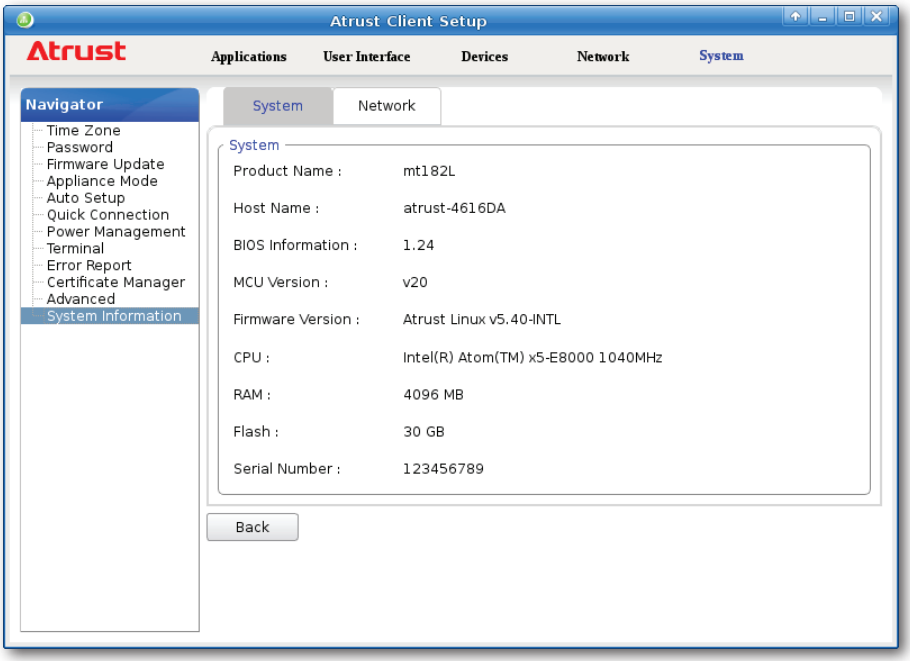
3. Click **Save** to apply.

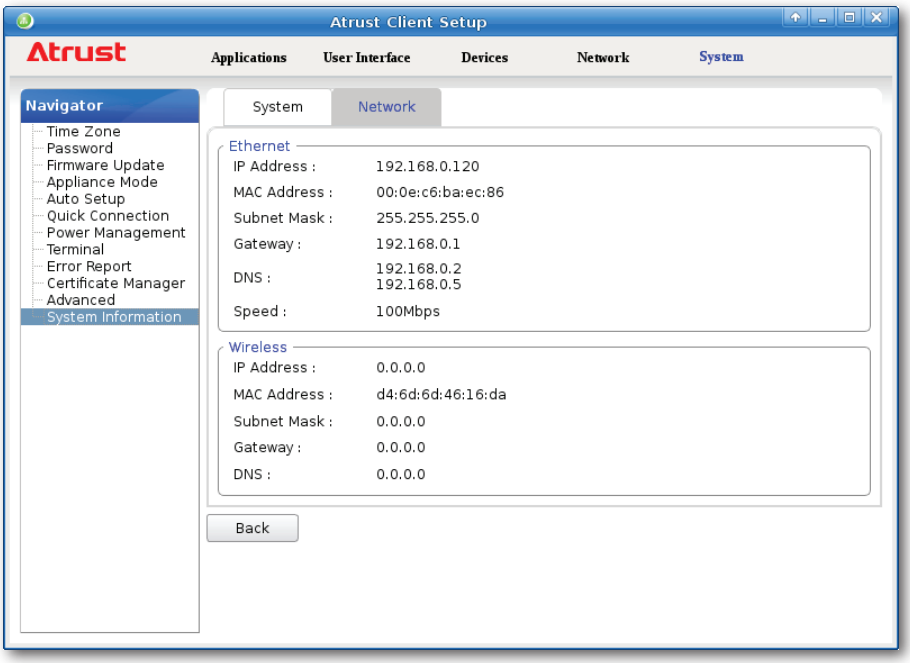
3.2.18 Viewing System and Network Information

You can view detailed system and network information through Atrust Client Setup.

To view detailed system and network information through Atrust Client Setup, please do the following:

1. On Atrust Client Setup, click **System** > **System Information**.
2. Click **System** / **Network** tab to view system / network information.



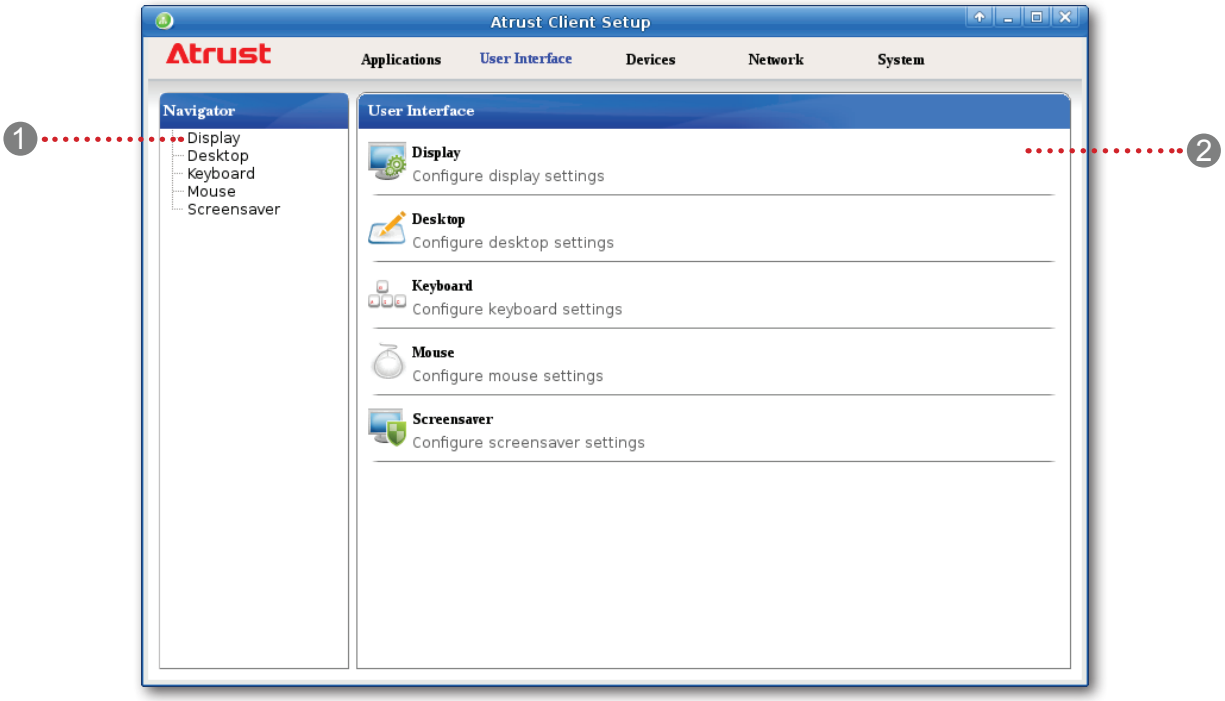


3.3 Configuring User Interface Settings

3.3.1 User Interface Tab Overview

User Interface tab enables you to configure settings for the user interface of clients. To access available settings of **User Interface** tab, click the tab on Atrust Client Setup.

User Interface Tab Overview



Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **User Interface** tab.
2	Configuration area	Configures setting values when a setting item or entry is selected.

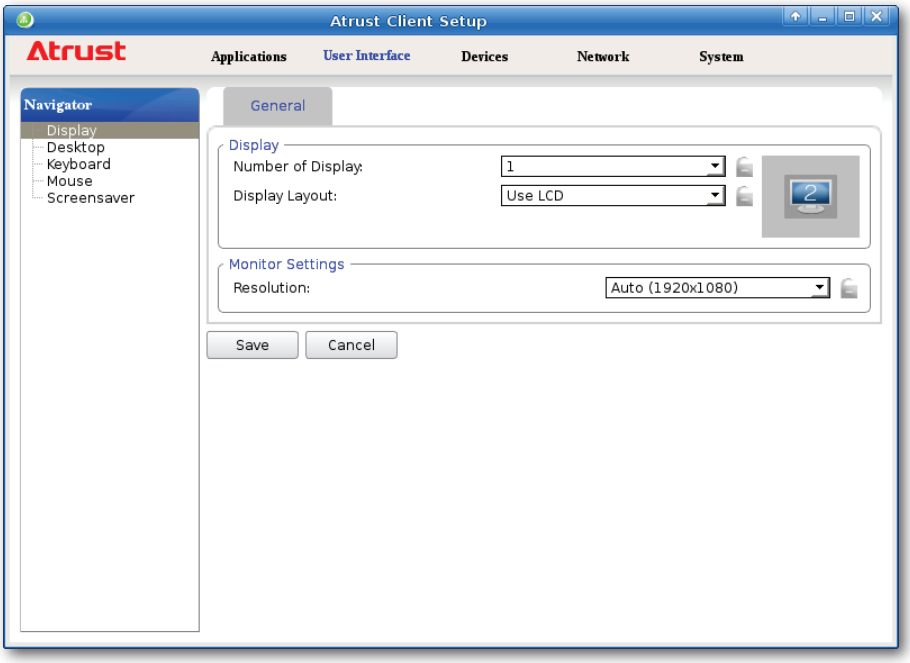
3.3.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
User Interface	Display		Click to configure display settings.	3.3.3	80
	Desktop		Click to customize desktop and system language.	3.3.4 3.3.5 3.3.6	83 86 87
	Keyboard		Click to adjust keyboard settings.	3.3.7	88
	Mouse		Click to adjust mouse settings.	3.3.8	90
	Screensaver		Click to configure screensaver settings.	3.3.9	91

3.3.3 Configuring Display Settings

To configure display settings for your mt182L, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Display**.



2. Click drop-down menus to select the number of attached display(s), arrangement of displays, resolution, etc. Refer to the following table to select appropriate setting values.

NOTE

- The available setting items vary, depending on your model and the selected number of display(s).

<table>
<tr><th colspan="2">Display</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Number of Display</td><td>Click to select the number of used display(s).
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>1</td><td>One display is used.</td></tr>
<tr><td>2</td><td>Two displays are used.</td></tr>
</table></td></tr>
<tr><td>Display Layout</td><td>Click to select the arrangement of displays.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Use External</td><td>Use the single external display attached.</td></tr>
<tr><td>Use LCD</td><td>Use the single internal display (LCD panel).</td></tr>
<tr><td>External - LCD horizontal</td><td>Use dual displays.
Two displays are arranged horizontally:
the external one is on the left; the LCD the right.
The external one is the main display for local desktop when Extend is selected.</td></tr>
<tr><td>LCD - External horizontal</td><td>Use dual displays.
Two displays are arranged horizontally:
the LCD one is on the left; the external the right.
The LCD one is the main display for local desktop when Extend is selected.</td></tr>
<tr><td>External - LCD vertical</td><td>Use dual displays.
Two displays are arranged vertically:
the external one is on the top; the LCD the bottom.
The external one is the main display for local desktop when Extend is selected.</td></tr>
<tr><td>LCD - External vertical</td><td>Use dual displays.
Two displays are arranged vertically:
the LCD one is on the top; the external the bottom.
The LCD one is the main display for local desktop when Extend is selected.</td></tr>
</table></td></tr>
<tr><td>Display Mode</td><td>This item is available only when 2 is selected in the Number of Display drop-down menu:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Extend</td><td>One display is used as the extended display of the other.</td></tr>
<tr><td>Clone</td><td>Two displays have the same display content.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="2">Monitor Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Enable Auto-Detection at Power-up</td><td>Check/Uncheck to enable/disable the automatic detection of the used monitor(s) when the client is powered on.

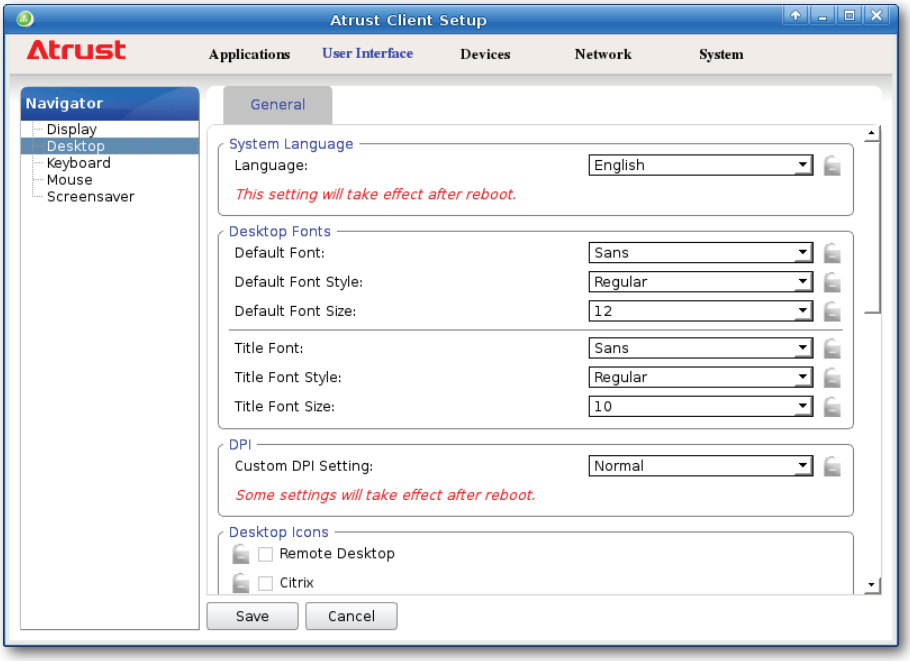
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Enabled</td><td>Automatic detection of the used monitor(s) is enabled. The system would set an appropriate resolution for the used monitor(s) when the client is powered on.</td></tr><tr><td>Disabled</td><td>Automatic detection of the used monitor(s) is disabled. All resolutions supported by the client will be listed in the Resolution drop-down menu when Auto-Detection at Power-up is disabled. Please note that some resolutions may not be applicable to your monitor(s).</td></tr></table></td></tr>
<tr><td>Monitor Resolution</td><td>Use this item to set an appropriate resolution for the used display.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Auto</td><td>This option is available only when Enable Auto-Detection at Power-up is selected.</td></tr><tr><td>Other options</td><td>Select the desired resolution from the Resolution drop-down menu for the used display.</td></tr></table>
NOTE: All resolutions supported by the client will be listed in the Resolution drop-down menu when Auto-Detection at Power-up is disabled. Please note that some resolutions may not be applicable to your monitor(s).</td></tr>
</table>

3.3.4 Customizing Desktop and System Language Settings

To customize desktop and system language settings for your mt182L, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Desktop**.



2. Click drop-down menus or tick/untick checkboxes to choose desired settings. Refer to the following table for a description of each setting item.

System Language	
Item	**Description**
Language	Click the drop-down menu to select the system language. **NOTE:** Available languages may vary with the firmware version of your device. **NOTE:** You need to restart the system for the change to take effect.
Desktop Fonts	
Item	**Description**
Default Font	Click the drop-down menus to select the desired font, its style and size used for the user interface of the operating system, such as menus, options on menus, text labels for desktop shortcuts, tabs on program windows etc. **NOTE:** Your changes will not apply to the titles of opened windows, the Atrust Client Setup console, and the System Information window (**START** > **System Settings** > **System Information**).
Default Font Style	
Default Font Size	
Title Font	Click the drop-down menus to select the desired font, its style and size used for the titles of the opened windows.
Title Font Style	
Title Font Size	

DPI	
Item	**Description**
Custom DPI Setting	Click the drop-down menu to change **D**ots **P**er **I**nch. Some changes to the user interface might need a reboot to take effect.
Desktop Icons	
Item	**Description**
Remote Desktop	Check/Uncheck to show/hide shortcuts **Remote Desktop** on the START menu and local Linux desktop for service quick access. For more information, please refer to section "3.3.5 Hiding or Showing Quick Access Shortcuts" on page 86.
Citrix	Check/Uncheck to show/hide shortcuts **Citrix** on the START menu and local Linux desktop for service quick access. For more information, please refer to section "3.3.5 Hiding or Showing Quick Access Shortcuts" on page 86.
VMware View	Check/Uncheck to show/hide desktop shortcuts **VMware View** on the START menu and local Linux desktop for service quick access. For more information, please refer to section "3.3.5 Hiding or Showing Quick Access Shortcuts" on page 86.
Parallels 2X Client	Check/Uncheck to show/hide desktop shortcuts **Parallels 2X Client** on the START menu and local Linux desktop for service quick access. For more information, please refer to section "3.3.5 Hiding or Showing Quick Access Shortcuts" on page 86.
AnyDesk	Check/Uncheck to show/hide desktop shortcuts **AnyDesk** on the START menu and local Linux desktop.
Teamviewer QuickSupport	Check/Uncheck to show/hide desktop shortcuts **Teamviewer QuickSupport** on the START menu and local Linux desktop.
Tokenadmin	Check/Uncheck to show/hide desktop shortcuts **Tokenadmin** on the START menu and local Linux desktop.
XDMCP	Check/Uncheck to show/hide desktop shortcuts **XDMCP** on the START menu and local Linux desktop.
Firefox Web Browser	Check/Uncheck to show/hide desktop shortcuts **Firefox Web Browser** on the START menu and local Linux desktop for quick access. Also see "Topic 5: Using Built-in Applications" on page 36.
LibreOffice	Check/Uncheck to show/hide desktop shortcuts **LibreOffice** on the START menu and local Linux desktop for quick access. Also see "Topic 5: Using Built-in Applications" on page 36.
PDF Viewer (Document Viewer)	Check/Uncheck to show/hide desktop shortcuts **Document Viewer** on the START menu and local Linux desktop for quick access. Also see "Topic 5: Using Built-in Applications" on page 36.

<table>
<tr><td>Icon Size</td><td>Click the drop-down menu to select the desired size of desktop icons/shortcuts.</td></tr>
<tr><td>Icon Font Size</td><td>Click the drop-down menu to select the desired text label size of desktop icons/shortcuts.</td></tr>
<tr><td colspan="2">Desktop Background</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Enable Desktop Wallpaper</td><td>Check/Uncheck to enable/disable the use of Atrust wallpaper.

NOTE: If disabled, the solid color background (dark blue) will be used.</td></tr>
<tr><td>Enable Custom Wallpaper</td><td rowspan="3">Check/Uncheck to enable/disable the use of a custom wallpaper. More settings appear when checked.

For details, please refer to “3.3.6 Using a Custom Wallpaper” on page 87.</td></tr>
<tr><td>Download From</td></tr>
<tr><td>Custom Wallpaper File</td></tr>
<tr><td>Wallpaper Style</td><td>Click the drop-down menu to select the way to apply the wallpaper. Five options are available: Centered, Tiled, Stretched, Scaled, and Zoomed.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Centered</td><td>Centers the original image on the screen.</td></tr><tr><td>Tiled</td><td>Tiles the screen with the original image.</td></tr><tr><td>Stretched</td><td>Centers and extends/shrinks the image to fit the screen.</td></tr><tr><td>Scaled</td><td>Centers and sizes the image proportionally to fit the screen until the top-bottom or left-right sides fit the screen.</td></tr><tr><td>Zoomed</td><td>Centers and sizes the image proportionally to fill the screen.</td></tr></table>
NOTE: Depending on the size of the connected display, two options might have the same effect.</td></tr>
<tr><td>Wallpaper</td><td>Click the drop-down menu to select the color of Atrust wallpaper. Four colors are available: Green, Blue, Orange, and Cyan.</td></tr>
<tr><td colspan="2">Taskbar</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Auto-hide the taskbar</td><td>Check/Uncheck to auto-hide or always show the taskbar.</td></tr>
<tr><td>Taskbar Size</td><td>Click the drop-down menu to select the desired taskbar size.</td></tr>
</table>

3. Click **Save** to apply.

3.3.5 Hiding or Showing Quick Access Shortcuts

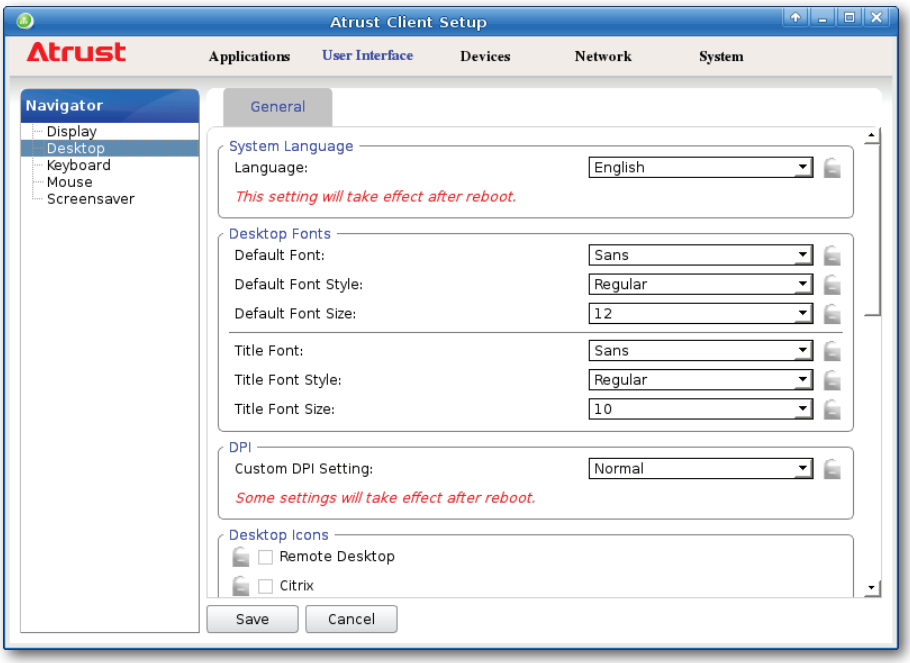
In case you want to access services quickly right on the local desktop, you can choose to show Quick Access shortcuts **Remote Desktop** / **Citrix** / **VMware View** on the START menu and local Linux desktop. These shortcuts enable you to access services quickly by clicking.

NOTE

- They're hidden by default.

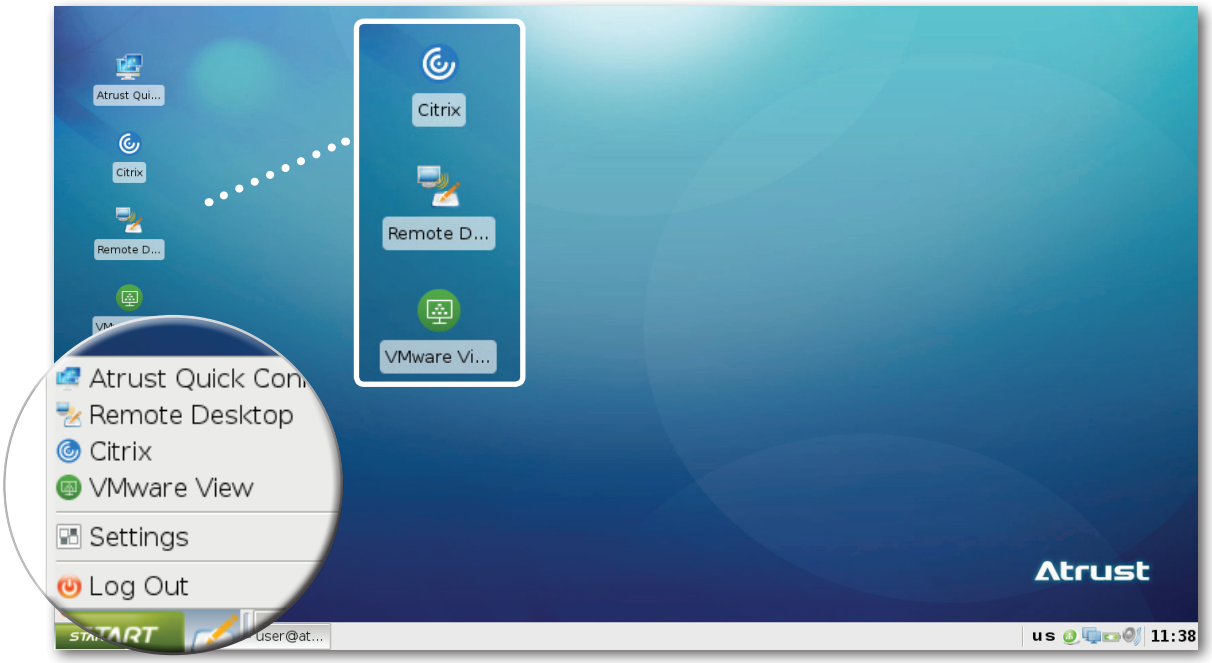
To show/hide shortcuts **Remote Desktop** / **Citrix** / **VMware View** on the START menu and local Linux desktop, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Desktop**.



2. Click to check/uncheck **Remote Desktop** / **Citrix** / **VMware View** in the Desktop Icons section to show/hide the quick access shortcuts **Remote Desktop** / **Citrix** / **VMware View** on the START menu and local Linux desktop.
3. Click **Save** to apply the change.

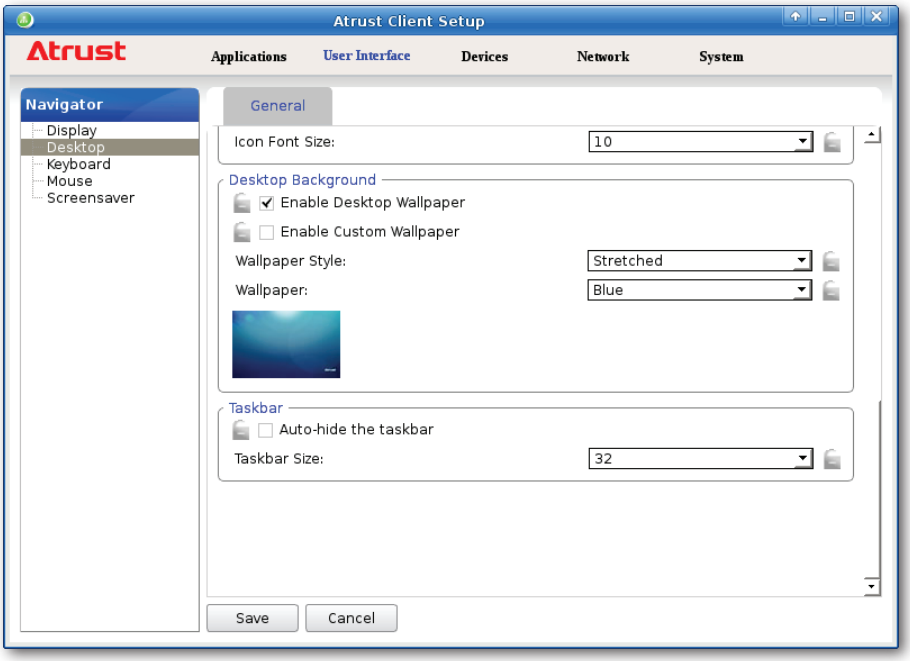
4. The selected shortcuts will be shown/hidden.



3.3.6 Using a Custom Wallpaper

To use a custom wallpaper, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Desktop**.



2. Check or Uncheck **Enable Custom Wallpaper** to enable or disable the use of a custom wallpaper.

3. Select the way to apply the wallpaper and where to download or get the image file. Three options are available to get the wallpaper: **Auto Setup**, **Atrust Device Manager**, and **File**.

> **NOTE**
>
> - If **Auto Setup** is selected, your thin client must be in Auto Setup environment and be well-configured for that environment. Please see "3.2.9 Enabling or Disabling Auto Setup" on page 62 for more information.
> - If **Atrust Device Manager** is selected, your thin client must be managed by Atrust Device Manager. For details, please see the User's Manual for Atrust Device Manager.

4. Provide other information if required.

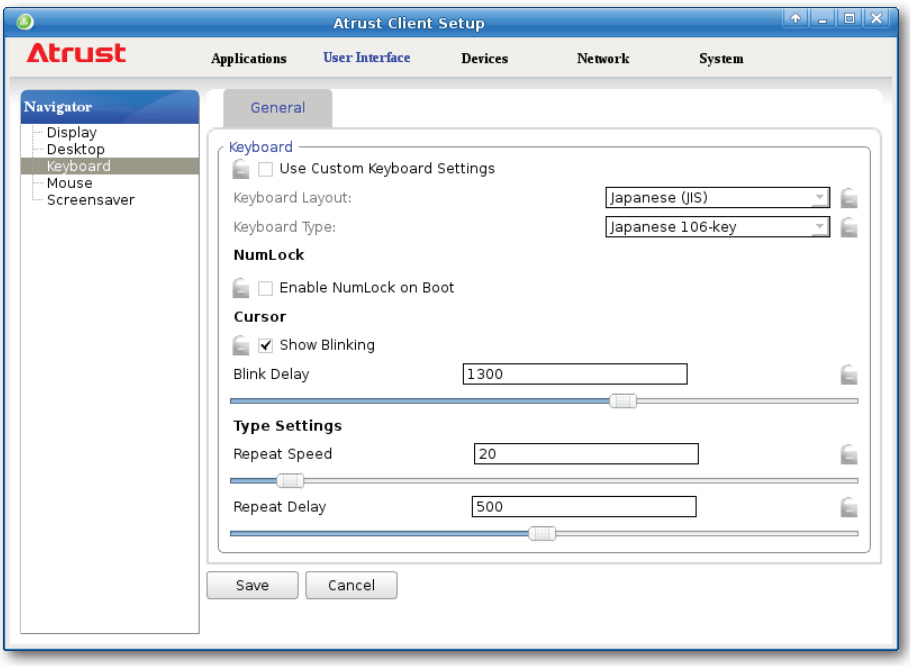
> **NOTE**
>
> - If **File** is selected, you need to specify where to get the image file locally, for example, a locally attached USB flash drive.
> - The maximum allowed size of a custom wallpaper file is **5 MB**.

5. Click **Save** to confirm.

3.3.7 Adjusting Keyboard Settings

To adjust keyboard settings for your mt182L, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Keyboard**.

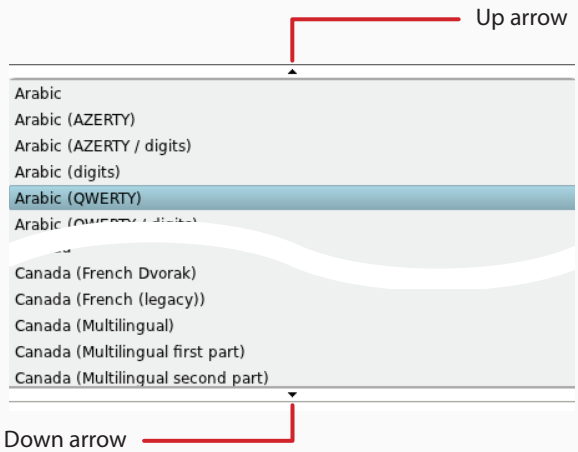


2. Click drop-down menus, tick/untick checkboxes, or move sliders to choose desired settings. Refer to the following table for a description of each setting item.

Keyboard		
Item		**Description**
Use Custom Keyboard Settings		Check/Uncheck to enable/disable the use of custom keyboard settings. **NOTE:** You are allowed to set the keyboard layout and type only when this setting is enabled.
Keyboard Layout		Click the drop-down menu to select the desired keyboard layout.
Keyboard Type		Click the drop-down menu to select the desired keyboard type.
Enable NumLock on Boot		Check/Uncheck to enable/disable the NumLock key after system startup.
Cursor	Show Blinking	Check/Uncheck to enable/disable the cursor blinking (local desktop only).
	Blink Delay	Move the slider to select the blink delay between each occurrence of cursor.
Type Settings	Repeat Speed	Move the slider to select the character repeat rate when a key is held down.
	Repeat Delay	Move the slider to select the character repeat delay between its each occurrence.

TIP

- Hang your mouse over the Up/Down arrow to quickly scroll up/down the Keyboard Layout list.



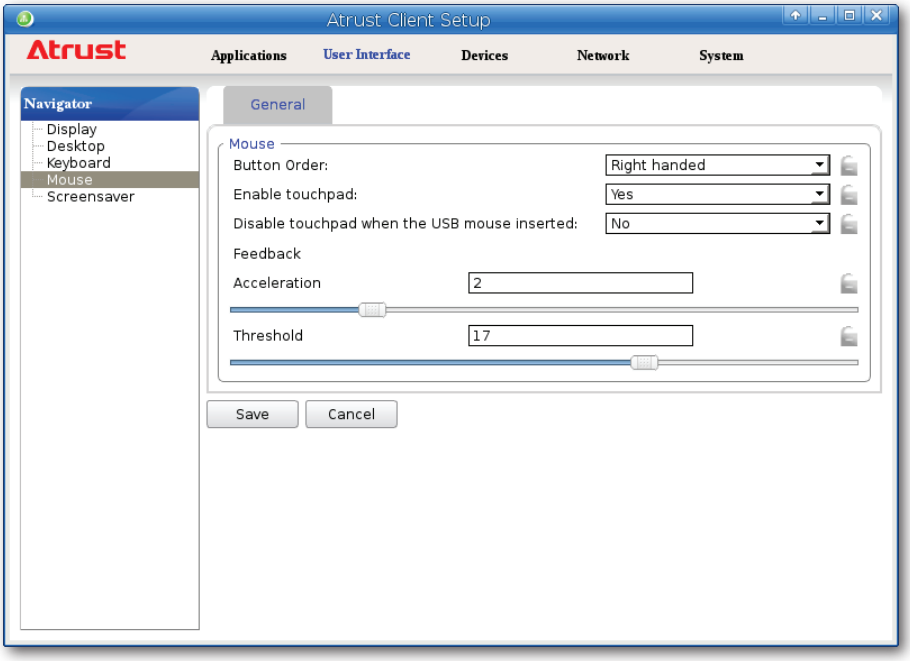
- To fine-tune a setting value, click its slider, and then use the Right/Left key to increase/decrease the value by 1 or the Page Up/Page Down key to increase/decrease by 10.

3. Click **Save** to apply.

3.3.8 Adjusting Mouse Settings

To adjust mouse settings for your mt182L, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Mouse**.



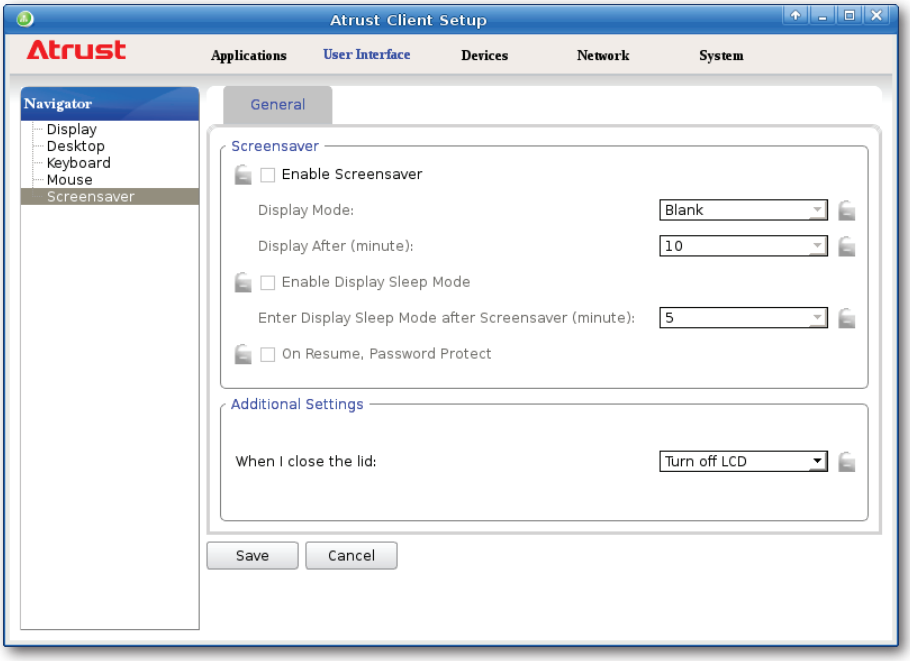
2. Click the drop-down menu or move sliders to choose desired setting values. Refer to the following table for a description of each setting item.

Mouse		
Item		**Description**
Button Order		Click the drop-down menu to switch mouse buttons for right-hand/left-hand use.
Enable touchpad		Click the drop-down menu to enable or disable the touchpad.
Disable touchpad when the USB mouse inserted		Click the drop-down menu to choose whether to disable the touchpad when a USB mouse is attached.
Feedback	Acceleration	Move the slider to select the rate at which the mouse increases speed while moving.
	Threshold	Move the slider to select the moved distance (pixels) after which the mouse starts to accelerate.

3.3.9 Configuring Screensaver Settings

To configure screensaver settings for your mt182L, please do the following:

1. On Atrust Client Setup, click **User Interface** > **Screensaver**.



2. Click drop-down menus or tick/untick checkboxes to choose desired settings.

<table>
<tr><th colspan="2">Screensaver</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Enable Screensaver</td><td>Check/Uncheck to enable/disable screensaver.</td></tr>
<tr><td>Display Mode</td><td>Click to select the display mode of screensaver. Three options are available: Blank, Logo, and Image.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Blank</td><td>Displays a black screen.</td></tr><tr><td>Logo</td><td>Displays the Atrust floating logo.</td></tr><tr><td>Image</td><td>Displays the specified images.</td></tr></table></td></tr>
<tr><td>Display After (minute)</td><td>Click to select the wait time for screensaver.</td></tr>
</table>

<table>
<tr><td>Specify the source</td><td>Click to select where to get the images and use for screensaver. Three options are available: Default, Auto Setup, Atrust Device Manager.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Default</td><td>Uses the default image in your thin client.</td></tr><tr><td>Auto Setup</td><td>Gets and uses images from Auto Setup.</td></tr><tr><td>Atrust Device Manager</td><td>Gets and uses images from Atrust Device Manager.</td></tr></table>NOTE: For details on Auto Setup, please refer to its User’s Guide.
NOTE: For details on Atrust Device Manager, please refer to its User’s Manual.</td></tr>
<tr><td>Change picture every</td><td>Click to set the interval to change the displayed image.</td></tr>
<tr><td>Enable Display Sleep Mode</td><td>Check to turn off (i.e. stop sending signals to) the display to maximize the energy savings.</td></tr>
<tr><td>Enter Display Sleep Mode after Screensaver (minute)</td><td>Click to select when to turn off (i.e. stop sending signals to) the display after Screensaver starts.</td></tr>
<tr><td>On Resume, Password Protect</td><td>Check/Uncheck to resume with/without a password.</td></tr>
<tr><td colspan="2">Additional Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>When I close the lid</td><td>Click to select what to do when you close the lid.</td></tr>
</table>

TIP

- While setting wait time for screensaver, you can hang your mouse over the Up / Down arrow to quickly scroll up / down the Minute list.

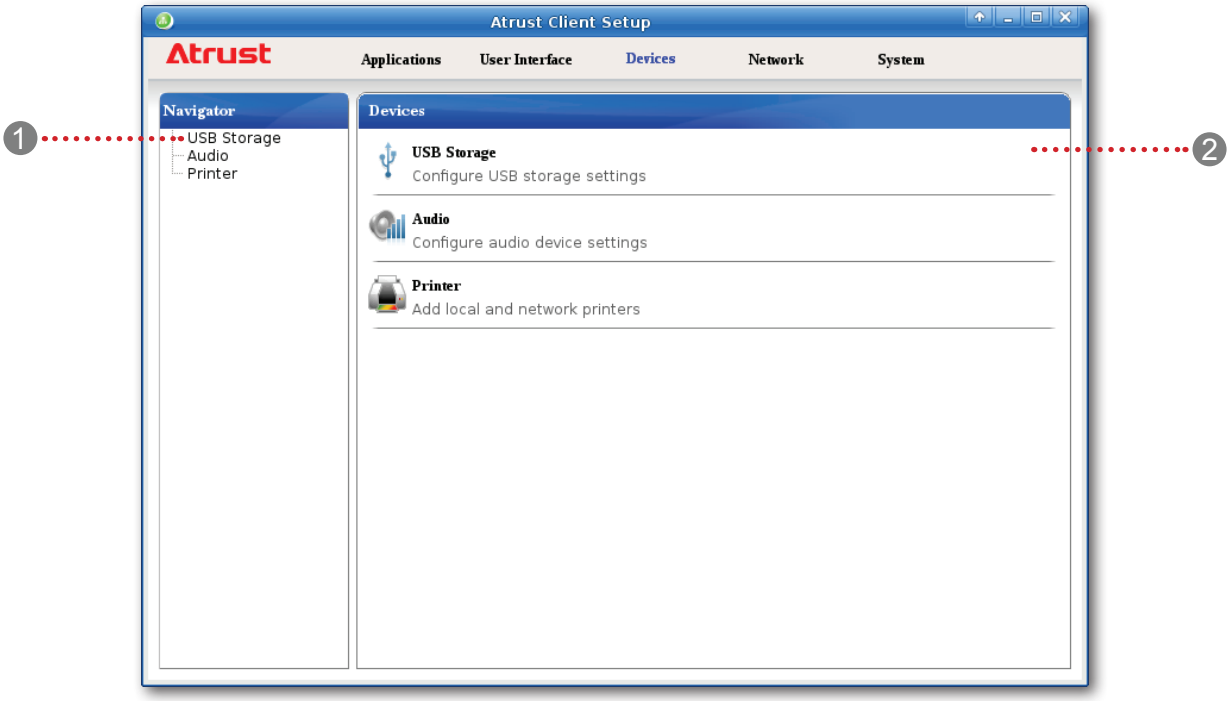
3. Click **Save** to apply.

3.4 Configuring External Device Settings

3.4.1 Devices Tab Overview

Devices tab enables you to configure settings for external devices of clients. To access available settings of **Devices** tab, click the tab on Atrust Client Setup.

Devices Tab Overview



Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **Devices** tab or to select a setting entry under a selected setting item.
2	Configuration area	Configures setting values when a setting item or entry is selected.

3.4.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
Devices	USB Storage		Click to configure settings for USB storage devices.	3.4.3 3.4.4	94 95
	Audio		Click to configure settings for audio devices.	3.4.5 3.4.6 3.4.7	96 97 98
	Printer		Click to add local or network printers.	3.4.8 3.4.9	99 102

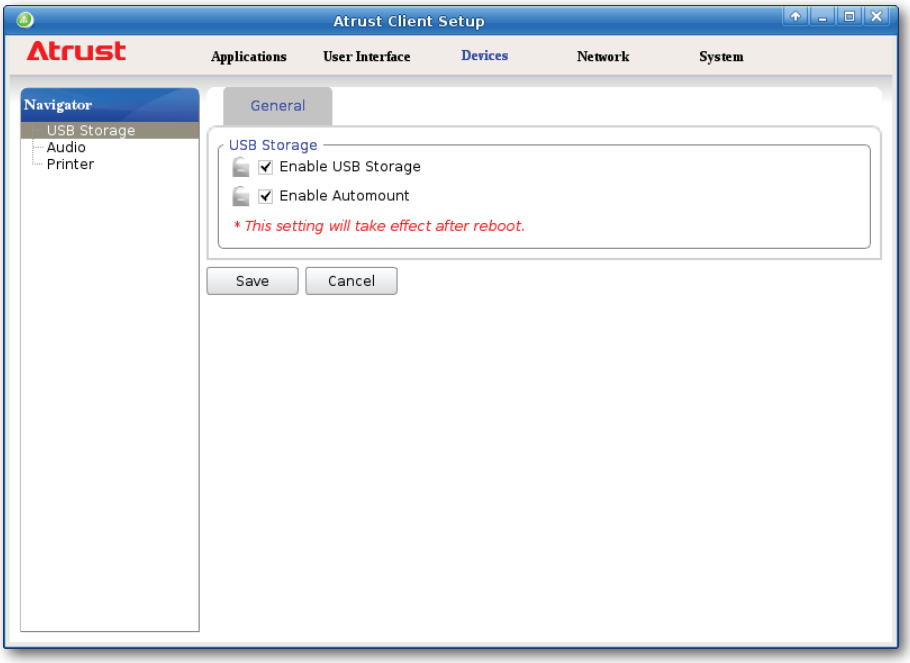
3.4.3 Configuring Settings for USB Storage Devices

To configure settings for USB storage devices, please do the following:

NOTE

- To access locally attached USB storage devices in a local or virtual session, you need to configure appropriate settings under this setting item.

1. On Atrust Client Setup, click **Devices** > **USB Storage**.



2. Tick/untick the checkboxes to choose the desired settings.

Settings for USB Storage Devices	
Item	**Description**
Enable USB Storage	Tick/Untick this checkbox to allow/disallow the access of USB storage devices. **NOTE:** To use the locally attached USB storage devices in an RDP / ICA / View / 2X session, the mapping of local USB storage devices must be enabled in this session's RDP / ICA / View / 2X connection settings. For detailed instructions and more related settings, please refer to sections: "3.6.5 Configuring Advanced RDP Connection Settings" on page 144 "3.6.11 Configuring Advanced ICA Connection Settings" on page 182 "3.6.14 Configuring Advanced View Connection Settings" on page 216 "3.6.22 Configuring Advanced RAS / RDP Connection Settings" on page 235
Enable Automount	Tick/Untick this checkbox to enable/disable the automount of USB storage devices. **NOTE:** If this setting is disabled, users need to manually mount the attached USB storage devices. For detailed instructions, please refer to section "3.4.4 Manually Mount and Eject Attached USB Storage Devices" on page 95.

3. Click **Save** to save your change.

NOTE

- For your changes to take effect, you need to restart your system.

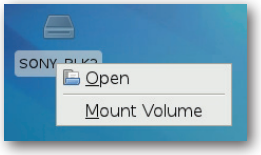
3.4.4 Manually Mount and Eject Attached USB Storage Devices

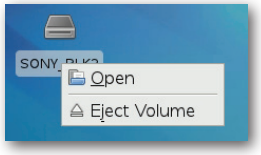
To mount/eject an attached USB storage device, please do the following:

NOTE

- If **Enable Automount** is checked (see section "3.4.3 Configuring Settings for USB Storage Devices" on page 94), then an attached USB storage device will be mounted automatically.

1. Right click the desktop icon of the attached USB storage device.
2. A popup menu appears.





3. Click to select **Mount Volume**/**Eject Volume** to mount\eject the attached USB storage device.

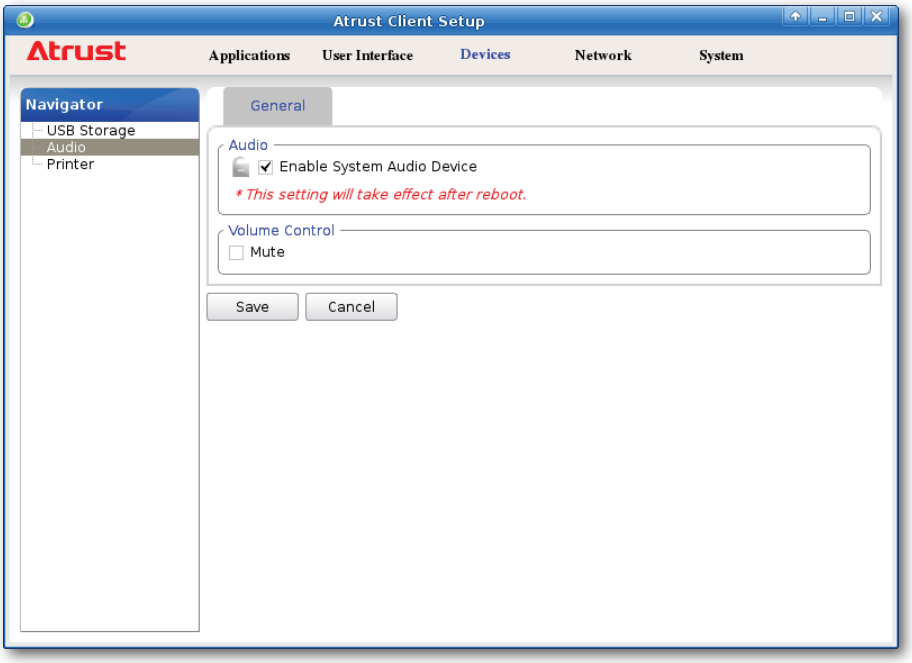
3.4.5 Disabling or Enabling Attached Audio Devices

To disable/enable attached audio devices, please do the following:

NOTE

- If you disable locally attached audio devices, client users are not allowed to perform audio playback or recording with these devices in an RDP / ICA / View session.
- To perform audio playback or recording with local audio devices in an RDP / ICA / View session, you need to enable locally attached audio devices here (the **Audio** setting item under **Devices** tab) and configure audio related settings in the RDP / ICA / View connection settings. For detailed instructions, please refer to sections:
  - ✧ "3.6.5 Configuring Advanced RDP Connection Settings" on page 144
  - ✧ "3.6.11 Configuring Advanced ICA Connection Settings" on page 182
  - ✧ "3.6.14 Configuring Advanced View Connection Settings" on page 216

1. On Atrust Client Setup, click **Devices** > **Audio**.



2. Click to check/uncheck **Enable System Audio Device**.
3. Click **Save** to confirm your selection.

NOTE

- The change will not take effect until mt182L has been restarted.

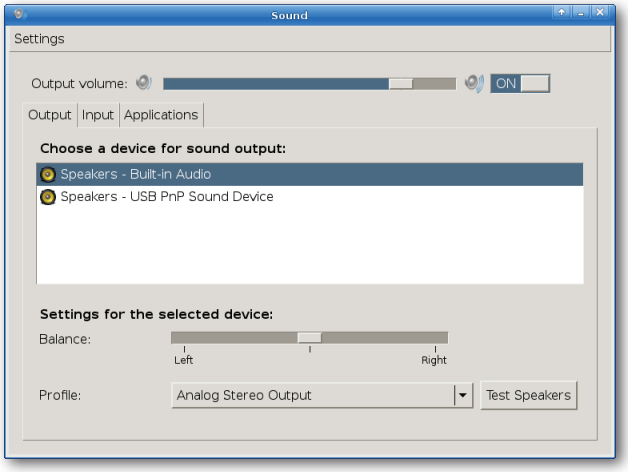
3.4.6 Using Audio Devices

By default, your mobile thin client would use built-in speaker and/or audio devices attached to 3.5 mm audio ports. In case that you want to use an audio device of other interfaces, you need to change the default.

To configure default audio devices, please do the following:

1. Connect the desired audio device to your thin client.
2. Open the Mixer window:

   - On the ***Quick Connection screen***, click icon in the bottom-right corner.
   - On the ***local desktop***, right-click icon in the bottom-right corner, and then select **Sound Preferences**.

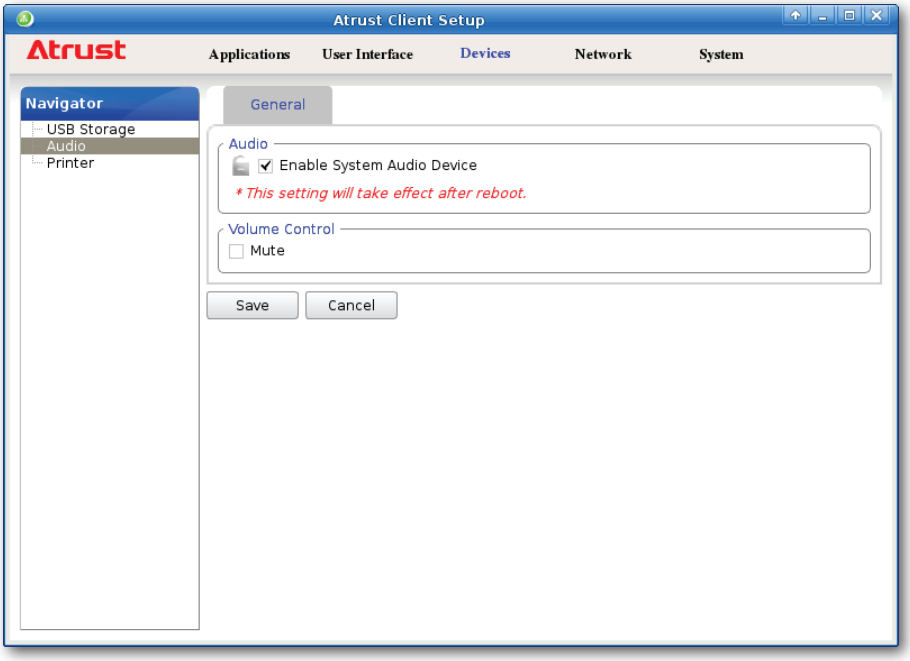


3. Click the Output / Input tab, select the default device for sound output / input.

3.4.7 Muting or Unmuting the Sound

To mute/unmute the sound through Atrust Client Setup, please do the following:

1. On Atrust Client Setup, click **Devices** > **Audio**.

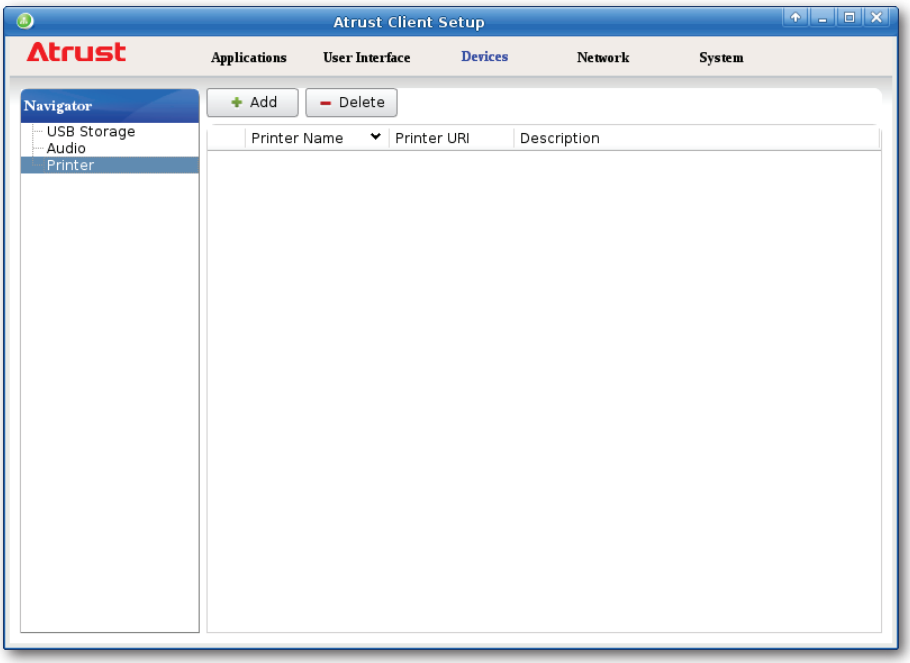


2. In the Volume Control section, check / uncheck **Mute** to mute / unmute the sound.
3. Click **Save** to apply.

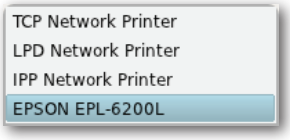
3.4.8 Adding a Local Printer

To add a local printer for your mt182L, please do the following:

1. Connect the desired printer to your mt182L and turn on the printer.
2. On Atrust Client Setup, click **Devices** > **Printer**.

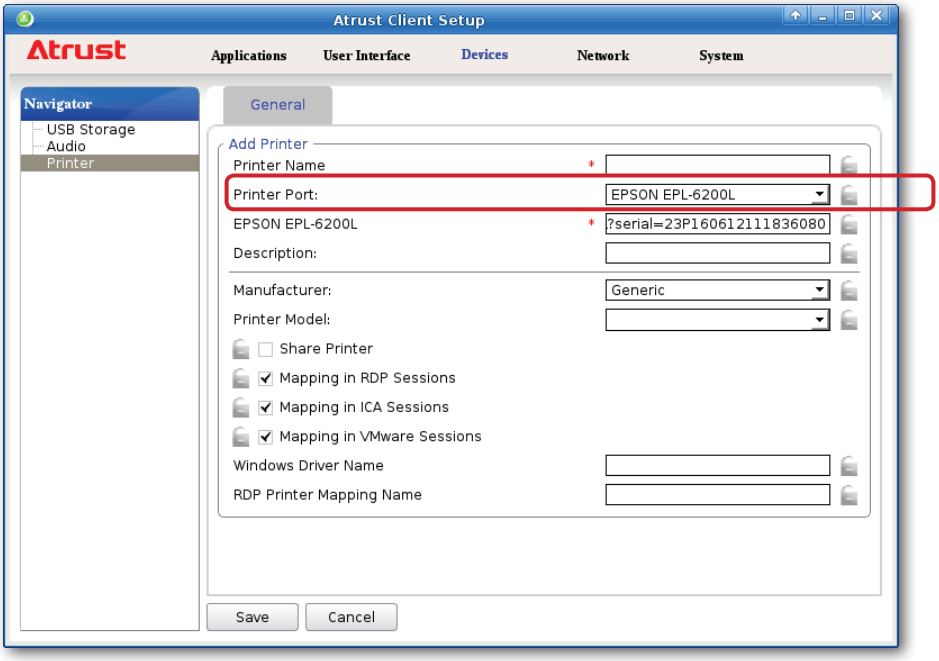


3. Click **Add** on the top of the Printer list.
4. The system automatically start searching for available local printers.
5. Upon completion, the discovered local printers will be listed on the Printer Port drop-down menu.
6. Click the Printer Port drop-down menu to select the desired local printer.



7. Fields in the Add Printer section will automatically change to fit the type of the selected printer.

8. A field for the selected printer appears and the printer URI (Uniform Resource Identifier) data is automatically filled out in the field.



NOTE

- A URI (Uniform Resource Identifier) is a sequence of characters that is used to identify a resource on the Internet.

9. Click the Manufacturer and Printer Model drop-down menus to select the manufacturer and model for the attached local printer.

NOTE

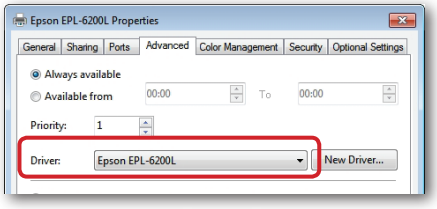
- For the printer to operate normally, you need to specify the correct information in these two fields. Otherwise, the printer would fail to work.

10. Refer to the following table to configure desired settings.

NOTE

- You may need to provide the Windows driver name for your printer. For details, please refer to descriptions in the table.

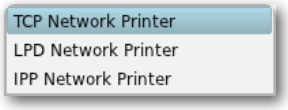
11. Type the desired printer name, and then click **Save** to apply.

Settings for Printers	
Item	**Description**
Share Printer	Check/Uncheck to share the printer. Once **Share Printer** is checked, other computers in the same network segment will be allowed to use the printer. To add this shared printer for use on other computers, please do the following: 1. For computers running a Windows Server operating system, such as Windows Server 2008 R2, please add the **Internet Printing Client** feature first (Click **Start** > **All Programs** > **Administrative Tools** > **Server Manager** > **Action** > **Add Features** > **Internet Printing Client**, follow the wizard to complete the task, and then restart your system). 2. Click **Start** > **Devices and Printers** > **Add a printer** > **Add a network, wireless or Bluetooth printer**. 3. Click **Stop** to cancel the automatic printer search, and then click **The printer that I want isn't listed**. 4. Under **Select a shared printer by name**, enter http://IP address of your thin client:631/printers/Printer Name. **NOTE:** For example, if a printer is locally attached to your thin client and is added as a local printer through Atrust Client Setup with the printer name **EPS**, and the IP address of your thin client is 192.168.50.146. Here you should enter: **http://192.168.50.146:631/printers/EPS** 5. Click **Next** to continue. 6. Select the manufacturer and model of the printer, and then click **OK** to install the correct driver. 7. Upon completion, a success message appears. Click **Next** to continue. 8. On the appeared page, click **Print a test page** to test the printer. 9. Click **Finish** to apply. The printer is added to the Printers and Faxes list.
Mapping in RDP Sessions	Check/Uncheck to enable/disable the locally connected printer in an RDP session.
Mapping in ICA Sessions	Check/Uncheck to enable/disable the locally connected printer in an ICA session.
Mapping in VMware Sessions	Check/Uncheck to enable/disable the locally connected printer in a View session.
Windows Driver Name	Keep this field blank, if the printer works well in a session. In case that the printer fails to work, filling in this field may solve the problem. To find out the required information, please do the following: 1. Attach the printer to a computer running a Windows OS, complete the required installation, and ensure the printer works well. 2. Click **Start** > **Devices and Printers**, and then, in the opened window, right click the printer to open a popup menu. 3. On the popup menu, click to select **Printer properties**. 4. In the opened window, click **Advanced**. The driver name is shown. 
RDP Printer Mapping Name (for RDP sessions only)	Type in the desired printer name in a session (Windows desktop). If this field remains blank, the name you typed in the Printer Name field will be used.

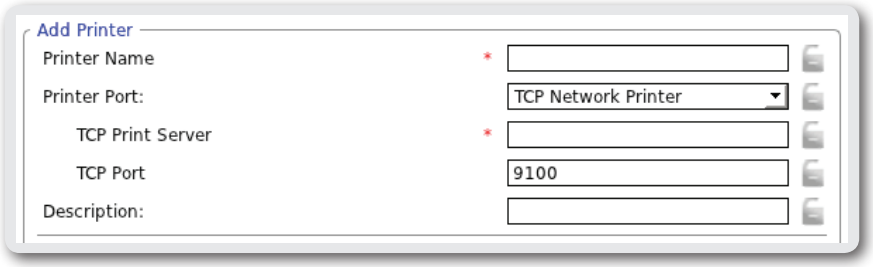
3.4.9 Adding a Network Printer

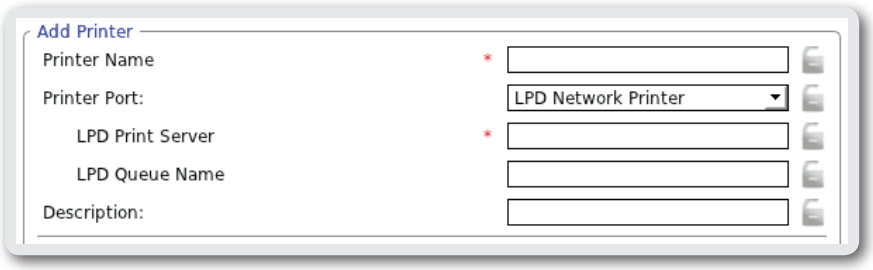
To add a network printer for your mt182L, please do the following:

1. Ensure that your mt182L is connected to the network and the desired network printer is turned on.
2. On Atrust Client Setup, click **Devices** > **Printer**.
3. Click **Add** on the top of the Printer list.
4. The system automatically starts searching for available local printers. Upon completion, the discovered local printers will be listed on the Printer Port drop-down menu.
5. Click the Printer Port drop-down menu to select the desired network printer. Three types of network printers are available: **TCP Network Printer**, **LPD Network Printer**, and **IPP Network Printer**.



6. Fields in the Add Printer section will automatically change to fit the type of the selected printer.
7. Type in the IP address of the network printer in the TCP Printer Server, LPD Printer Server, or IPP URI field.





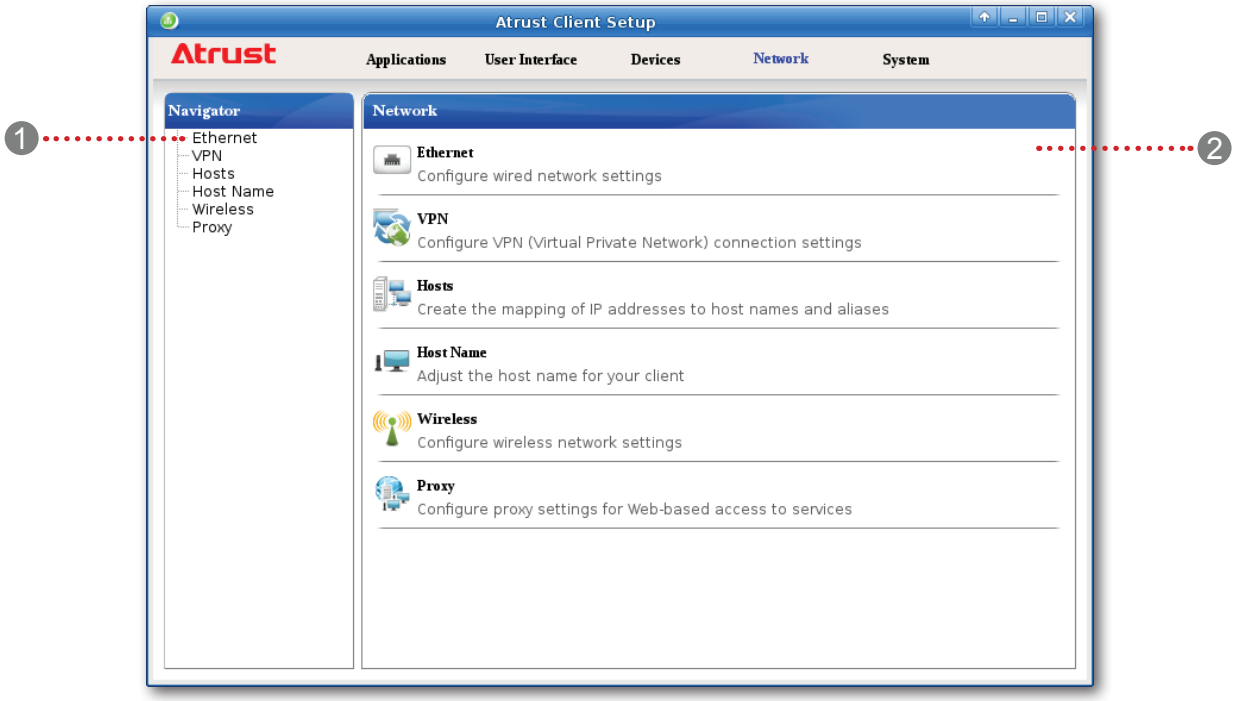
8. Click the Manufacturer and Printer Model drop-down menus to select the manufacturer and model for the desired network printer.
9. Refer to the table on page 101 to configure other printer settings, and then click **Save** to apply.

3.5 Configuring Network Settings

3.5.1 Network Tab Overview

Network tab enables you to configure network settings for clients. To access available settings of **Network** tab, click the tab on Atrust Client Setup.

Network Tab Overview



Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **Network** tab or to select a setting entry under a selected setting item.
2	Configuration area	Configures setting values when a setting item or entry is selected.

3.5.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
Network	Ethernet		Click to configure wired network settings.	3.5.3 3.5.4	105 108
	VPN		Click to configure VPN (Virtual Private Network) connection settings and create a VPN connection.	3.5.5 3.5.6	109 113
	Hosts		Click to create the mapping of IP addresses to names or aliases of hosts and create the Failover Cluster list.	3.5.7 3.5.8	114 116
	Host Name		Click to change the host name of your thin client.	3.5.9	118
	Wireless		Click to configure wireless network settings and create a wireless connection.	3.5.10 3.5.11 3.5.12 3.5.13	119 120 121 124
	Proxy		Click to configure proxy settings for Web-based access to services.	3.5.14	125

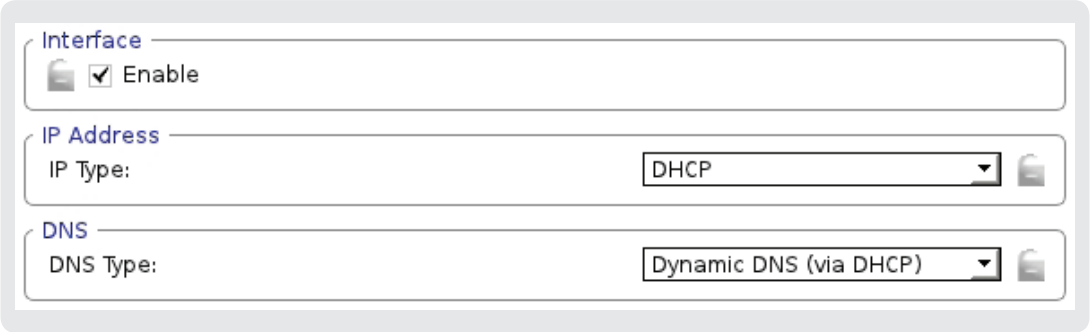
3.5.3 Configuring Wired Network Settings

The **Ethernet** setting enables you to configure the wired network settings for your mt182L thin client.

Enabling or Disabling the Ethernet Network Interface

To enable/disable the Ethernet network interface, please to the following:

1. On Atrust Client Setup, click **Network** > **Ethernet**.
2. Under Interface section, check/uncheck **Enable** to enable/disable the Ethernet network interface.



3. Click **Save** to apply.

Using a Dynamic IP Address

To use a dynamic IP address, please do the following:

1. On Atrust Client Setup, click **Network** > **Ethernet**.
2. Under the IP address section, click the drop-down menu to select **DHCP** for the IP type field.

> **NOTE**
> - If **DHCP** is selected, the DHCP server over the network will automatically assign an IP address to your mt182L thin client. This is the default setting.

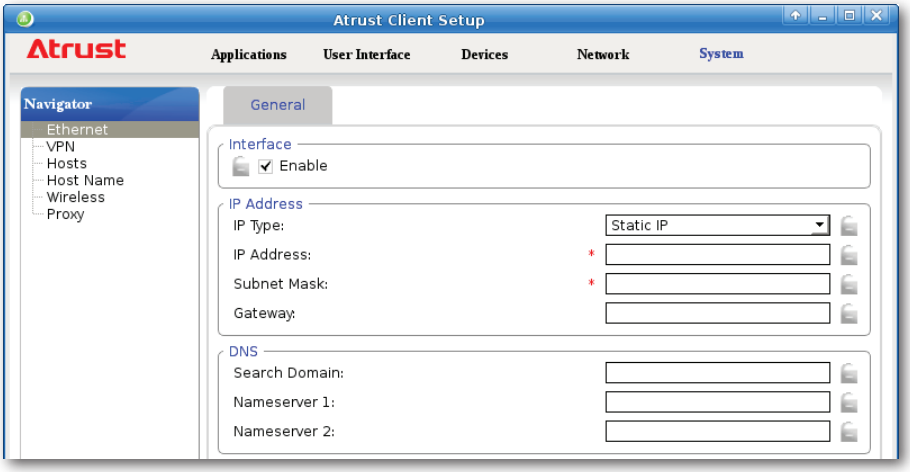
3. Click **Save** to apply.

Using a Static IP Address

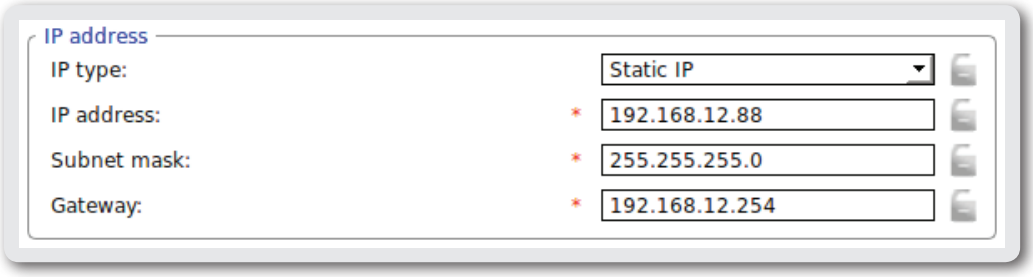
To use a static IP address, please do the following:

> **NOTE**
> - It's recommended to use a dynamic IP address for your mt182L thin client in a corporate network environment.

1. On Atrust Client Setup, click **Network** > **Ethernet**.
2. Under the IP address section, click the drop-down menu to select **Static IP** for the IP type field.
3. The IP address, Subnet mask, and Gateway fields appear in the IP address section.



4. Type in the IP address, subnet mask, and gateway for your mt182L thin client.



NOTE

- Consult your network administrator for a free IP address and other required data about the network to which your mt182L connects.
- The red asterisks indicate the required fields.

5. Click **Save** to apply.

NOTE

- You need to further specify DNS server addresses manually if you choose to use a static IP address.

Obtaining DNS Server Addresses Automatically

To obtain DNS Server addresses automatically, please do the following:

NOTE

- You cannot obtain DNS server addresses automatically through the DHCP server if you choose not to get the IP address via the DHCP server.

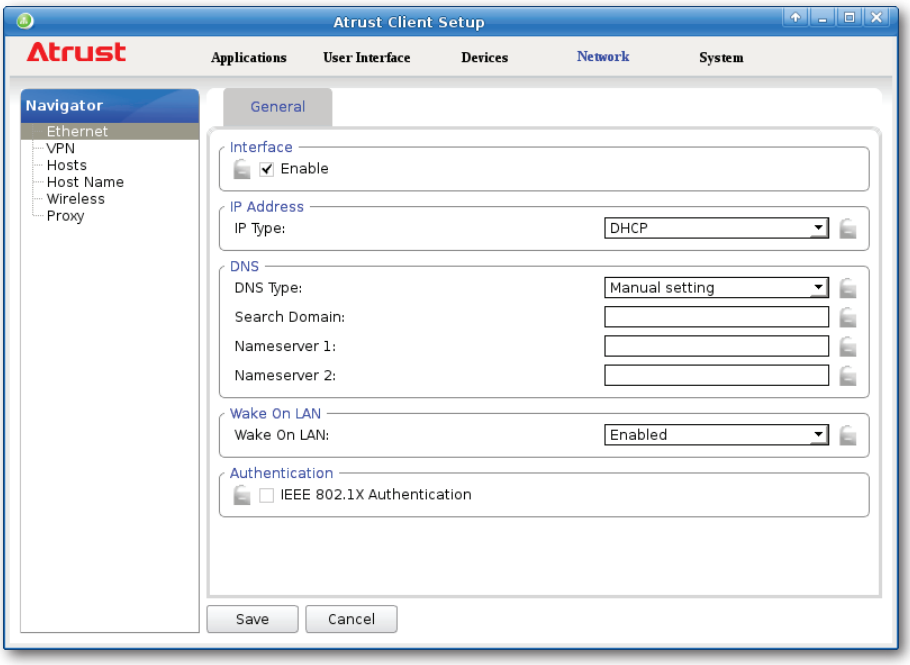
1. On Atrust Client Setup, click **Network** > **Ethernet**.
2. Under the DNS section, click the drop-down menu to select **Dynamic DNS (via DHCP)** for the DNS type field.
3. Click **Save** to apply.

Specifying DNS Server Addresses Manually

To specify DNS Server addresses manually, please do the following:

1. On Atrust Client Setup, click **Network** > **Ethernet**.
2. Under the DNS section, click the drop-down menu to select **Manual setting**.
3. The **Search domain**, **Nameserver 1**, and **Nameserver 2** fields appear in the DNS section.

> **NOTE**
>
> - If you choose to use a static IP address for your mt182L thin client, then you need to specify DNS server addresses manually. In this case, the DNS type field will not appear for you to select **Manual setting** or **Dynamic DNS (via DHCP)**.



4. Type in the preferred DNS server address in the Nameserver 1 field and the alternate DNS server address in the Nameserver 2 field if any.

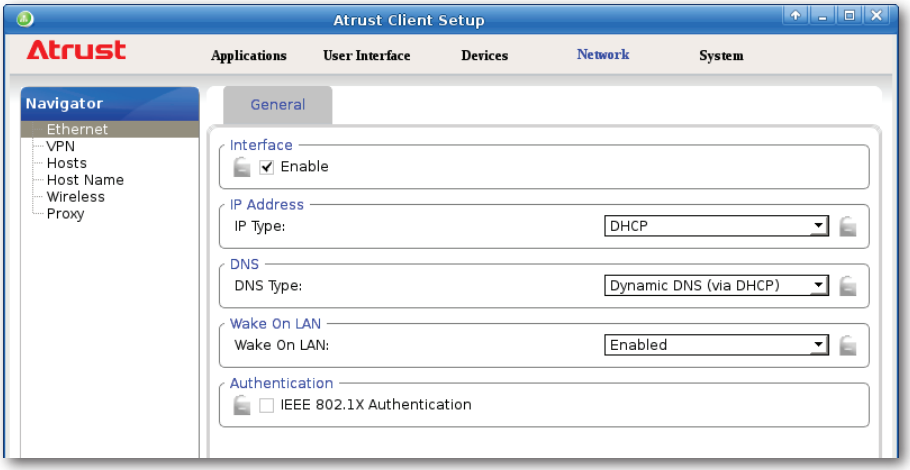
> **NOTE**
>
> - Specifying a domain name in the Search Domain field will enable your system to discover a computer in that domain simply with its computer name rather than its FQDN (Fully Qualified Domain Name).

5. Click **Save** to apply.

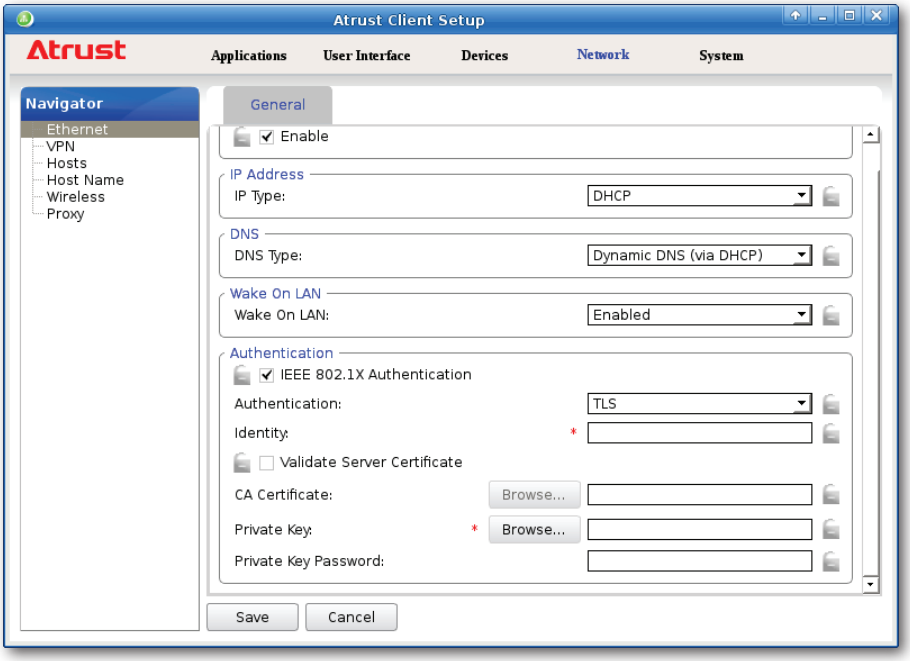
3.5.4 Configuring IEEE 802.1X Authentication

To configure IEEE 802.1X authentication, please do the following:

1. On Atrust Client Setup, click **Network** > **Ethernet**.



2. Under the Authentication section, check/uncheck **IEEE 802.1X Authentication** to enable/disable the IEEE 802.1X authentication.



3. Select the desired authentication method, and then provide files or information as required.

NOTE

- Consult your network administrator for required files or information on configuration and authentication.

3.5.5 Establishing and Stopping a VPN connection

The **VPN** setting enables you to establish/stop a virtual private network connection for your mt182L.

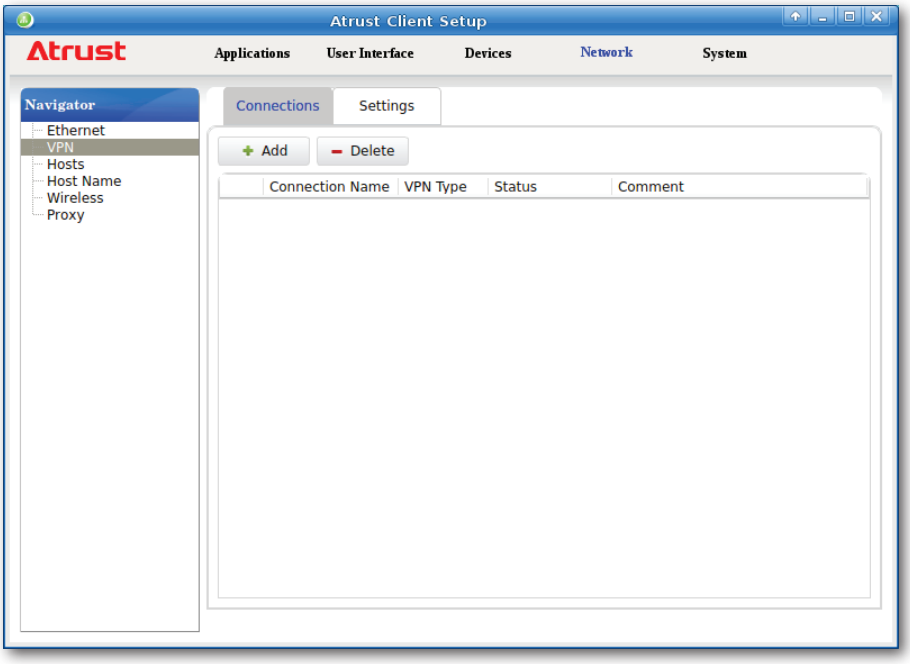
NOTE

- The **VPN** setting also allows you to configure and manage virtual private network settings. For instructions on how to configure and manage virtual private network settings, please refer to section "3.5.6 Configuring Virtual Private Network Settings" on page 113.

Adding a Virtual Private Network

To add a virtual private network, please do the following:

1. On Atrust Client Setup, click **Network** > **VPN** to open the Virtual Private Network list.

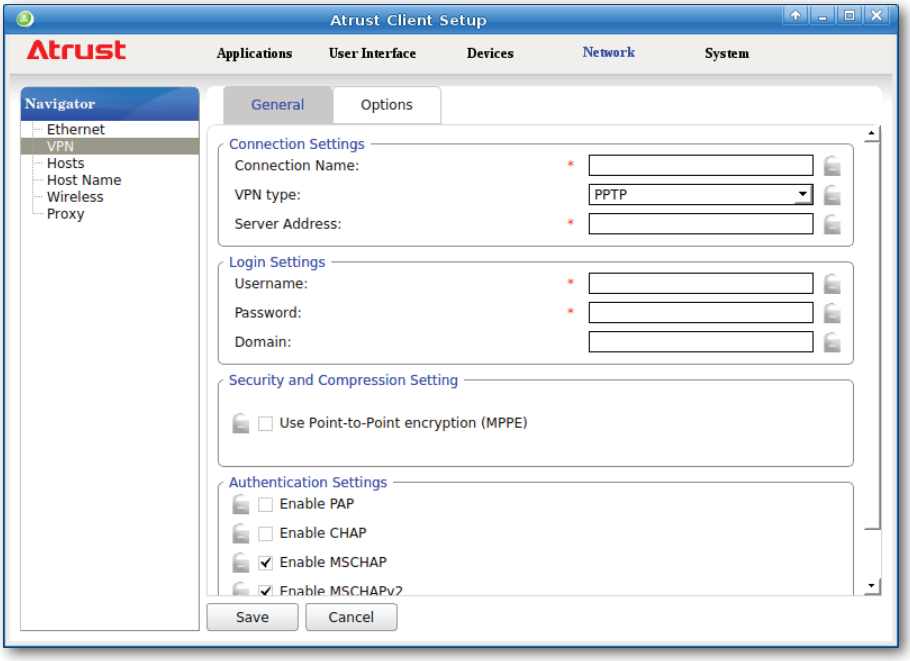


NOTE

- If you haven't created any entry, the Virtual Private Network list will be empty.

2. Click **Add** on the top of the Virtual Private Network list.

3. On **General** tab, click the drop-down menu to select the desired VPN type. Three types are available: **PPTP**, **L2TP**, and **Cisco AnyConnect**.



NOTE

- The setting items will vary with the selected VPN type.

4. Type in or click drop-down menus to provide information about configuration and authentication.

NOTE

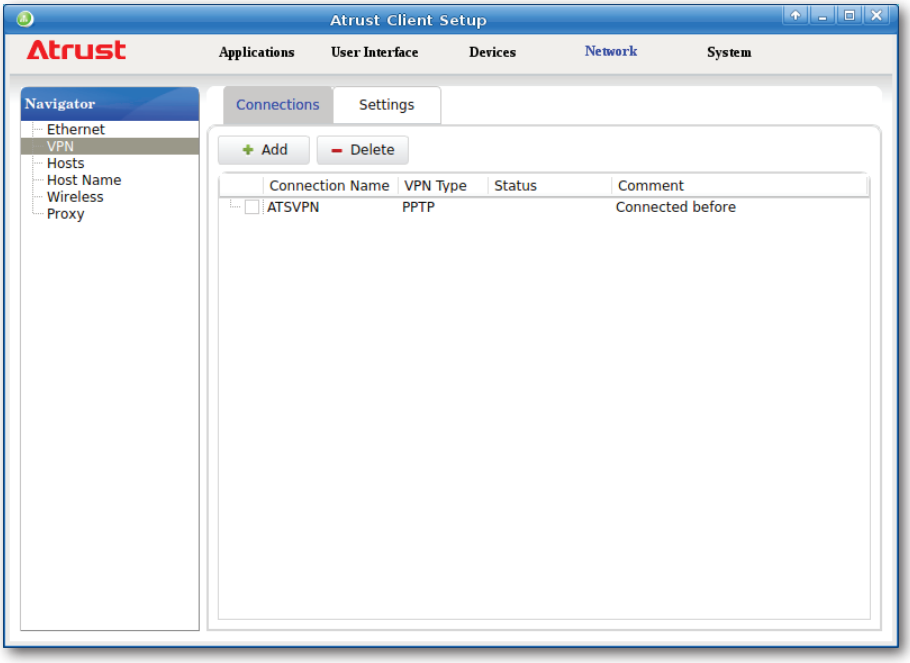
- Consult your network administrator for required information on configuration and authentication.

5. On **Options** tab, configure the DNS-related settings if needed.
6. Click **Save** to add the virtual private network.

Establishing a Virtual Private Network Connection

To establish a virtual private network connection for your mt182L, please do the following:

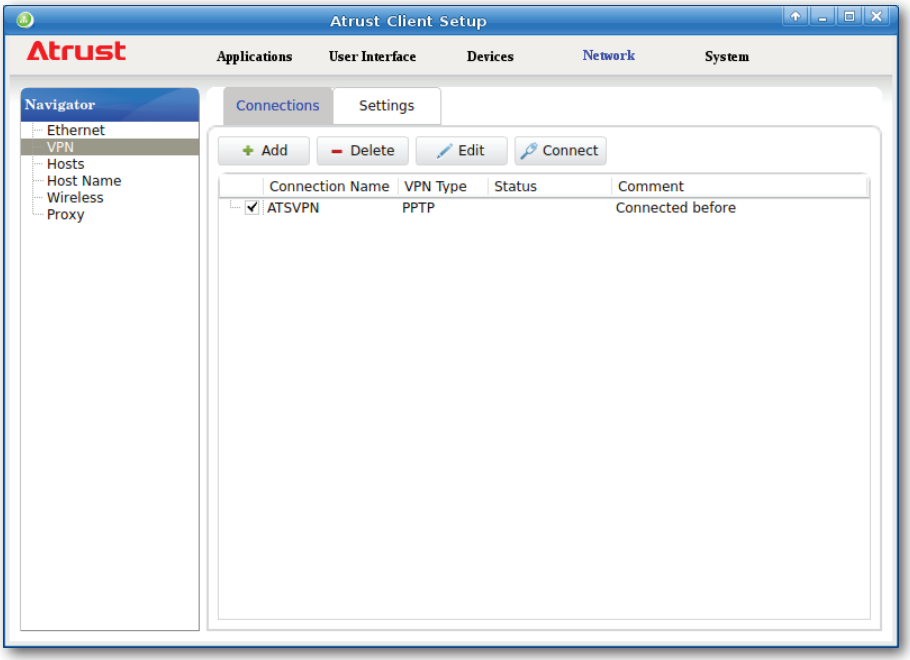
1. On Atrust Client Setup, click **Network** > **VPN** to open the Virtual Private Network list.



NOTE

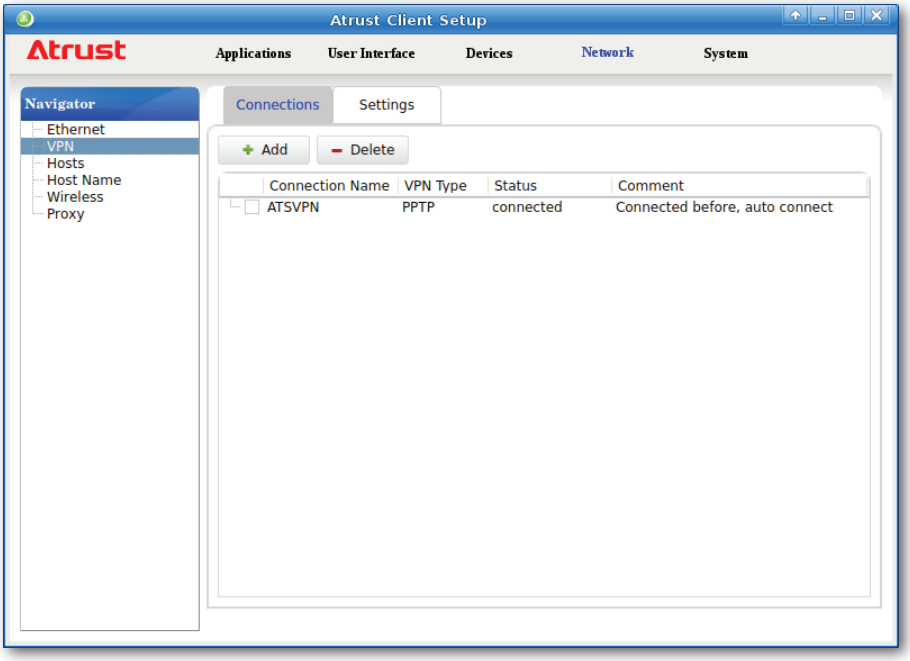
- If you haven't created any entry, the Virtual Private Network list will be empty. For instructions on adding a virtual private network, please see the preceding topic.

2. Click to check the desired virtual private network. The Connect button then appears on the top of the Virtual Private Network list.



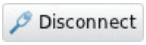
3. Click **Connect** to create a virtual private network connection through the selected network entry.

4. Upon completion, the Status column of the virtual private network will show **connected**.



Stopping a Virtual Private Network Connection

To stop a virtual private network connection, please do the following:

1. On Atrust Client Setup, click **Network** > **VPN** to open the Virtual Private Network list.
2. Click to check the desired virtual private network. The Disconnect  button appears on the top of the Virtual Private Network list.
3. Click **Disconnect** to stop the virtual private network connection.

Deleting a Virtual Private Network

To delete a virtual private network, please do the following:

1. On Atrust Client Setup, click **Network** > **VPN** to open the Virtual Private Network list.
2. Click to check the desired virtual private network.
3. Click **Delete** to remove the selected virtual private network.

3.5.6 Configuring Virtual Private Network Settings

Adjusting Connection settings for a Virtual Private Network

To adjust connection settings for a virtual private network, please do the following:

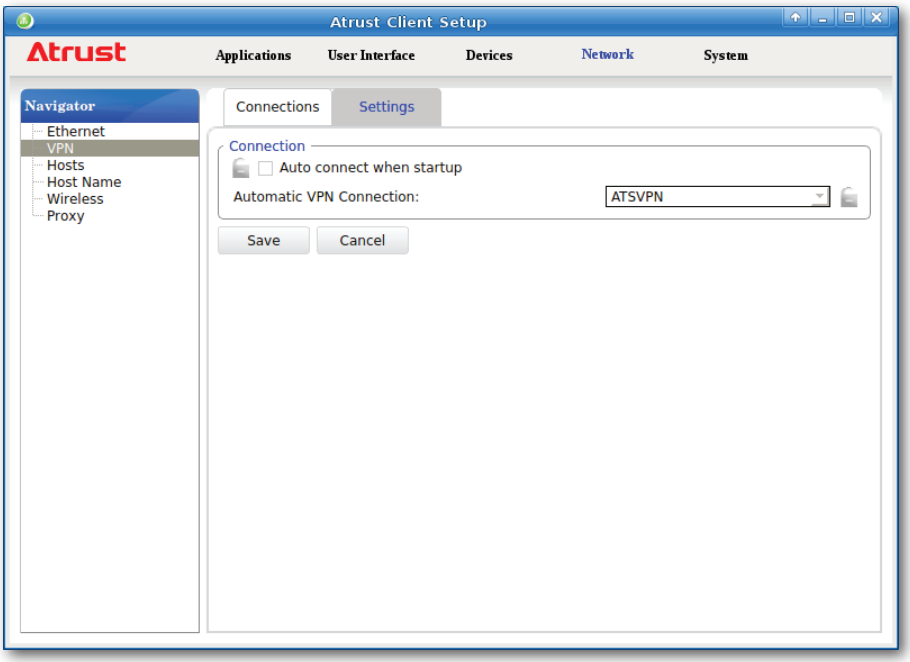
1. On Atrust Client Setup, click **Network** > **VPN** to open the Virtual Private Network list.
2. Click to check the desired virtual private network. The Edit

button appears on the top of the Virtual Private Network list.
3. Click **Edit** to adjust the settings, and then click **Save** to apply.

Configuring General Settings for Virtual Private Network Connections

To configure general settings for virtual private network connections, please do the following:

1. On Atrust Client Setup, click **Network** > **VPN**, and then click **Settings** sub-tab.



2. Under the Connection section, click to check/uncheck **Auto connect when startup** to allow/disallow automatic virtual private network connection after system startup. When this feature is enabled, select the desired virtual private network through the drop-down menu.

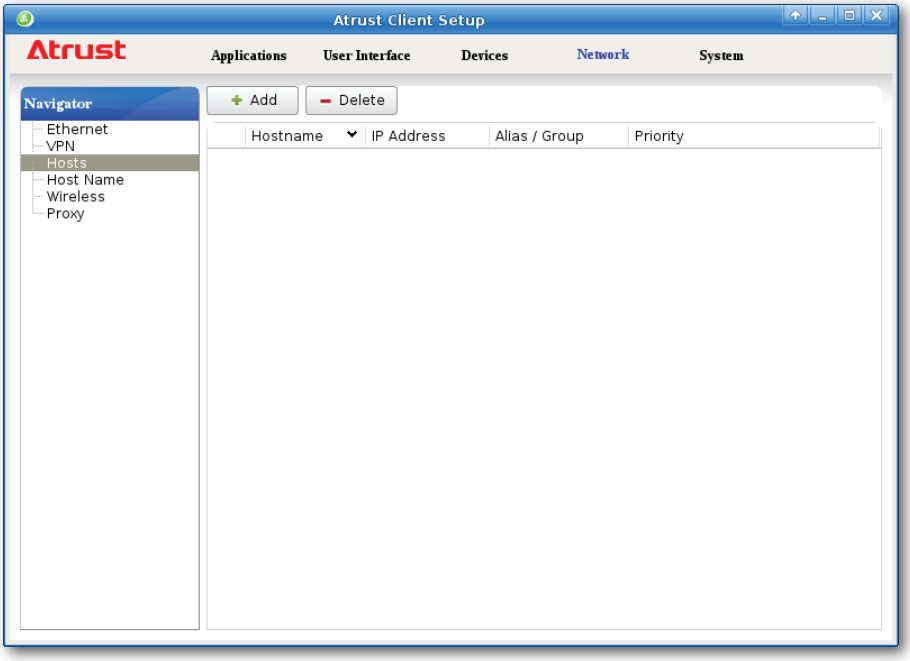
3.5.7 Creating the Mapping of IP Addresses to Names of Hosts

Atrust Client Setup allows you to use the name or alias of a host instead of its IP address wherever you need to specify an IP address while configuring client settings. To use this feature, first you need to create the mapping of IP addresses to names or aliases of hosts.

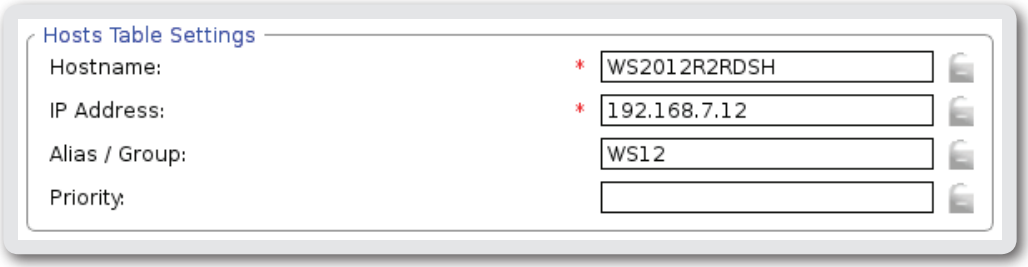
Creating the Mapping List

To create the mapping of IP addresses to names or aliases, please do the following:

1. On Atrust Client Setup, click **Network** > **Hosts** to open the Host list.



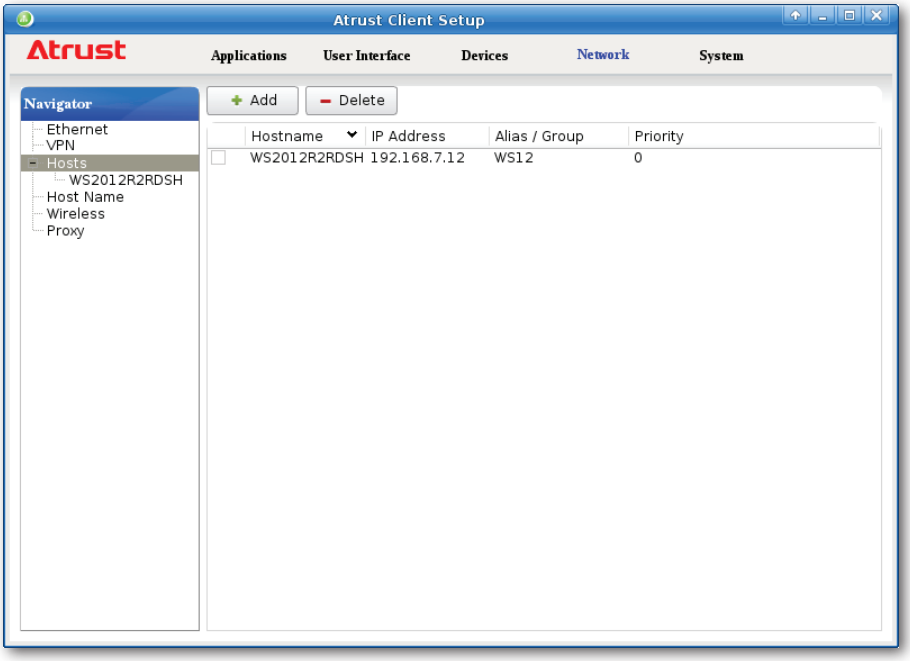
2. Click **Add** to start adding a new host entry.
3. Type in the name, IP address, alias of a host, leave the Priority field blank, and then click **Save** to apply.



NOTE

- If your host belongs to a domain, please don't enter the FQDN (Fully Qualified Domain Name) or ***full*** computer name in the Hostname field. Enter *only* the computer name of the host in this required field.
- You need to type a number in the Priority field ***only when*** creating a Failover Cluster list to allow host failover feature. For details, please refer to "3.5.8 Configuring the Failover Cluster List" on page 116.

4. The newly added entry appears in the Host list.



5. Repeat steps 2 through 3 to add another new entry.
6. Now you can use the name or alias of a host instead of its IP address wherever you need to specify an IP address on Atrust Client Setup while configuring client settings.

Managing the Mapping List

To manage the Mapping list, please do the following:

1. On Atrust Client Setup, click **Network** > **Hosts** to open the Host list.
2. Select to manage entries on the Host list.

   - To adjust the settings of an entry, double click the entry, or check off an entry, and then click the **Edit** button on the top of the Mapping list.
   - To delete an entry, check off the entry, and then click **Delete** on the top of the Mapping list.
   - To delete multiple entries, check off all the desired entries, and then click **Delete**. A window appears prompting for confirmation. Click **Yes** to confirm.

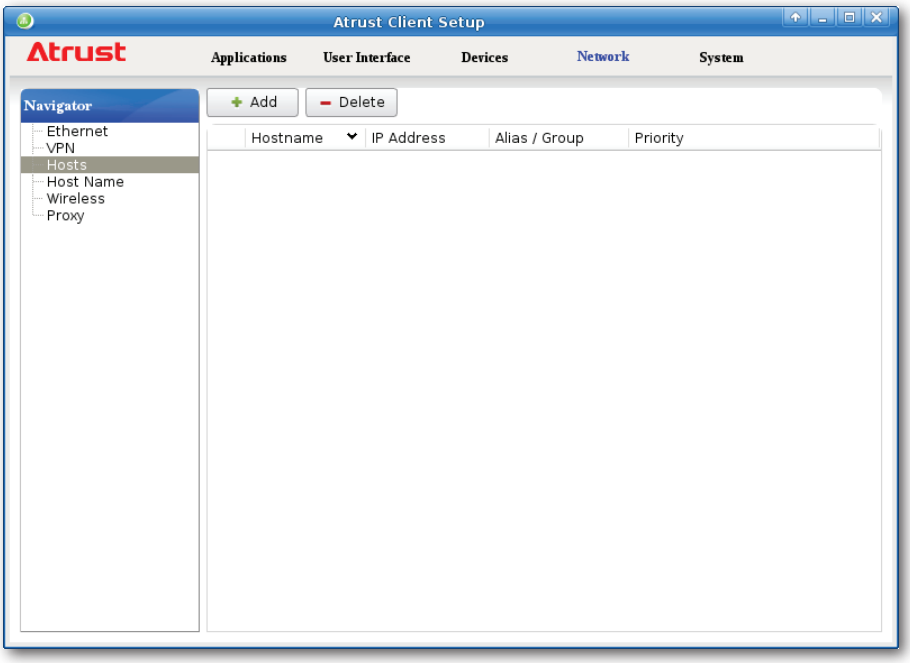
3.5.8 Configuring the Failover Cluster List

Atrust Client Setup allows you to create the Failover Cluster list, maintaining the high availability of services from that group of servers (failover cluster).

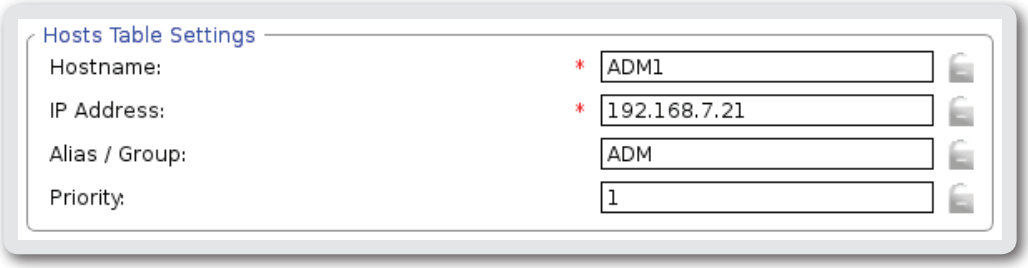
Creating the Failover Cluster List

To create a Failover Cluster list, please do the following:

1. On Atrust Client Setup, click **Network** > **Hosts** to open the Host list.



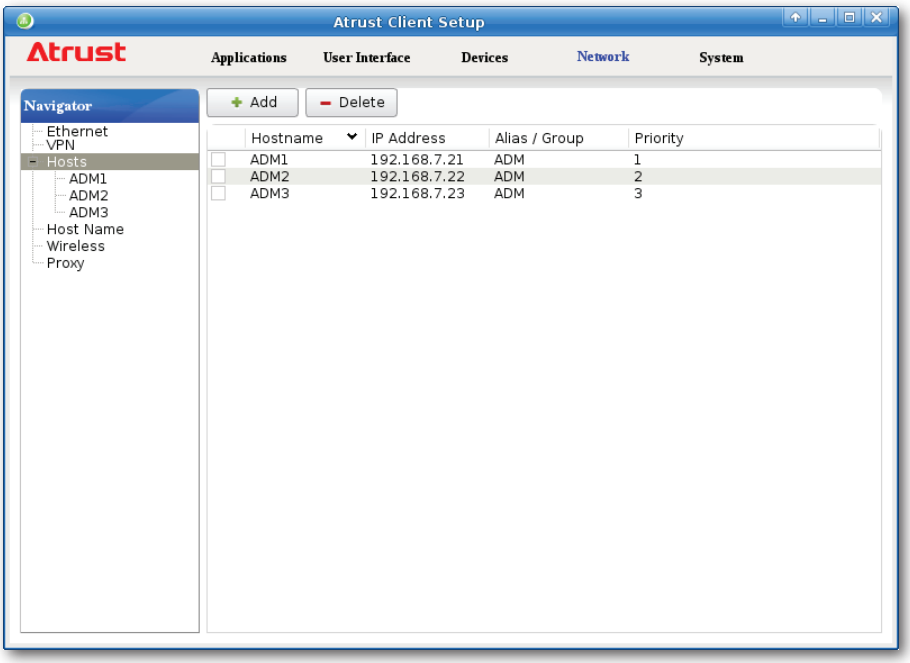
2. Click **Add** to start adding a new host entry.
3. Type in the name, IP address, alias and also cluster (group) name, priority order in the cluster (group), and then click **Save** to apply.



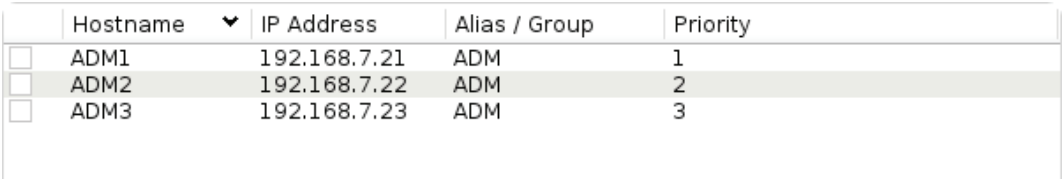
NOTE

- If your host belongs to a domain, please don't enter the FQDN (Fully Qualified Domain Name) or ***full*** computer name in the Hostname field. Enter *only* the computer name of the host in this required field.

4. Repeat steps 2 though 3 to add another new entry.
5. All added entries appear on the Host list.



6. Your mt182L will follow the given priority order while connecting to this failover cluster (group).



Managing the Failover Cluster List

To manage the Host list, please do the following:

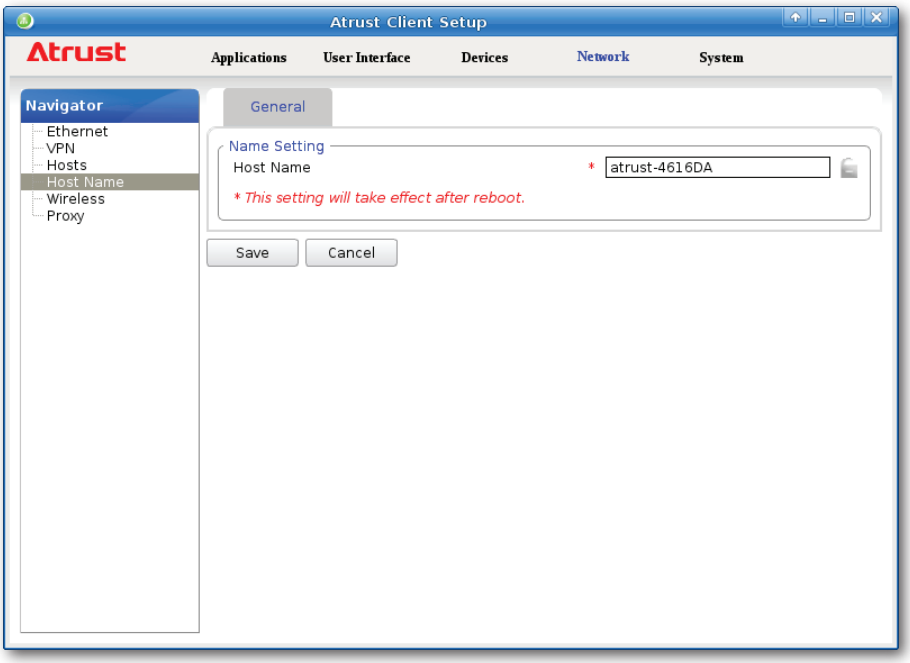
1. On Atrust Client Setup, click **Network** > **Hosts** to open the Host list.
2. Select to manage entries on the Host list.

   - To adjust the settings of an entry, double click the entry, or check off an entry, and then click the **Edit** button on the top of the Host list.
   - To delete an entry, check off the entry, and then click **Delete** on the top of the Host list.
   - To delete multiple entries, check off all the desired entries, and then click **Delete**. A window appears prompting for confirmation. Click **Yes** to confirm.

3.5.9 Changing the Host Name of Your Thin Client

To change the host name of your thin client, please do the following:

1. On Atrust Client Setup, click **Network** > **Host Name**.
2. Change the default host name of your thin client.



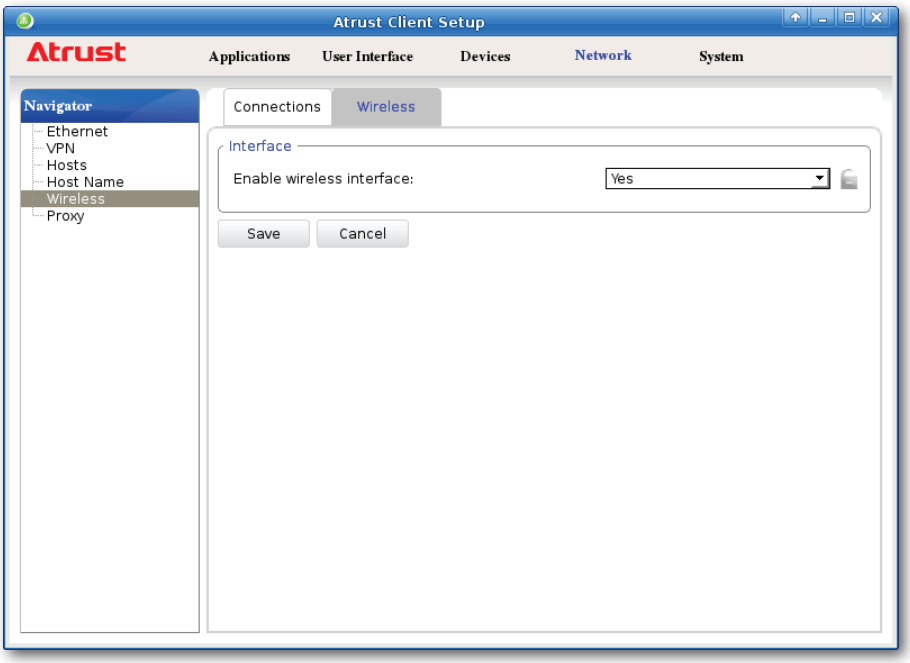
3. Click **Save** to confirm.
4. A restart is required for the change to take effect.

3.5.10 Enabling or Disabling the Wireless Interface

To enable or disable the wireless interface, please do the following:

> **NOTE**
>
> - By default, the wireless interface is ***enabled***.

1. On Atrust Client Setup, click **Network** > **Wireless**, and then click **Wireless** sub-tab.

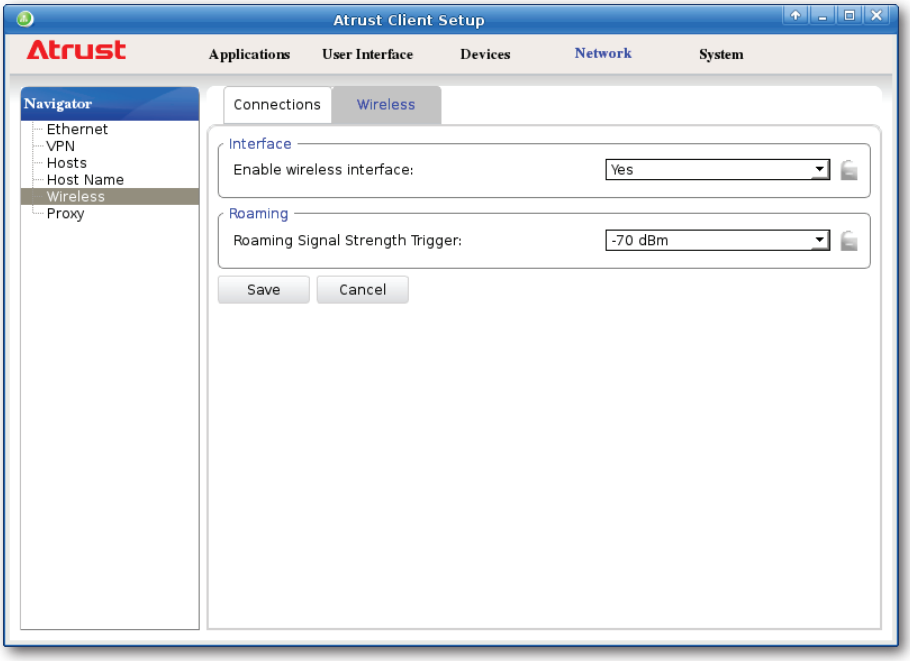


2. Under the Interface section, click the drop-down menu to enable / disable the wireless network interface.
3. Click **Save** to apply.

3.5.11 Configuring the Trigger Threshold for Roaming

To configure the roaming trigger threshold for your wireless connection, please do the following:

1. On Atrust Client Setup, click **Network** > **Wireless**, and then click **Wireless** sub-tab.



2. Under the Roaming section, click the drop-down menu to choose the desired trigger threshold.

> **NOTE**
> - To disable wireless roaming, you can choose **No roaming** here.

3. Click **Save** to apply.

3.5.12 Establishing and Stopping a Wireless Connection

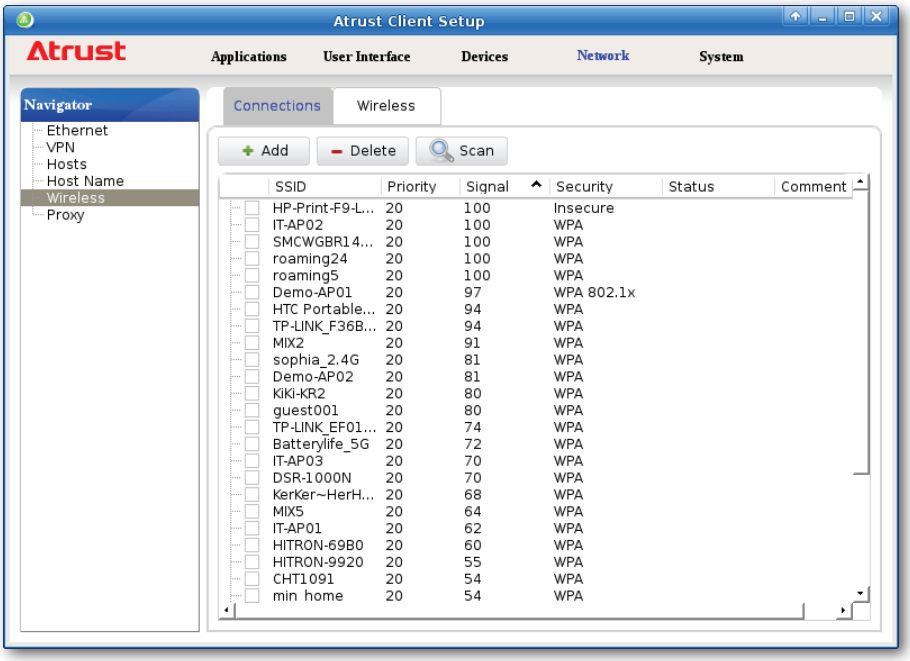
NOTE

- Ensure that the wireless interface is ***enabled***. Please refer to "Enabling or Disabling the Wireless Interface" on page 119.

Establishing a Wireless Network Connection

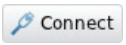
To establish a wireless network connection for your mt182L thin client, please do the following:

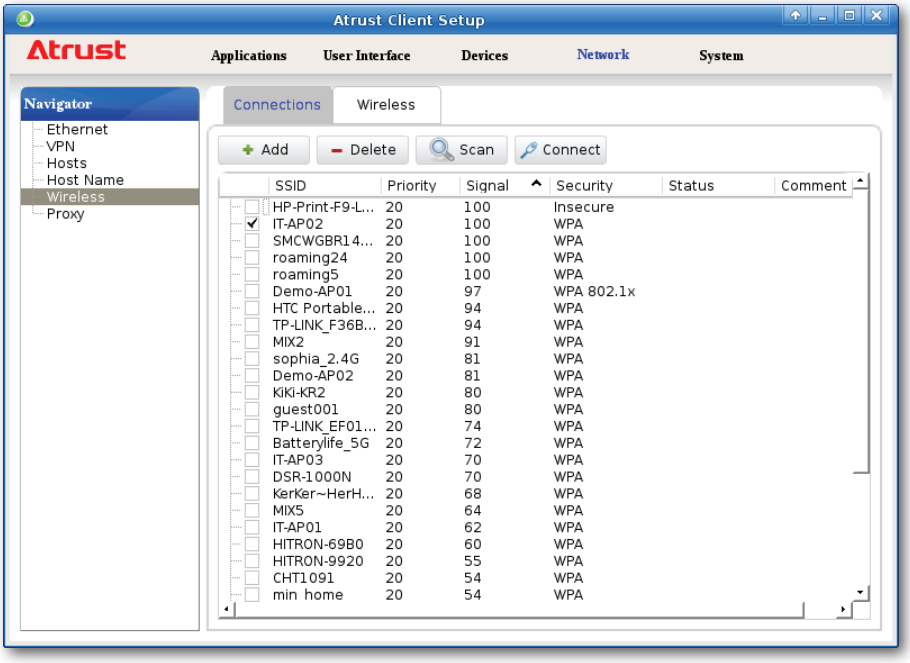
1. On Atrust Client Setup, click **Network** > **Wireless** to open the Wireless Network list.



NOTE

- Your mt182L will perform network discovery ***once*** and specify all available wireless networks. To refresh, click **Scan** on the top of the Wireless Network list.

2. Click to check the desired wireless network. The Connect  button then appears on the top of the Wireless Network list.

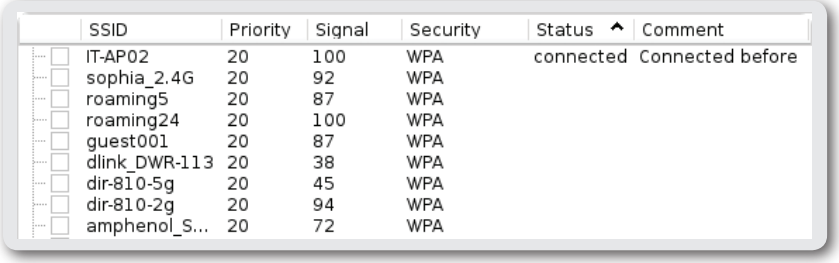


3. Click **Connect** to create a wireless network connection through the selected wireless network.
4. A window appears prompting for confirmation or authentication.

NOTE

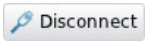
- If you ever accessed this wireless network before, the password will be automatically recorded for future access. In this case, you don't need to provide the password again; you only need to confirm the establishment of a wireless connection.
- Consult your network administrator for required information on authentication.

5. Type in the required password, and then click **Connect** to continue. Or, click **OK** to confirm the establishment of a wireless connection.
6. Upon completion, the Status column of the wireless network will show **connected**.



Stopping a Wireless Network Connection

To stop a wireless network connection, please do the following:

1. On Atrust Client Setup, click **Network** > **Wireless** to open the Wireless Network list.
2. Click to check the desired wireless network. The Disconnect  button appears on the top of the Wireless Network list.
3. Click **Disconnect** to stop the wireless network connection.

Adding a Wireless Network

In case that you cannot find the desired wireless network in the Wireless Network list, you can manually add it.

To add a wireless network to the Wireless Network list, please do the following:

1. On Atrust Client Setup, click **Network** > **Wireless** to open the Wireless Network list.
2. Click **Add** on the top of the Wireless Network list.
3. On the opened window, type the wireless network name (SSID), select the used wireless security method, and then provide the required information.

4. Click **Connect** to create a wireless connection.

NOTE

- For instructions on how to configure the IP address settings, please refer to section "3.5.3 Configuring Wired Network Settings" on page 105.
- The default is to use a dynamic IP address assigned by the DHCP server.

5. Upon completion, the added wireless network will be shown on the Wireless Network list and **connected** will be shown on its Status column.

Deleting a Wireless Network

To delete a wireless network, please do the following:

1. On Atrust Client Setup, click **Network** > **Wireless** to open the Wireless Network list.
2. Click to check the desired wireless network, and then click **Delete** to remove the selected wireless network.

NOTE

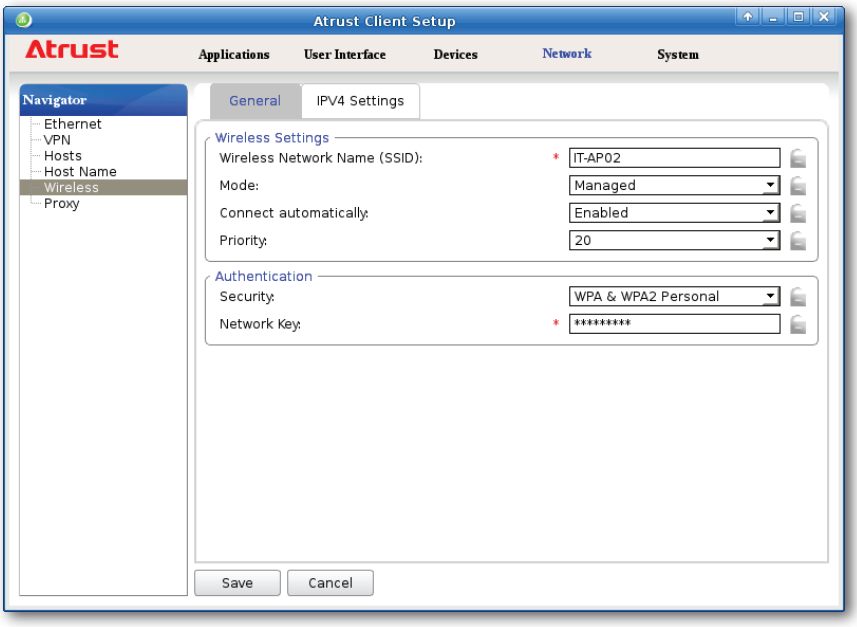
- Your mt182L detects available wireless networks automatically and put the discovered networks on the Wireless Network list. A deleted wireless network may therefore appear again on the list, but the connection settings, including the stored authentication data, will be removed.

3.5.13 Configuring Wireless Connection Settings

To adjust connection settings for a wireless network, please do the following:

1. On Atrust Client Setup, click **Network** > **Wireless** to open the Wireless Network list.
2. Click to check the desired wireless network which is currently connected. The Edit

button appears on the top of the Wireless Network list.
3. Click **Edit** to adjust the settings:



- On the General tab, click the drop-down menu to configure the automatic connection when this wireless network is in range, the priority, and other connection settings.

> **NOTE**
>
> - By default, your client will connect to a wireless network automatically if it ever connected to that network successfully.
> - To connect to wireless networks in order of priority, you can set **Priority**. By default, there is no priority, and the lowest value, **20**, is given for all networks.

- On the IPV4 Settings tab, click the drop-down menu or type values in fields to configure IP settings.

> **NOTE**
>
> - For instructions on how to configure connection settings on the General tab, please see section "3.5.12 Establishing and Stopping a Wireless Connection" on page 121. For instructions on how to configure IP address settings on the IPV4 Settings tab, please see section "3.5.3 Configuring Wired Network Settings" on page 105.

4. Click **Save** to apply.

3.5.14 Configuring Proxy Settings for Web-based Access to Services

To configure proxy settings for Web-based access to services, please do the following:

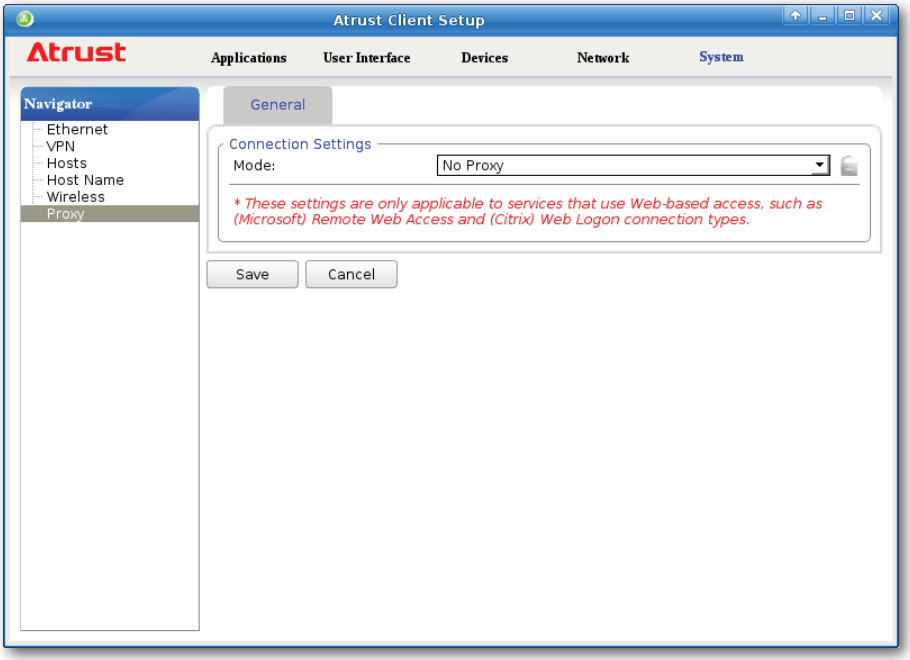
NOTE

- Settings available here are only applicable to services that use Web-based access, such as (Microsoft) Remote Web Access and (Citrix) Web Logon connection types.

1. On Atrust Client Setup, click **Network** > **Proxy**.
2. Click the Mode drop-down menu to select the desired configuration mode. Four modes are available: **No Proxy**, **Auto-detect proxy settings**, **Manual proxy configuration**, and **Auto proxy configuration**.

NOTE

- The setting items will vary with the selected mode.



3. Provide the data as required. Please refer to the following table for a description of each setting item.

<table>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Mode</td><td>Click to select the desired proxy configuration mode.

<table><tr><th>Mode</th><th>Description</th></tr><tr><td>No Proxy</td><td>Don’t use any proxy server.</td></tr><tr><td>Auto-detect proxy settings</td><td>Detects the proxy settings for your network automatically.</td></tr><tr><td>Manual proxy configuration</td><td>Configures the proxy settings manually.</td></tr><tr><td>Auto proxy configuration</td><td>Loads proxy settings automatically through the connection to a proxy configuration file.</td></tr></table></td></tr>
<tr><td colspan="2">Mode: Manual proxy configuration</td></tr>
<tr><td>HTTP Proxy</td><td>Provides the IP address of your HTTP proxy server.</td></tr>
<tr><td>Port</td><td>Provides the port number which your HTTP proxy server uses.</td></tr>
<tr><td>No Proxy for</td><td>Provides No Proxy list.
Don’t use any proxy server while connecting to the specified URLs.</td></tr>
<tr><td colspan="2">Mode: Auto proxy configuration</td></tr>
<tr><td>URL</td><td>Provides the URL of a proxy configuration file where proxy settings can be loaded through the network.</td></tr>
</table>

3.6 Configuring Service Access Settings

3.6.1 Applications Tab Overview

Applications tab enables you to configure settings for service access on clients. To access available settings of **Applications** tab, click the tab on Atrust Client Setup.

Applications Tab Overview

Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **Applications** tab or to select a setting entry under a selected setting item.
2	Configuration area	Configures setting values when a setting item or entry is selected.

3.6.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
Applications	Remote Desktop		Click to configure RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for Remote Desktop sessions.	3.6.3 3.6.4 3.6.5	129 138 144
	Citrix ICA		Click to configure ICA (Independent Computing Architecture) connection settings and create shortcuts on the local desktop and START menu for ICA sessions.	3.6.6 3.6.7 3.6.8 3.6.9 3.6.10 3.6.11	159 172 173 174 175 182
	VMware View		Click to configure VMware View connection settings and create shortcuts on the local desktop and START menu for View sessions.	3.6.12 3.6.13 3.6.14	212 214 216
	SSH		Click to configure SSH (Secure SHell) connection settings and create shortcuts on the local desktop and START menu for SSH sessions.	3.6.15 3.6.16	221 223
	Web Browser		Click to configure settings and create shortcuts on the local desktop and START menu for browser sessions.	3.6.17 3.6.18 3.6.19	224 226 227
	Parallels 2X Client		Click to configure RAS (Remote Application Server) / RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for RAS / RDP sessions.	3.6.20 3.6.21 3.6.22	228 233 235

3.6.3 Configuring Basic RDP Connection Settings

The **Remote Desktop** setting allows you to configure RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for service access. You can access remote desktops or applications for work simply through these shortcuts.

NOTE

- For more information on Microsoft Remote Desktop services, please visit Microsoft website at www.microsoft.com.

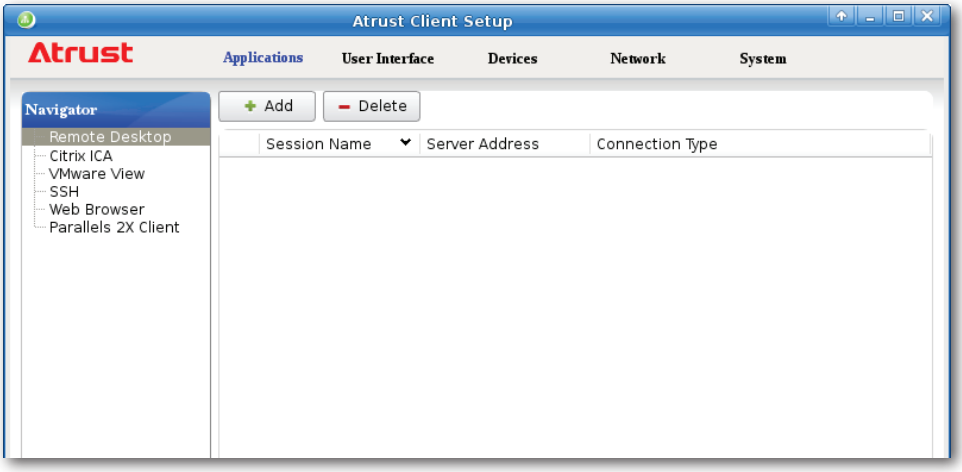
Three connection types are available:

Connection Type	Description	Page
Remote Desktop	Select to access remote desktop/application services.	130
Remote Web Access	Select to access remote application services through a Web browser.	132
Web Feed	Select to access remote application services through published desktop shortcuts.	134

Connection Type: Remote Desktop

To quickly configure RDP connection settings for the Remote Desktop connection type, please do the following:

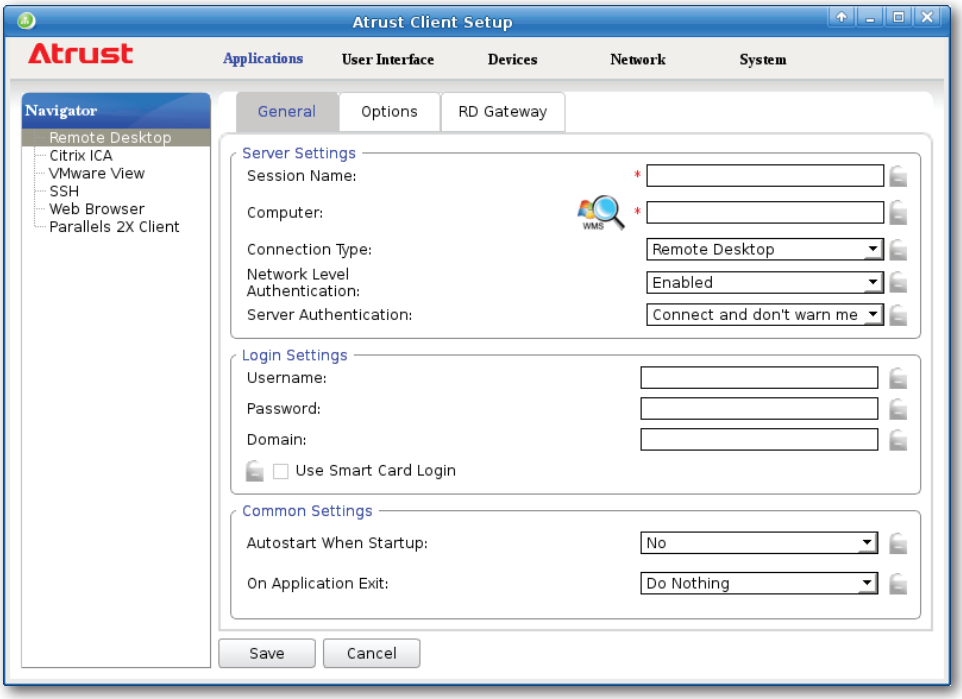
1. On Atrust Client Setup, Click **Applications** > **Remote Desktop**.
2. The RDP Connection list appears in the Configuration area.



NOTE

- If you haven't created any entry, the RDP Connection list will be empty.

3. Click **Add** on the top of the RDP Connection list to create a new entry of RDP connection.



4. On **General** sub-tab, type in the session name and the server/virtual machine address under the Server Settings section.

NOTE

- The red asterisks indicate the required fields.
- The remote service-hosted computer can be a physical server or a virtual machine. Please visit Microsoft's websites at www.microsoft.com or support.microsoft.com for more information.
- mt182L supports up to two Remote Desktop sessions at the same time.
- Windows® RemoteFX™ is the technology that offers a rich user experience over a network for remote desktop users.

NOTE

- To create an entry of RDP connection settings for MultiPoint™ Remote Desktop sessions, please do the following:

  1. In the Server Settings section, click

to start discovering MultiPoint™ Server systems over your network.
  2. In the opened window, click the drop-down menu to select the desired server, and then click **OK** to confirm.
  3. The name and IP address of the selected server will be filled out in the corresponding fields automatically.

- The default session name will be the name of the selected MultiPoint host server, but you still can change the default.
- Windows® MultiPoint™ Server is a shared resource technology. This Windows-based operating system enables a host server to power multiple and independent stations, allowing users to share the computing power of one single server. Based on this operating system, Atrust offers a complete solution including both servers and clients. For more information, please visit our website at www.atrustcorp.com.

5. Click **Save** to add this RDP connection entry.
6. The shortcuts for Remote Desktop services are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced RDP connection settings for service access. For more information on other available settings, please refer to section "3.6.5 Configuring Advanced RDP Connection Settings" on page 144.

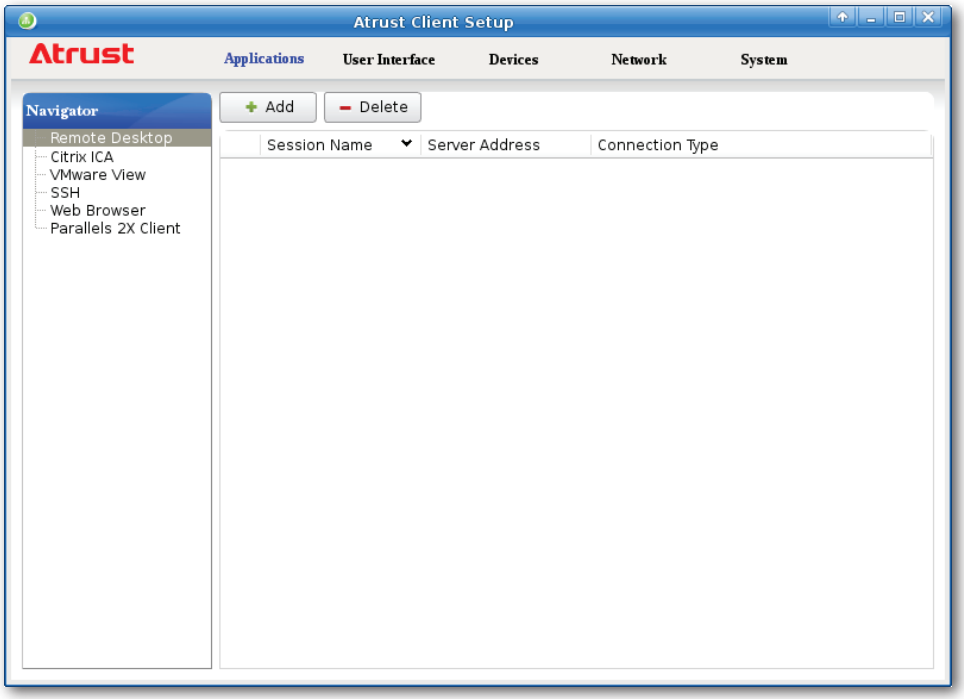
Connection Type: Remote Web Access

To quickly configure RDP connection settings for the Remote Web Access connection type, please do the following:

NOTE

- Atrust mt182L supports only RD Web Access based on Windows Sever 2012 R2; Windows Server 2008 R2 based is not supported.

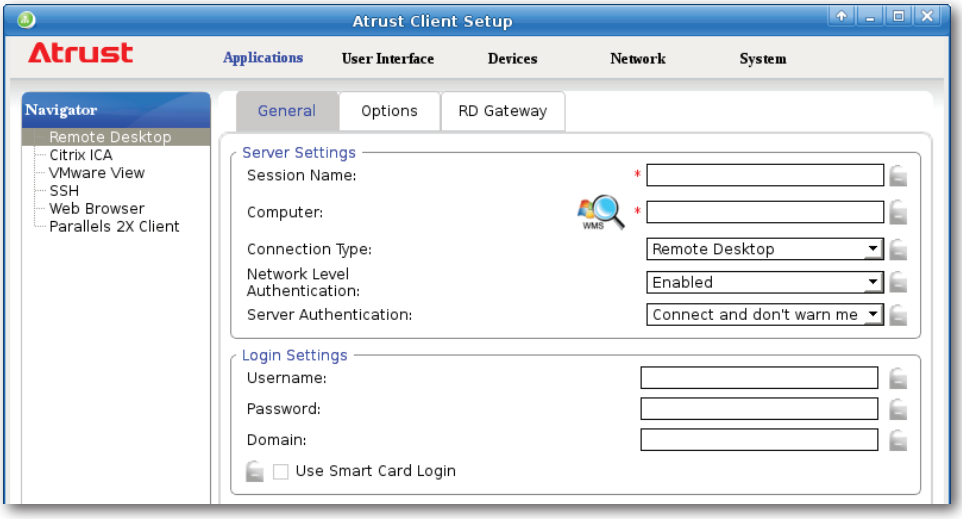
1. On Atrust Client Setup, Click **Applications** > **Remote Desktop**.
2. The RDP Connection list appears in the Configuration area.



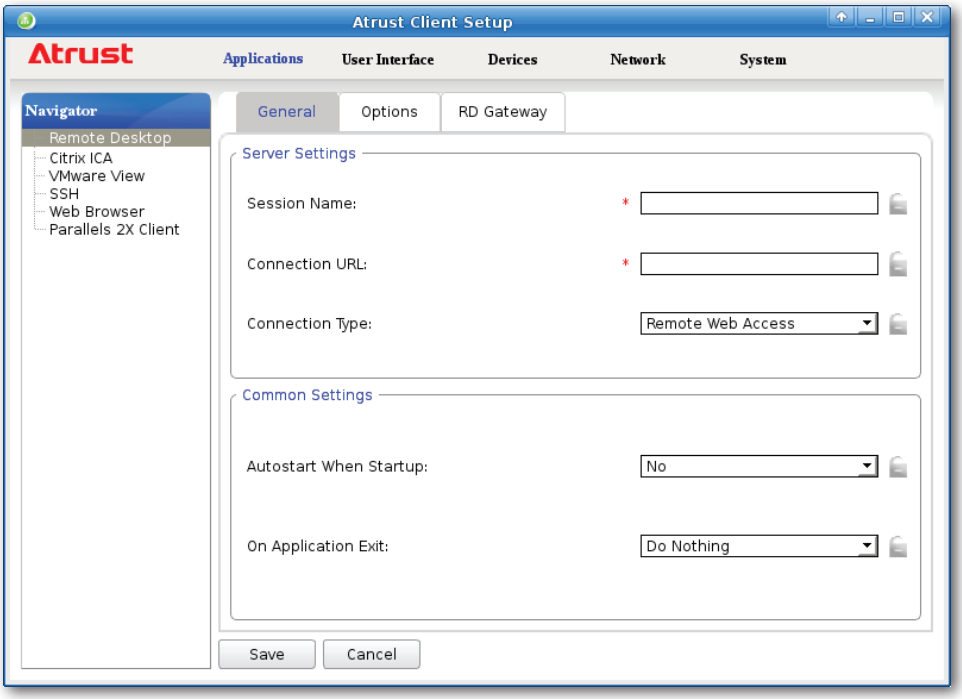
NOTE

- If you haven't created any entry, the RDP Connection list will be empty.

3. Click **Add** on the top of the RDP Connection list to create a new entry of RDP connection.



4. On **General** sub-tab, click the Connection Type drop-down menu to select **Remote Web Access**.



5. Type in the session name and connection URL through which Web-based remote applications is accessible.

> **NOTE**
>
> - The red asterisks indicate the required fields.
> - Consult your IT administrator about the appropriate connection URL.

6. Click **Save** to add this RDP connection entry.
7. The shortcuts for Remote Web Access are automatically created on the local desktop and START menu.

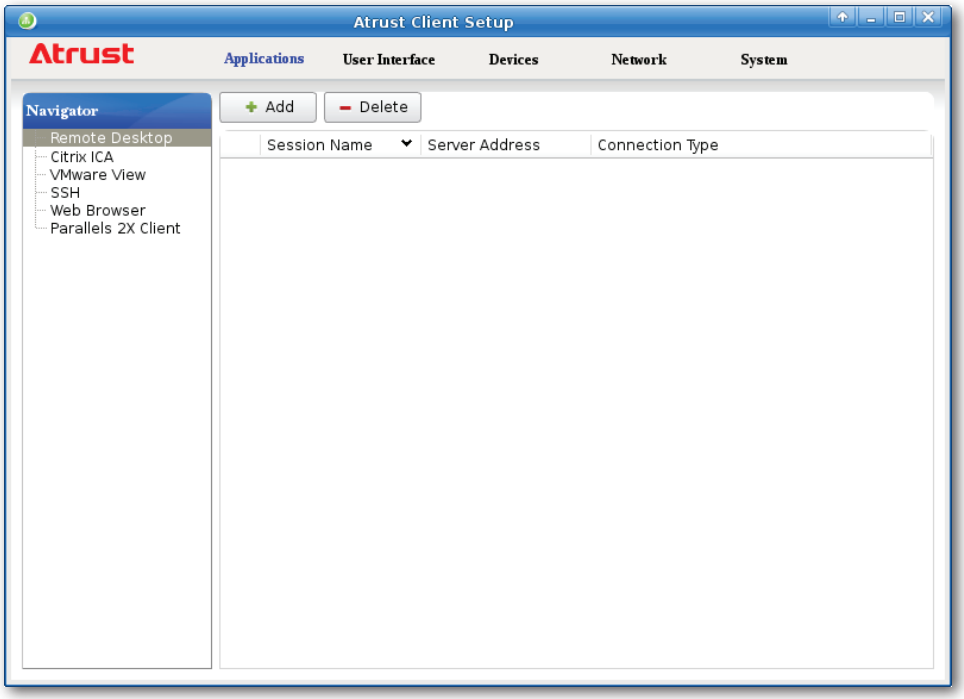
Connection Type: Web Feed

To quickly configure RDP connection settings for the Web Feed connection type, please do the following:

NOTE

- Atrust mt182L supports only RD Web Feed based on Windows Sever 2012 R2; Windows Server 2008 R2 based is not supported.

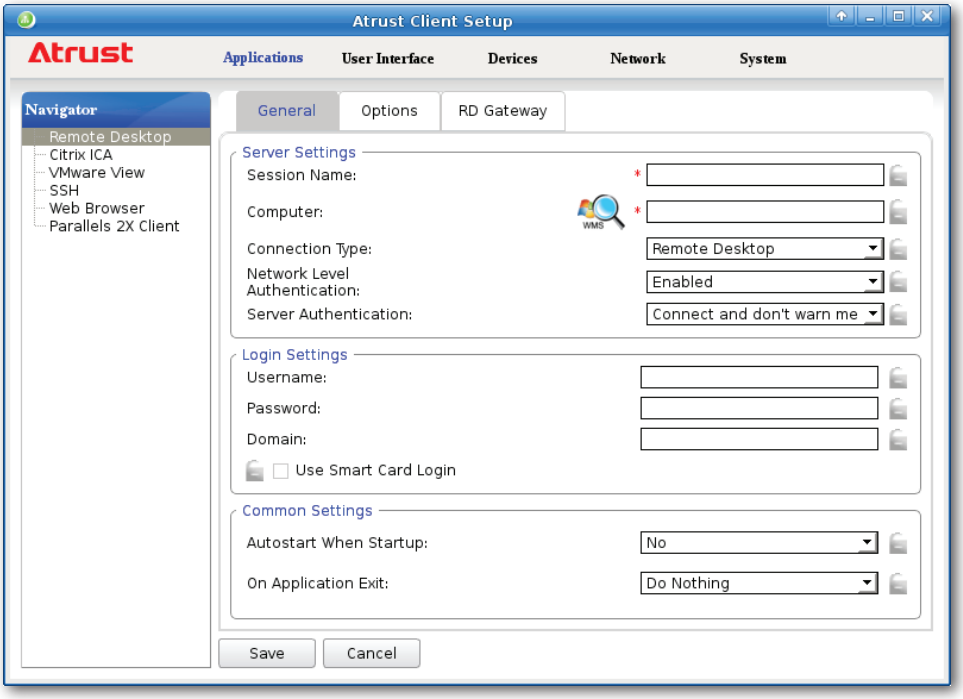
1. On Atrust Client Setup, Click **Applications** > **Remote Desktop**.
2. The RDP Connection list appears in the Configuration area.



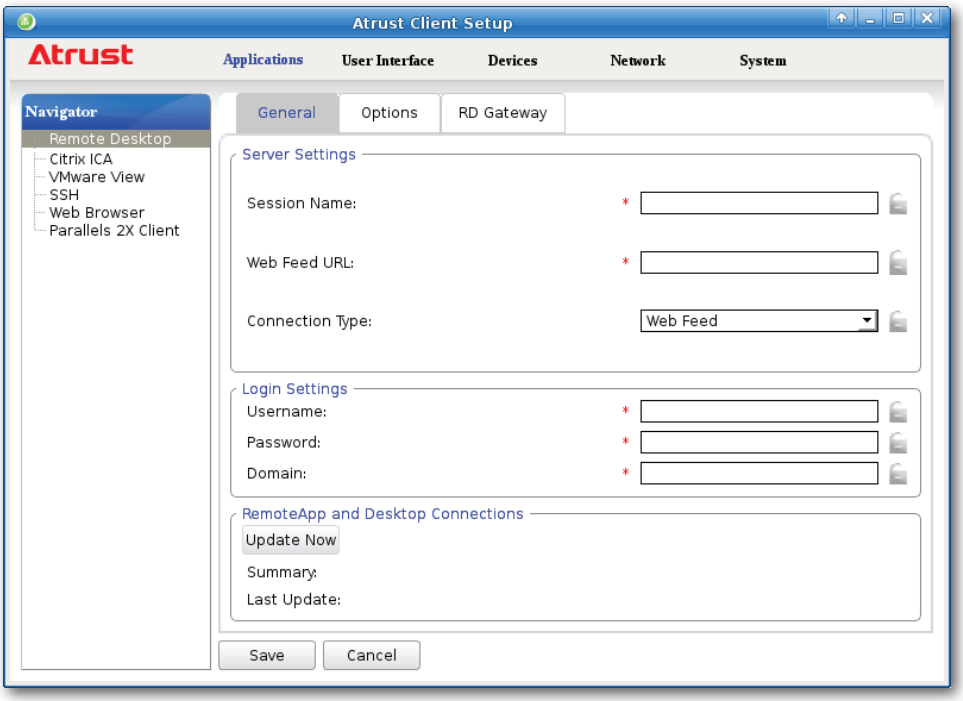
NOTE

- If you haven't created any entry, the RDP Connection list will be empty.

3. Click **Add** on the top of the RDP Connection list to create a new entry of RDP connection.



4. On **General** sub-tab, click the Connection Type drop-down menu to select **Web Feed**.

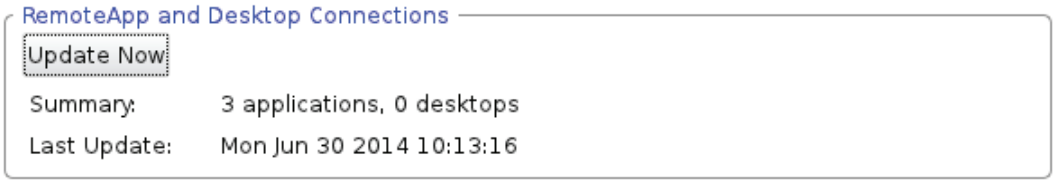


5. Type in the session name, Web Feed URL through which remote applications is accessible, and your credentials for Web Feed.

NOTE

- The red asterisks indicate the required fields.
- Consult your IT administrator about the appropriate Web Feed URL.

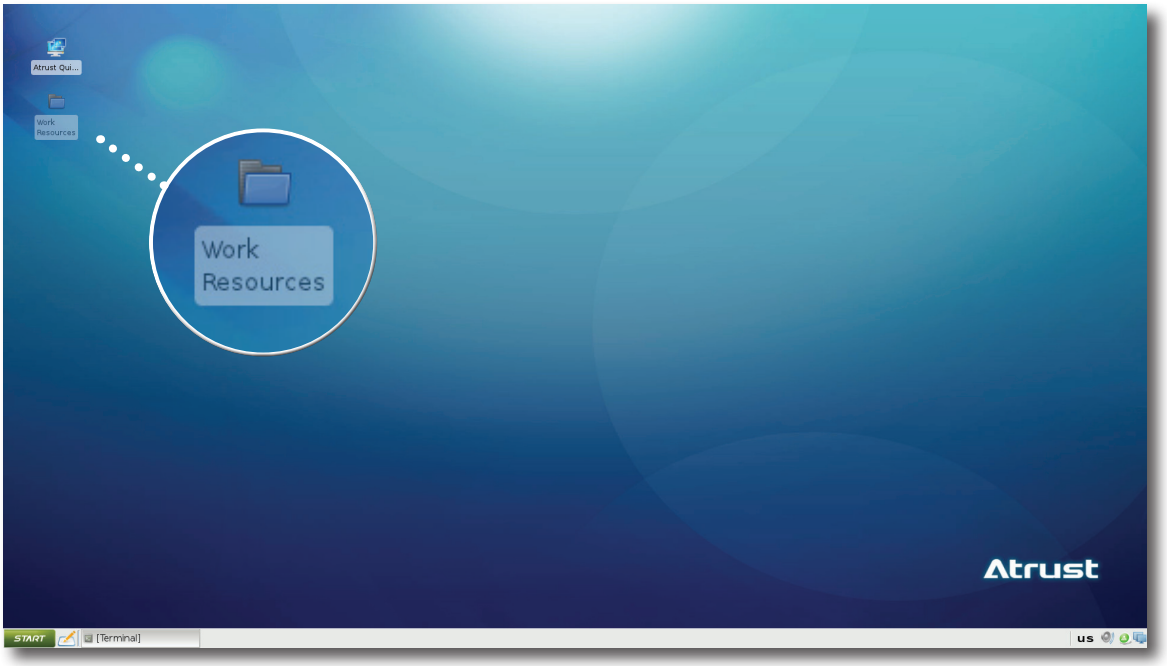
6. Click **Update Now** in the RemoteApp and Desktop Connections section. After completion, the result will be shown as below in that section.



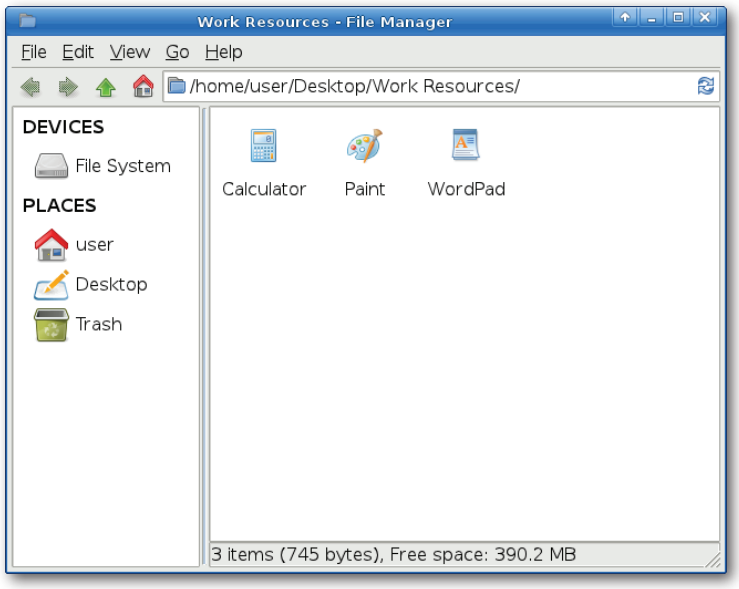
NOTE

- You can and need to use **Update Now** to refresh the Web Feed summary if there are newly published applications. Otherwise, new applications will not be accessible.

7. Click **Save** to add this RDP connection entry.
8. A folder named **Work Resources** with access shortcuts will be automatically created on the local desktop.



9. Access shortcuts for available applications can be found in that folder.



NOTE

- You need to use **Update Now** described in Step 6 to refresh the Web Feed if there are newly published applications. Otherwise, new applications will not be shown.

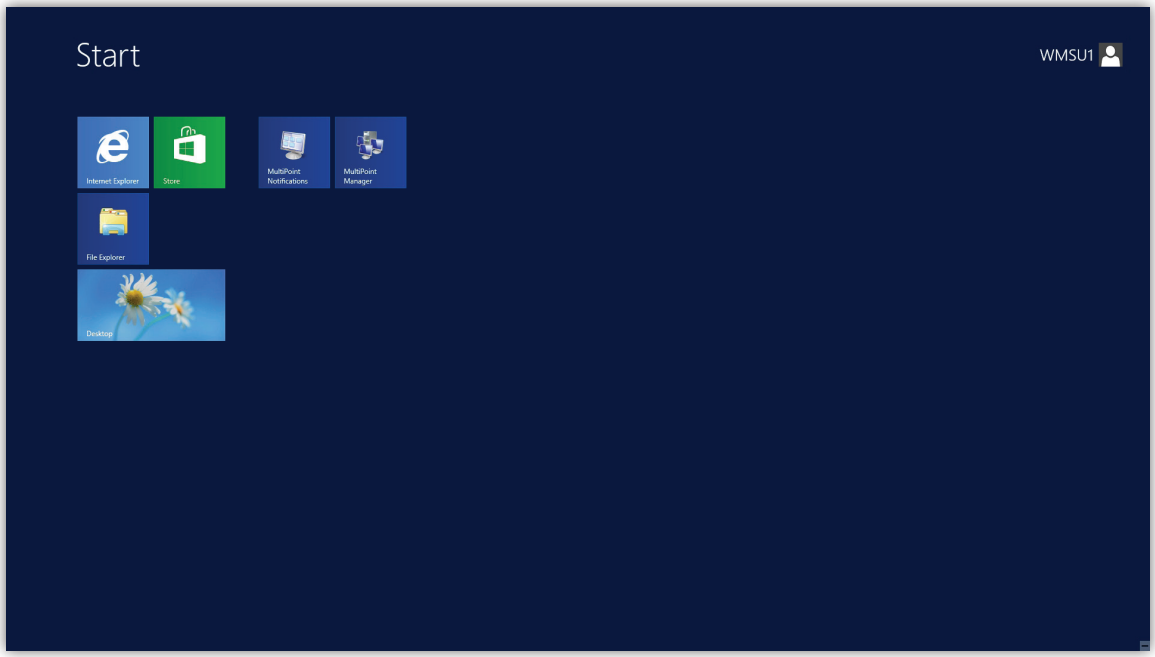
3.6.4 Accessing Remote Desktop Services

Connection Type: Remote Desktop

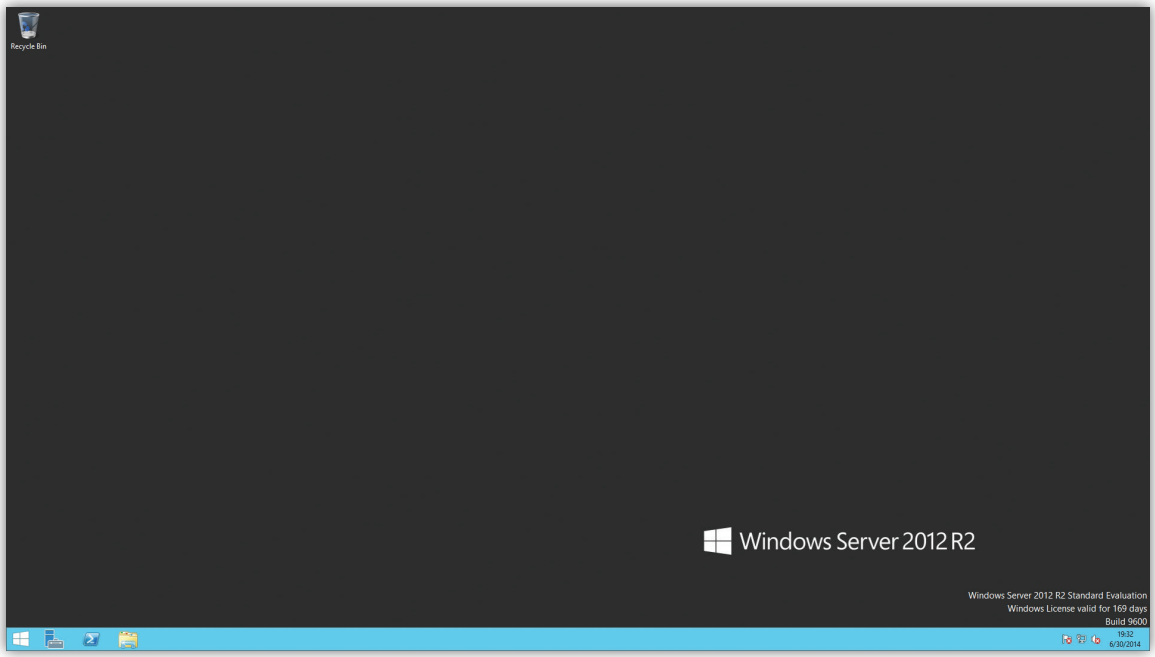
To access remote desktops, please do the following:

1. Double click the created shortcut on the desktop.
2. Follow the on-screen instructions and provide required credentials if needed.
3. The remote desktop will be displayed on the screen.

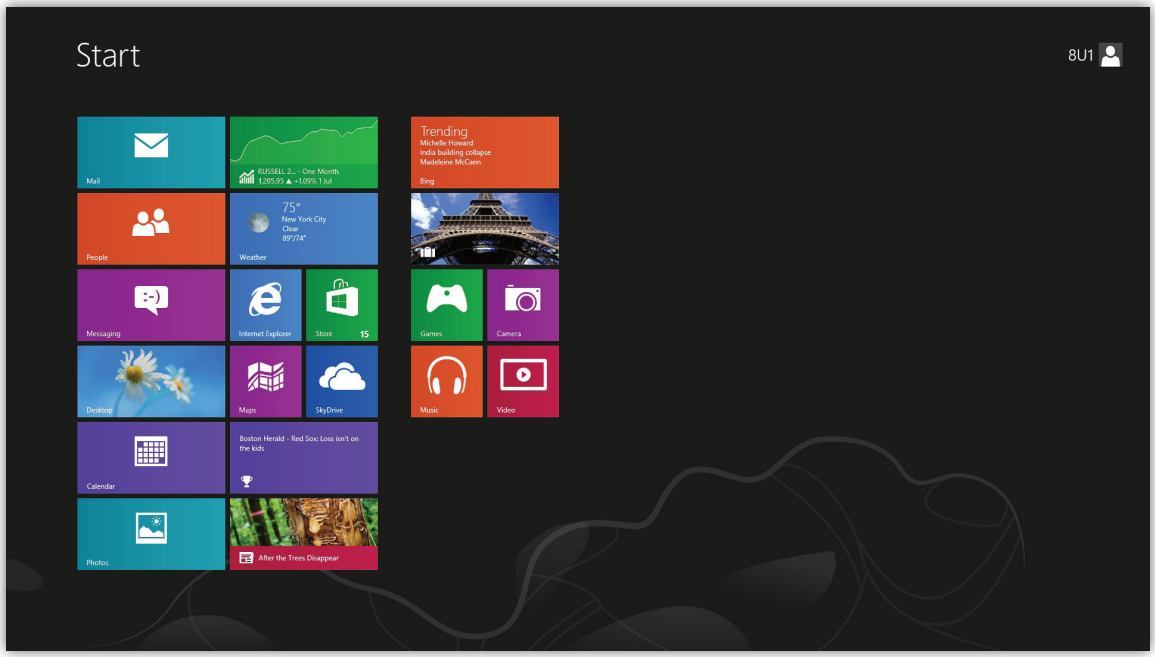
Example: Windows MultiPoint Server 2012



Example: Windows Server 2012



Example: Windows 8 Enterprise



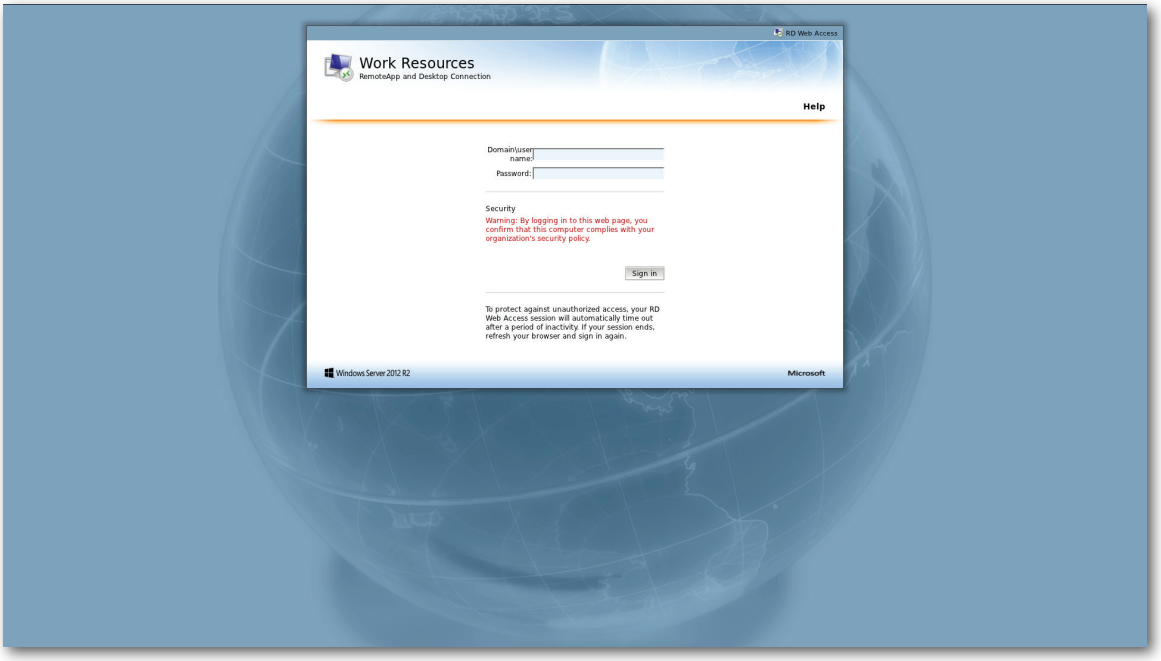
NOTE

- The connection type of Remote Desktop also allow you to launch ***application-only*** sessions; only a specific application is launched rather than a full desktop. For details, please refer to section "3.6.5 Configuring Advanced RDP Connection Settings" on page 144.

Connection Type: Remote Web Access

To access remote applications, please do the following:

1. Double click the created shortcut on the desktop.
2. A window appears prompting for credentials.



NOTE

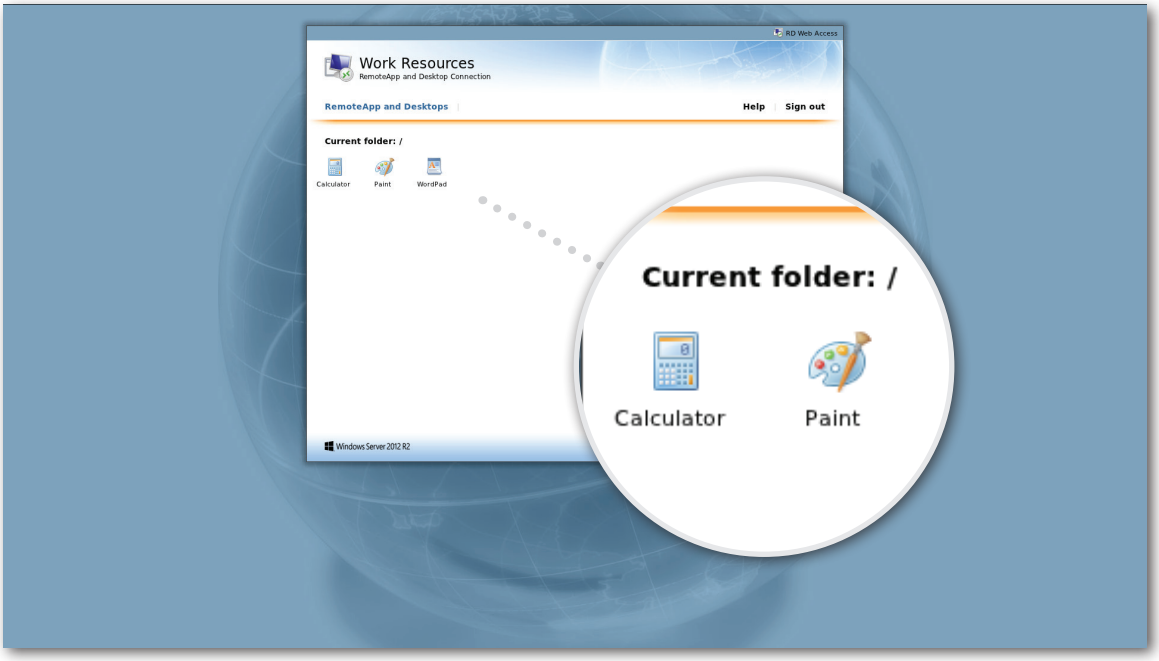
- A warning message "This Connection is Untrusted" might appear. Consult the IT administrator for details and ensure the connection is secure ***first***. To import a security certificate, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73. To bypass, click **I Understand the Risks** > **Add Exception** > **Confirm Security Exception**.

TIP

- To ***exit*** this Logon screen or other screens and return to the local desktop, please press **Alt + F4**.

3. Provide your credentials, and then click **Sign in**.

4. Access shortcuts will be shown on the screen.



5. Click or Double-click to select the desired application.
6. A window appears prompting for credentials.

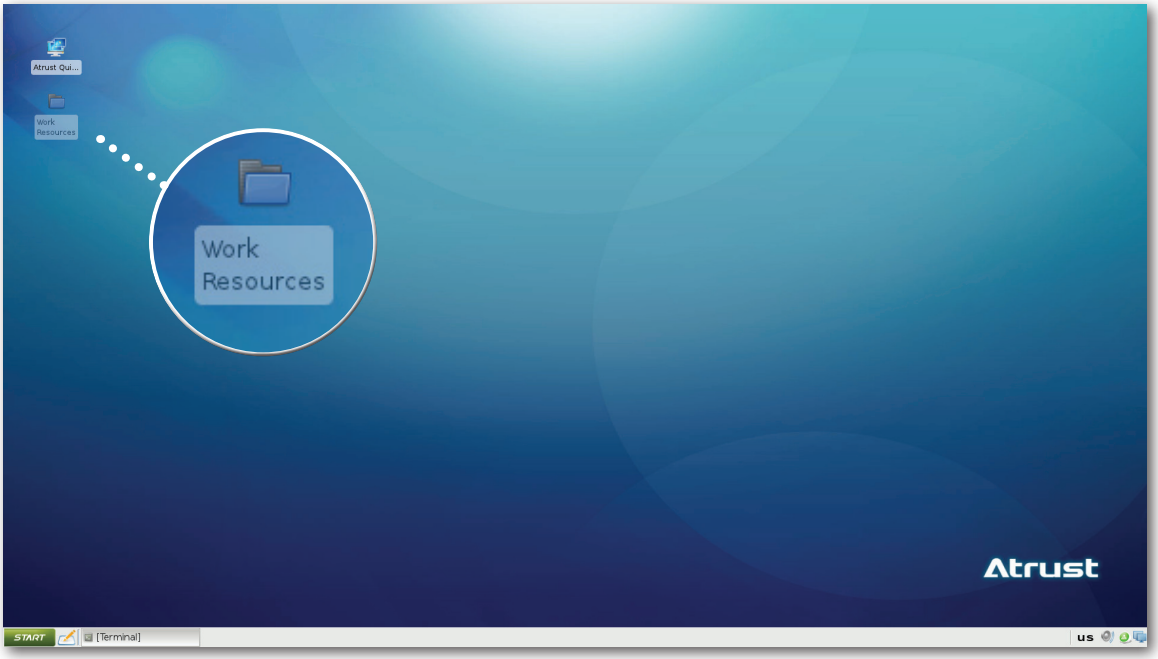
7. Provide your credentials, and then click **OK** to launch the selected application.

TIP

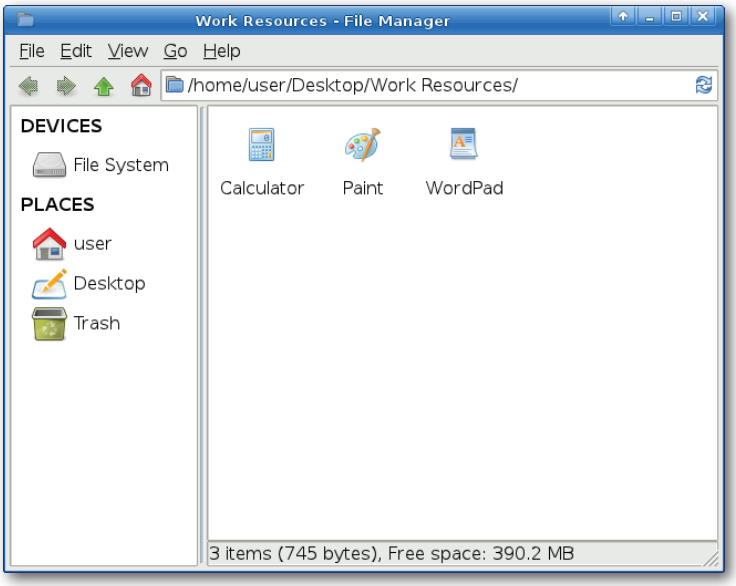
- Use **Alt + Tab** to select and restore a hidden or minimized application or desktop.

Connection Type: Web Feed

1. Double click **Work Resources** folder on the local desktop.



2. Access shortcuts for available applications can be found in that folder.

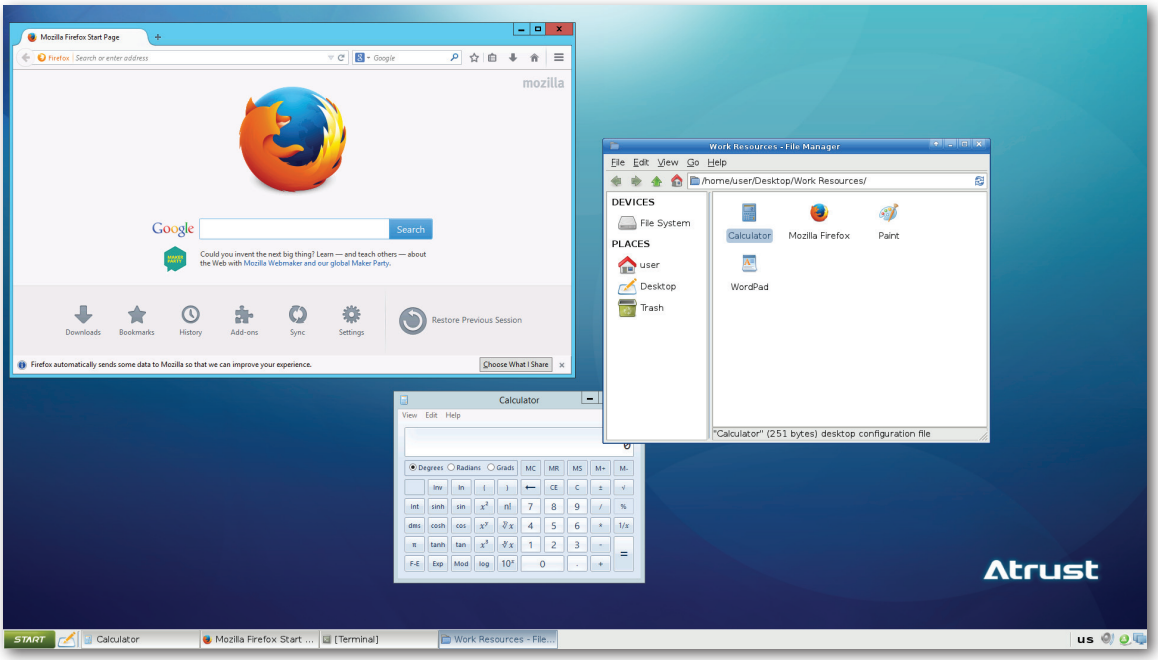


3. Double-click to select the desired application.

4. A window appears prompting for credentials.

5. Provide your credentials, and then click **OK** to launch the selected application.

Remote Application Examples
Mozilla Firefox and Calculator



3.6.5 Configuring Advanced RDP Connection Settings

The tables below provide a description of each setting item for RDP connections. Please refer to these tables to configure advanced settings and customize shortcuts on local desktop and START menu for service access.

NOTE

- Please note that available settings vary with the selected connection type.

Settings for the Connection Type of Remote Desktop

NOTE

- For descriptions of settings for the connection type of Remote Web Access, please refer to "Settings for the Connection Type of Remote Web Access" on page 152.
- For descriptions of settings for the connection type of Web Feed, please refer to "Settings for the Connection Type of Web Feed" on page 155.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Remote Desktop sessions.</td></tr>
<tr><td>Computer</td><td>Type in the computer name or IP address of the server where to deliver a Remote Desktop session.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when Remote Desktop is selected.

Three connection types are available:<table><tr><th>Option</th><th>Description</th></tr><tr><td>Remote Desktop</td><td>Select to access remote desktop/application services.</td></tr><tr><td>Remote Web Access</td><td>Select to access remote application services through a Web browser (Mozilla Firefox).</td></tr><tr><td>Web Feed</td><td>Select to access remote application services through published desktop shortcuts.</td></tr></table></td></tr>
<tr><td>Network Level Authentication</td><td>Select to enable/disable Network Level Authentication.

NOTE: Network Level Authentication is the authentication method used to enhance the server security by requiring that the user be authenticated before the logon screen is displayed and a session is created. This is a more secure authentication method that can help protect the remote computer from malicious users and software.</td></tr>
</table>

<table>
<tr><td>Server Authentication</td><td>Select what to do next if the client cannot verify the identity of the remote computer. Three options are available: Connect and don’t warn me, Warn me, and Do not connect.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Connect and don’t warn me</td><td>Connects anyway without any warning.</td></tr><tr><td>Warn me</td><td>Warns and allows users to choose whether to connect or not.</td></tr><tr><td>Do not connect</td><td>Disallows the connection.</td></tr></table>
NOTE: To import certificates for remote computers, please refer to section “3.2.16 Importing Certificates for Remote Computers” on page 73.</td></tr>
<tr><td colspan="2">Login Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.

NOTE: Domain is a collection of computers on a network that share a common database and security policy. Leave this field blank if the server doesn’t belong to any domain.</td></tr>
<tr><td>Use Smart Card Login</td><td>Check to enable logon with a smart card.</td></tr>
</table>

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>
Select whether to open a Remote Desktop session automatically or not when mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:
<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.
</td></tr>
<tr><td>On Application Exit</td><td>
Select what to do when a Remote Desktop session is ended. Five options are available: Do Nothing, Restart Application, Force-Restart Application, Reboot, and Shutdown.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Returns to the mt182L local Linux desktop.</td></tr>
<tr><td>Restart Application</td><td>Opens a Remote Desktop session again.</td></tr>
<tr><td>Force-Restart Application</td><td>Opens a Remote Desktop session again and skips any messages in-between.</td></tr>
<tr><td>Reboot</td><td>Restarts your mt182L.</td></tr>
<tr><td>Shutdown</td><td>Turns off your mt182L.</td></tr>
</table>
</td></tr>
</table>

Options Sub-tab

<table>
<tr><th colspan="2">Programs</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Start the following program on connection</td><td>Click the drop-down menu to enable or disable the Application mode. Use this option to select the session type. Two remote session types are available:
• Remote Desktop (when the Application mode is disabled)
• Remote Application (when the Application mode is enabled)

NOTE: Remote Application sessions are Remote sessions used to access only specific applications rather than full desktops.

NOTE: Before you can open a Remote Application session, you need to add the desired application to the RemoteApp Programs list with RemoteApp Manager on the host server. For detailed instructions on how to add a desired application to the RemoteApp Programs list on the server, please visit Microsoft's website at www.microsoft.com.</td></tr>
<tr><td>Start in the following folder</td><td>Type in the location of the desired application (on the host server) if Start the following program on connection is enabled.

NOTE: You can type in the location/path of the desired application in this field, and specify only the name of the application in Program path and file name (the next field). Or, you can type in the full path and name of the application in Program path and file name, and leave this field empty.</td></tr>
<tr><td>Program path and file name</td><td>Type in the name of the desired application if Start the following program on connection is enabled.

<table><tr><th>Remote APP</th><th>Format Example</th></tr><tr><td>Windows Media Player</td><td>C:\Programs Files (x86)\Windows Media Player\wmplayer.exe</td></tr><tr><td>Adobe Reader X</td><td>C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32.exe</td></tr><tr><td>Adobe Reader X</td><td>C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32</td></tr></table>
NOTE: the file extension can be omitted.</td></tr>
<tr><th colspan="2">Window Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Color Depth</td><td>Click the drop-down menu to select the desired color depth for a Remote Desktop session. Five options are available: Automatic, 15 Bit, 16 Bit, 24 Bit, and 32 Bit.

NOTE: If RemoteFX is enabled, then no matter which color depth you choose here, 32 bit per pixel will be applied.

NOTE: The Automatic option uses the setting defined by the host server.

NOTE: You can configure the upper limit of the color depth for a Remote Desktop session on the host server. In this case, no matter which color depth you choose here, the value cannot exceed the defined limit.</td></tr>
</table>

<table>
<tr><td>Resolution</td><td>Click the drop-down menu to select the desired display resolution on a Remote Desktop session. Four options are available: Fullscreen, Large Window, Medium Window, and Small Window.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Fullscreen</td><td>Opens a Remote Desktop session in full screen with the same display resolution as the local desktop.</td></tr><tr><td>Large Window</td><td>Opens a Remote Desktop session in a large display resolution.</td></tr><tr><td>Medium Window</td><td>Opens a Remote Desktop session in a medium display resolution.</td></tr><tr><td>Small Window</td><td>Opens a Remote Desktop session in a small display resolution.</td></tr></table>
NOTE: To configure the display resolution of the local desktop, please refer to section “3.3.3 Configuring Display Settings” on page 80.</td></tr>
<tr><td>Use Toolbar</td><td>Click the drop-down menu to select whether to use the Atrust Toolbar on a Remote Desktop session. The tool bar allows you to adjust a session window size or suspend a session.
 </td></tr>
<tr><td>Fullscreen Toggle</td><td>Click the drop-down menu to allow/disallow fullscreen toggle for a remote session by Ctrl + Alt + Enter.</td></tr>
<tr><td>Cursor Auto-hide</td><td>Click the drop-down menu to enable/disable the auto-hiding of the mouse cursor or pointer on inactivity in Remote Desktop sessions.</td></tr>
<tr><td>Use RemoteFX</td><td>Click the drop-down menu to disable/enable RemoteFX.

NOTE: Windows® RemoteFX™ is a technology that offers a rich user experience over a network for remote desktop users.

NOTE: To enable the RemoteFX feature for Remote Desktop sessions on your mt182L thin client, you still need to configure the host server. For detailed instructions on how to enable RemoteFX on a host server, please visit Microsoft Support website at support.microsoft.com.</td></tr>
<tr><td>GFX Preferred Mode</td><td>Click the drop-down menu to select preferred graphics compression methods: RemoteFX, Progressive RemoteFX, or H.264/AVC 444.

NOTE: This setting item is shown only when Use RemoteFX is enabled.</td></tr>
<tr><td>Use Bulk Compression</td><td>Click to enable/disable the bulk compression for the data traffic between the server and client.</td></tr>
</table>

Optimization Settings	
Item	**Description**
Connection Quality	Select the option that best describes the quality of your network connection. Three options are available: **LAN (Very Fast)**, **Broadband (Fast)**, and **Modem (Slow)**. **NOTE:** Selection here will determine the defaults of items in this section as listed below.
Desktop background	Check to use the desktop background.
Font smoothing	Check to use ClearType® technology to make fonts clear and smooth.
Show window contents while dragging	Check to show window contents while dragging a window.
Menu and window animation	Check to show menu and window animation.
Visual styles	Check to allow non-classic themes.
Persistent bitmap caching	Check to allow client-side cache of bitmaps for a session.
Connection Settings	
Item	**Description**
Multimedia Redirection	Click the drop-down menu to disable/enable multimedia redirection. When enabled, the client receives original compressed multimedia streams and decodes locally for display. This feature increases the load on the client, but saves server resources, decreases the bandwidth usage, and improves audio and video playback experiences.
USB Storage Mapping	Click the drop-down menu to enable/disable USB storage mapping. When **Enable** is selected, users can access the local USB storage devices, such as a USB flash drive and memory card reader, in a Remote Desktop session. **NOTE:** Atrust Client Setup also allows you to enable or disable the use of locally attached USB storage devices. You need to enable locally attached USB storage devices first in order to use them in a Remote Desktop session. The default is enabled. **NOTE:** To configure the use of USB storage devices, please refer to section "3.4.3 Configuring Settings for USB Storage Devices" on page 94.
Printer Mapping	Click the drop-down menu to enable/disable printer mapping. When **Enable** is selected, users can access a local or network printer in a Remote Desktop session. **NOTE:** You need to add a local or network printer for your mt182L first, and then enable this feature here to use that printer in a Remote Desktop session. **NOTE:** For detailed instructions on how to add a local or network printer for your mt182L, please refer to section "3.4.8 Adding a Local Printer" on page 99 or "3.4.9 Adding a Network Printer" on page 102.
Serial Port Mapping	Click the drop-down menu to enable/disable serial port mapping. When **Enable** is selected, users can access a serial device, such as a barcode scanner, in a Remote Desktop session.

Parallel Port Mapping	Click the drop-down menu to enable/disable parallel port mapping. When **Enable** is selected, users can access a parallel device, such as a printer or scanner, in a Remote Desktop session.
Smart Card Mapping	Click the drop-down menu to enable/disable smart card mapping. When **Enable** is selected, users can access smart cards through a smart card reader in a Remote Desktop session.
Load Balance Info	Use this field to specify the value for the desired Remote Desktop Services collection if needed.
Server Status Check	Click the drop-down menu to enable/disable connection status check. **NOTE:** Some servers deployed for remote sessions may not support connection status check. Enabling this feature would cause remote sessions disconnected. In this case, disable it to avoid disconnection.
Connection Dialog Settings	
Item	**Description**
Show Connection Information Using	Click the drop-down menu to select what to show for a remote computer in the connection dialog window: **Computer field** or **Session Name field**.
Show Domain Field	Click the drop-down menu to show/hide the domain field in the connection dialog window.
Show Remember Field	Click the drop-down menu to ***show*** or ***hide*** the checkbox **Remember my credentials** on the dialog window.
Local Resources Settings	
Item	**Description**
Remote Audio Playback	Click the drop-down menu to configure the audio playback setting in a Remote Desktop session. Three options are available: **Play on this computer**, **Play on remote computer**, and **Do not play**.

Option	Description
Play on this computer	Allows audio playback in a Remote Desktop session using locally attached audio devices.
Play on remote computer	Allows audio playback in a Remote Desktop session using audio devices attached to the remote computer.
Do not play	Disables audio playback in a Remote Desktop session using locally attached audio devices.

<table>
<tr><td>Remote Audio Recording</td><td>Click the drop-down menu to configure the audio playback setting in a Remote Desktop session. Two options are available: Recording from this computer and Do not record.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Recording from this computer</td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr><tr><td>Do not record</td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr></table></td></tr>
<tr><th colspan="2">RemoteFX USB Redirection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Use RemoteFX USB Redirection</td><td>Check/Uncheck to enable/disable locally attached USB devices in a Remote Desktop session (virtual machine based only).

NOTE: RemoteFX USB Redirection allows the redirection of USB devices into server-hosted virtual machines (with guest operating systems).

NOTE: RemoteFX USB Redirection is only applicable to the virtual machine based Remote Desktop service not to session based one. For more information, please visit Microsoft Support website at support.microsoft.com.

On the client side, please do the following to enable locally attached USB devices in a virtual machine based desktop:

1. Ensure that the desired USB device has been connected to your client.
2. Ensure that RemoteFX is enabled on your mt182L (see “Use RemoteFX” on page 148).
3. Click to check Use RemoteFX USB Redirection.
4. A new checkbox appears with the required device driver. Check to enable the driver.
5. Click Save to apply.

NOTE: You also need to configure the host server and its guest OSs to enable RemoteFX USB Redirection in a Remote Desktop session. For instructions on server-side configuration, please visit Microsoft Support website at support.microsoft.com.</td></tr>
</table>

RD Gateway Sub-tab

Connection Settings	
Item	**Description**
Use RD Gateway server	Check/Uncheck to enable/disable the use of an RD Gateway server. When checked, the following two items in this table appear.
Server Name	Type the name of the RD Gateway server. Ask the network administrator for this information.
Use my Remote Desktop credentials for the RD Gateway	Check to use the same set of credentials for authenticating to both the Remote Desktop computer and the RD Gateway server.
Bypass RD Gateway for local address	Check to prevent traffic to and from local network addresses from being routed through the RD Gateway server. This could make your RDP connection faster.

Settings for the Connection Type of Remote Web Access

NOTE

- For descriptions of settings for the connection type of Remote Desktop, please refer to "Settings for the Connection Type of Remote Desktop" on page 144.
- For descriptions of settings for the connection type of Web Feed, please refer to "Settings for the Connection Type of Web Feed" on page 155.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Remote Web Access sessions.</td></tr>
<tr><td>Connection URL</td><td>Type in the URL of the server where to deliver Remote Web Access sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when Remote Web Access is selected.

Three connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Remote Desktop</td><td>Select to access remote desktop/application services.</td></tr><tr><td>Remote Web Access</td><td>Select to access remote application services through a Web browser (Mozilla Firefox).</td></tr><tr><td>Web Feed</td><td>Select to access remote application services through published desktop shortcuts.</td></tr></table></td></tr>
</table>

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>
Select whether to open a Remote Web Access session automatically or not when mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.
</td></tr>
<tr><td>On Application Exit</td><td>
Select what to do when a Remote Web Access session is ended. Five options are available: Do Nothing, Restart Application, Force-Restart Application, Reboot, and Shutdown.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Returns to the mt182L local Linux desktop.</td></tr>
<tr><td>Restart Application</td><td>Opens a Remote Web Access session again.</td></tr>
<tr><td>Force-Restart Application</td><td>Opens a Remote Web Access session again and skips any messages in-between.</td></tr>
<tr><td>Reboot</td><td>Restarts your mt182L.</td></tr>
<tr><td>Shutdown</td><td>Turns off your mt182L.</td></tr>
</table>
</td></tr>
</table>

Options Sub-tab

NOTE

- No settings are available under the **Options** sub-tab in the connection type of Remote Web Access.

RD Gateway Sub-tab

NOTE

- No options are available under the **RD Gateway** sub-tab in the connection type of Remote Web Access.

Settings for the Connection Type of Web Feed

NOTE

- For descriptions of settings for the connection type of Remote Desktop, please refer to "Settings for the Connection Type of Remote Desktop" on page 144.
- For descriptions of settings for the connection type of Remote Web Access, please refer to "Settings for the Connection Type of Remote Web Access" on page 152.

General Sub-tab

Server Settings	
Item	**Description**
Session Name	Type in the name for Web Feed sessions.
Web Feed URL	Type in the URL of the server where to deliver Web Feed sessions.
Connection Type	This table only provides descriptions for available settings when **Web Feed** is selected. Three connection types are available: **Option** / **Description** Remote Desktop — Select to access remote desktop/application services. Remote Web Access — Select to access remote application services through a Web browser (Mozilla Firefox). Web Feed — Select to access remote application services through published desktop shortcuts.
Login Settings	
Item	**Description**
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server.
RemoteApp and Desktop Connections	
Item	**Description**
Update Now	Click to fetch and update the published applications list from the server.

Options Sub-tab

Window Settings	
Item	**Description**
Color Depth	Click the drop-down menu to select the desired color depth for a Remote Desktop session. Five options are available: **Automatic**, **15 Bit**, **16 Bit**, **24 Bit**, and **32 Bit**. **NOTE:** If RemoteFX is enabled, then no matter which color depth you choose here, 32 bit per pixel will be applied. **NOTE:** The **Automatic** option uses the setting defined by the host server. **NOTE:** You can configure the upper limit of the color depth for a Remote Desktop session on the host server. In this case, no matter which color depth you choose here, the value cannot exceed the defined limit.
Cursor Auto-hide	Click the drop-down menu to enable/disable the auto-hiding of the mouse cursor or pointer on inactivity in Remote Desktop sessions.
Use RemoteFX	Click the drop-down menu to disable/enable RemoteFX. **NOTE:** Windows® RemoteFX™ is a technology that offers a rich user experience over a network for remote desktop users. **NOTE:** To enable the RemoteFX feature for Remote Desktop sessions on your mt182L thin client, you still need to configure the host server. For detailed instructions on how to enable RemoteFX on a host server, please visit Microsoft Support website at support.microsoft.com.
Use Bulk Compression	Click to enable/disable the bulk compression for the data traffic between the server and client.
Connection Settings	
Item	**Description**
USB Storage Mapping	Click the drop-down menu to enable/disable USB storage mapping. When **Enable** is selected, users can access the local USB storage devices, such as a USB flash drive and memory card reader, in a Remote Desktop session. **NOTE:** Atrust Client Setup also allows you to enable or disable the use of locally attached USB storage devices. You need to enable locally attached USB storage devices first in order to use them in a Remote Desktop session. The default is enabled. **NOTE:** To configure the use of USB storage devices, please refer to section "3.4.3 Configuring Settings for USB Storage Devices" on page 94.
Printer Mapping	Click the drop-down menu to enable/disable printer mapping. When **Enable** is selected, users can access a local or network printer in a Remote Desktop session. **NOTE:** You need to add a local or network printer for your mt182L first, and then enable this feature here to use that printer in a Remote Desktop session. **NOTE:** For detailed instructions on how to add a local or network printer for your mt182L, please refer to section "3.4.8 Adding a Local Printer" on page 99 or "3.4.9 Adding a Network Printer" on page 102.

Serial Port Mapping	Click the drop-down menu to enable/disable serial port mapping. When **Enable** is selected, users can access a serial device, such as a barcode scanner, in a Remote Desktop session.
Parallel Port Mapping	Click the drop-down menu to enable/disable parallel port mapping. When **Enable** is selected, users can access a parallel device, such as a printer or scanner, in a Remote Desktop session.
Smart Card Mapping	Click the drop-down menu to enable/disable smart card mapping. When **Enable** is selected, users can access smart cards through a smart card reader in a Remote Desktop session.
Load Balance Info	Use this field to specify the value for the desired Remote Desktop Services collection if needed.
Server Status Check	Click the drop-down menu to enable/disable connection status check. **NOTE:** Some servers deployed for remote sessions may not support connection status check. Enabling this feature would cause remote sessions disconnected. In this case, disable it to avoid disconnection.
Connection Dialog Settings	
Show Connection Information Using	Click the drop-down menu to select what to show for a remote computer in the connection dialog window: **Computer field** or **Session Name field**.
Show Domain Field	Click the drop-down menu to show/hide the domain field in the connection dialog window.
Show Remember Field	Click the drop-down menu to ***show*** or ***hide*** the checkbox **Remember my credentials** on the dialog window.
Local Resources Settings	
Item	**Description**
Remote Audio Playback	Click the drop-down menu to configure the audio playback setting in a Remote Desktop session. Three options are available: **Play on this computer**, **Play on remote computer**, and **Do not play**.

Option	Description
Play on this computer	Allows audio playback in a Remote Desktop session using locally attached audio devices.
Play on remote computer	Allows audio playback in a Remote Desktop session using audio devices attached to the remote computer.
Do not play	Disables audio playback in a Remote Desktop session using locally attached audio devices.

<table>
<tr><td>Remote Audio Recording</td><td>Click the drop-down menu to configure the audio playback setting in a Remote Desktop session. Two options are available: Recording from this computer and Do not record.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Recording from this computer</td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr><tr><td>Do not record</td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr></table></td></tr>
<tr><td colspan="2">RemoteFX USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Use RemoteFX USB Redirection</td><td>Check/Uncheck to enable/disable locally attached USB devices in a Remote Desktop session (virtual machine based only).

NOTE: RemoteFX USB Redirection allows the redirection of USB devices into server-hosted virtual machines (with guest operating systems).

NOTE: RemoteFX USB Redirection is only applicable to the virtual machine based Remote Desktop service not to session based one. For more information, please visit Microsoft Support website at support.microsoft.com.

On the client side, please do the following to enable locally attached USB devices in a virtual machine based desktop:

1. Ensure that the desired USB device has been connected to your mt182L.
2. Ensure that RemoteFX is enabled on your mt182L (see “Use RemoteFX” on page 148).
3. Click to check Use RemoteFX USB Redirection.
4. A new checkbox appears with the required device driver. Check to enable the driver.
5. Click Save to apply.

NOTE: You also need to configure the host server and its guest OSs to enable RemoteFX USB Redirection in a Remote Desktop session. For instructions on server-side configuration, please visit Microsoft Support website at support.microsoft.com.</td></tr>
</table>

RD Gateway Sub-tab

NOTE

- No options are available under the **Options sub**-tab in the connection type of Web Logon.

3.6.6 Configuring Basic ICA Connection Settings

The **Citrix ICA** setting allows you to configure ICA connections for Citrix services and create shortcuts on the local desktop and START menu for service access. You can access virtual desktops and applications for work simply through these shortcuts.

NOTE

- For more information on Citrix desktop virtualization solutions, please visit Citrix website at www.citrix.com or Citrix Knowledge Center at support.citrix.com.

Six connection types are available:

Connection Type	Description	Page
Web Logon	Select to access desktop/application services through a Web browser.	160
StoreFront	Select to access desktop/application services through a StoreFront.	162
VDI-in-a-Box	Select to access desktop services through VDI-in-a-Box.	164
XenDesktop	Select to access desktop services through an earlier version of XenDesktop.	166
XenApp	Select to access application services through an earlier version of XenApp.	168
Server Connection	Select to access service delivery servers (XenApp servers only).	170

NOTE

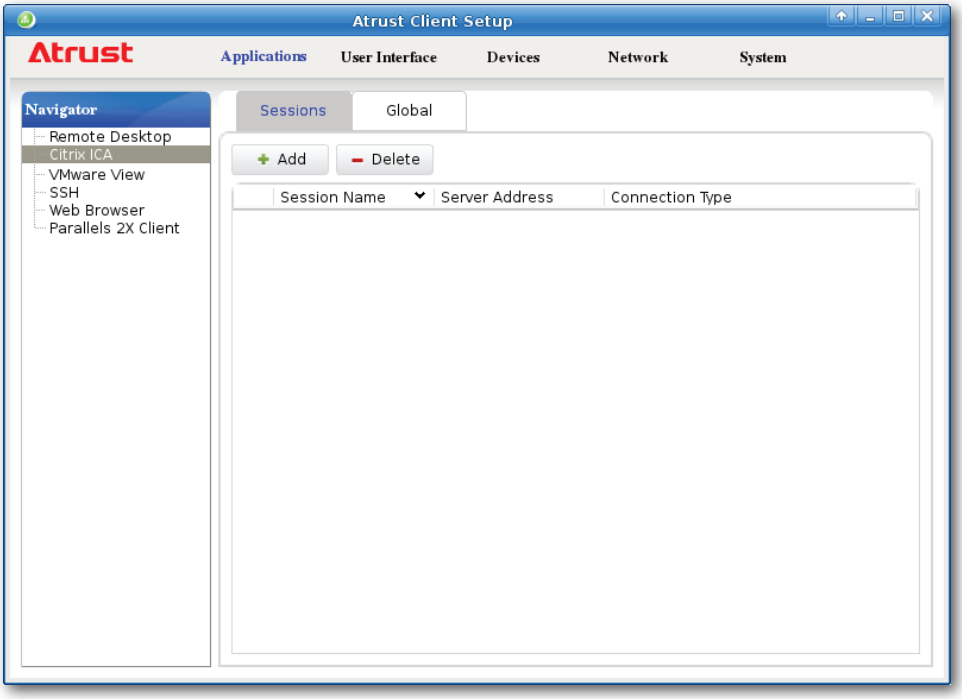
- You can refer to the following table for Citrix products and recommended connection types:

Citrix Product	Recommended Connection Type
XenApp 6.5 or earlier	XenApp / Web Logon
XenDesktop 5.6 or earlier	XenDesktop / Web Logon
Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)	StoreFront / Web Logon
VDI-in-a-Box	VDI-in-a-Box / Web Logon

Connection Type: Web Logon

To quickly configure ICA connection settings for the Web Logon connection type, please do the following:

1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

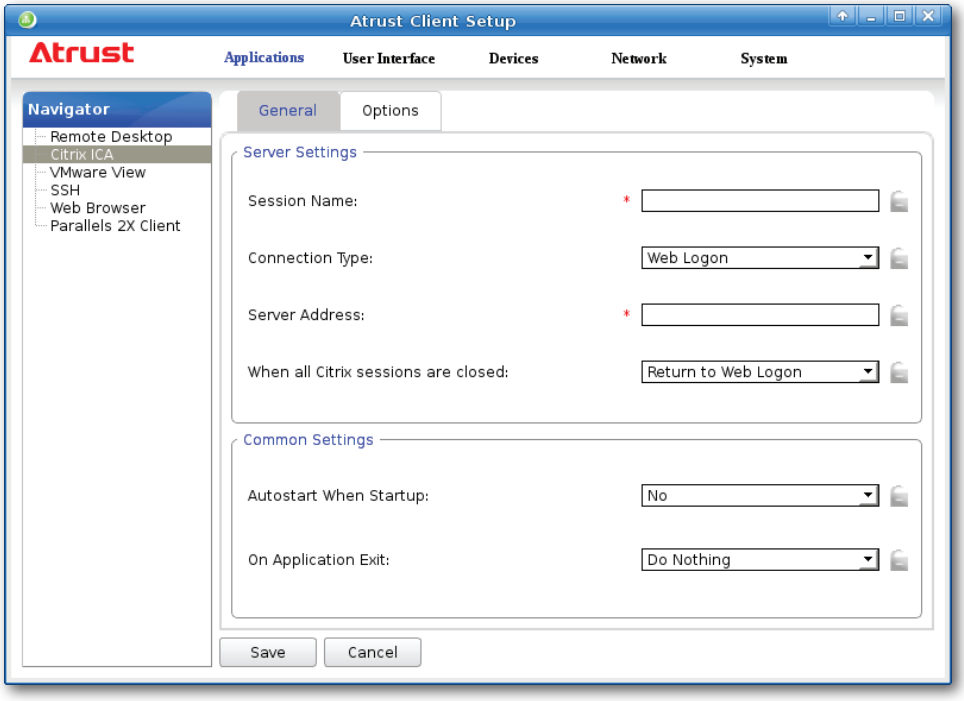


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, leave the connection type as **Web Logon** as default, and then type in the desired session name and the IP address / URL / FQDN of the server through which Citrix services are accessible.



NOTE

- For newer versions of XenDesktop and XenApp, you may need to further specify the ***sub-path*** of the server. Refer to the following table for details:

Citrix Product	Component to Connect	Connection Address
XenApp 6.5 or earlier	Web Interface	IP / URL / FQDN
XenDesktop 5.6 or earlier	Web Interface	IP / URL / FQDN
Virtual Apps and Desktops (XenApp and XenDesktop 7.5 or later)	StoreFront	IP / URL / FQDN **plus** *sub-path* **For example —** **FQDN:** X75.CTX.poc **Sub-path:** /Citrix/StoreWeb (default) **Connection Address:** X75.CTX.poc/Citrix/StoreWeb

- FQDN is the acronym of Fully Qualified Domain Name.

5. Click **Save** to add this ICA connection entry. The access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

Connection Type: StoreFront

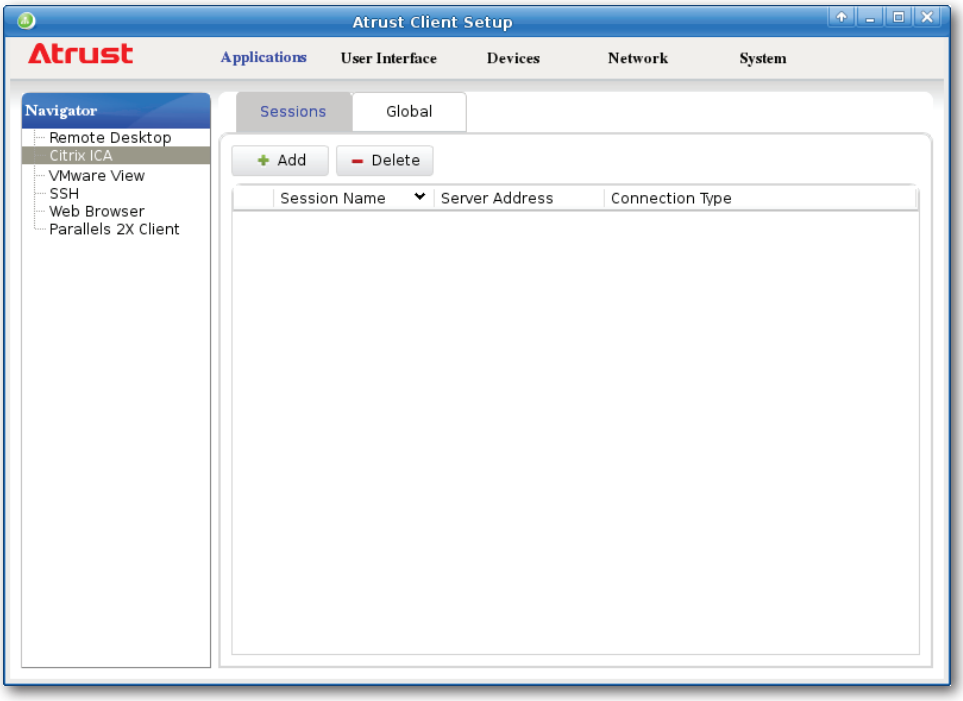
To quickly configure ICA connection settings for the connection type of StoreFront, please do the following:

NOTE

- You can refer to the following table for Citrix products and recommended connection types:

Citrix Product	Recommended Connection Type
XenApp 6.5 or earlier	XenApp / Web Logon
XenDesktop 5.6 or earlier	XenDesktop / Web Logon
Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)	StoreFront / Web Logon
VDI-in-a-Box	VDI-in-a-Box / Web Logon

1. On Atrust Client Setup, Click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

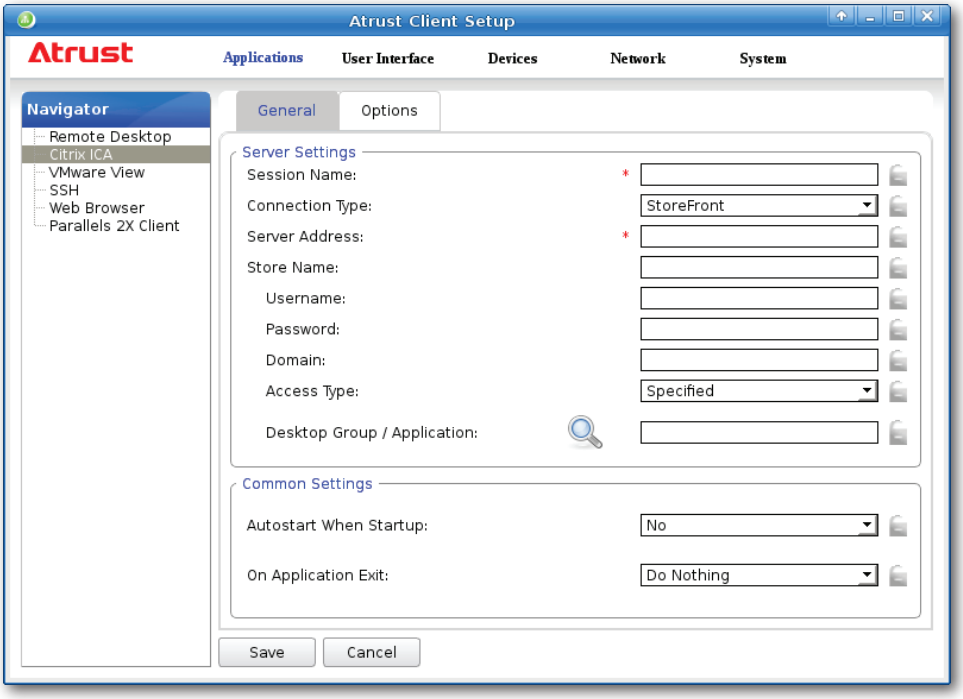


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, click the Connection Type drop-down menu to select **StoreFront**.



5. Type the session name, the IP address / URL / FQDN of the server through which virtual applications/ desktops are accessible, and the name of desktop group or application.

NOTE

- You can use the Search icon to help you discover available desktop groups or applications for a given set of credentials.

6. Click **Save** to confirm. The customized access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

Connection Type: VDI-in-a-Box

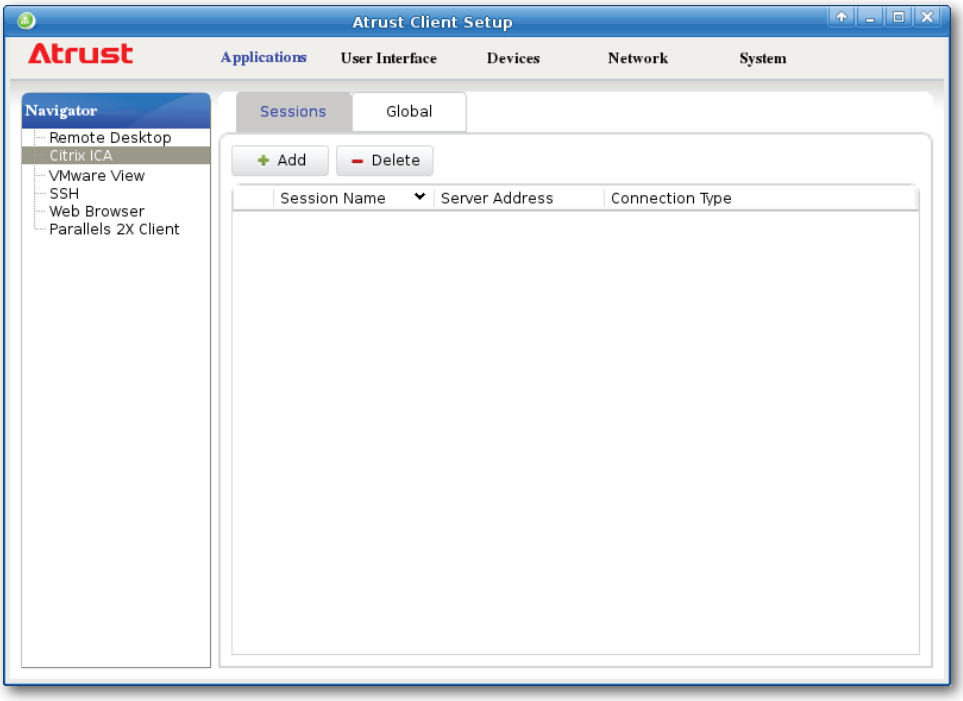
To quickly configure ICA connection settings for the connection type of VDI-in-a-Box, please do the following:

NOTE

- You can refer to the following table for Citrix products and recommended connection types:

Citrix Product	Recommended Connection Type
XenApp 6.5 or earlier	XenApp / Web Logon
XenDesktop 5.6 or earlier	XenDesktop / Web Logon
Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)	StoreFront / Web Logon
VDI-in-a-Box	VDI-in-a-Box / Web Logon

1. On Atrust Client Setup, Click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

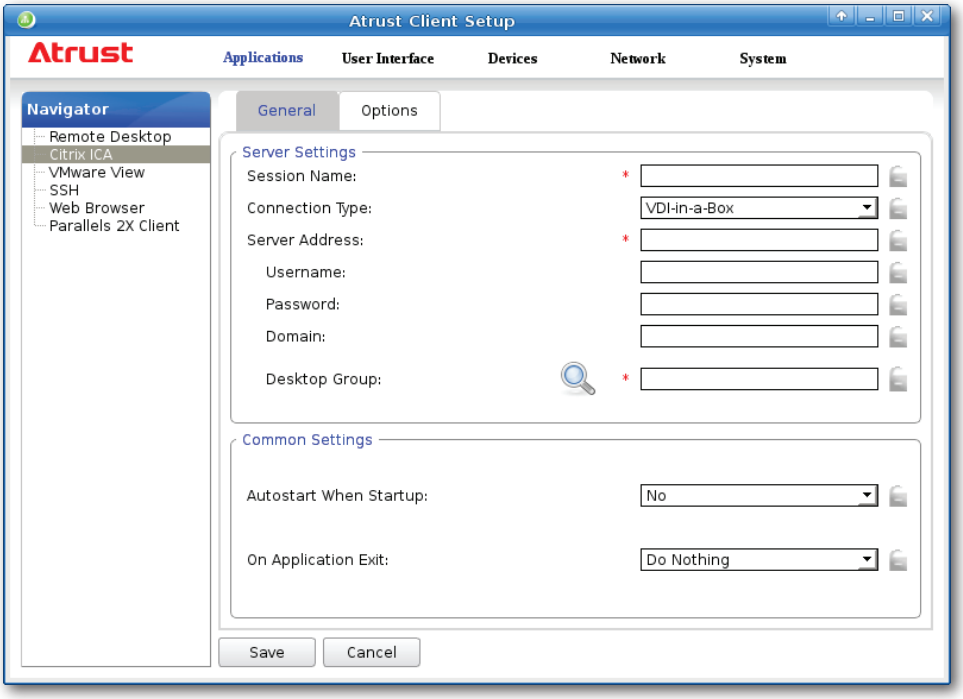


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, click the Connection Type drop-down menu to select **VDI-in-a-Box**.



5. Type the session name, the IP address / URL / FQDN of the server through which virtual desktops are accessible, and the name of the desktop group.

NOTE

- You can use the Search icon to help you discover available desktop groups for a given set of credentials.

6. Click **Save** to confirm. The customized access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

Connection Type: XenDesktop

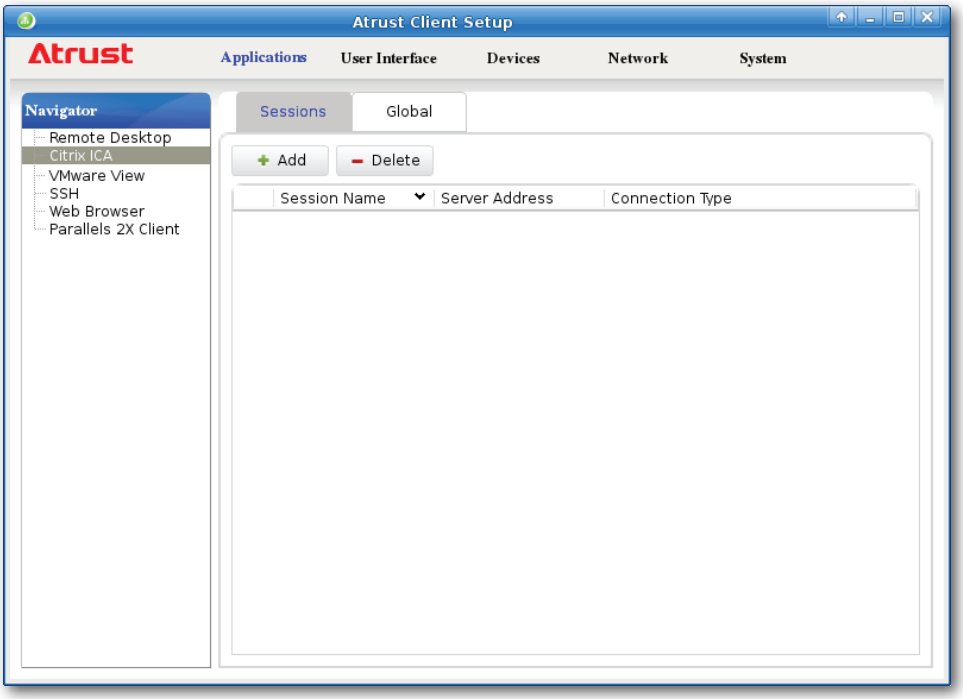
To quickly configure ICA connection settings for the connection type of XenDesktop, please do the following:

NOTE

- You can refer to the following table for Citrix products and recommended connection types:

Citrix Product	Recommended Connection Type
XenApp 6.5 or earlier	XenApp / Web Logon
XenDesktop 5.6 or earlier	XenDesktop / Web Logon
Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)	StoreFront / Web Logon
VDI-in-a-Box	VDI-in-a-Box / Web Logon

1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

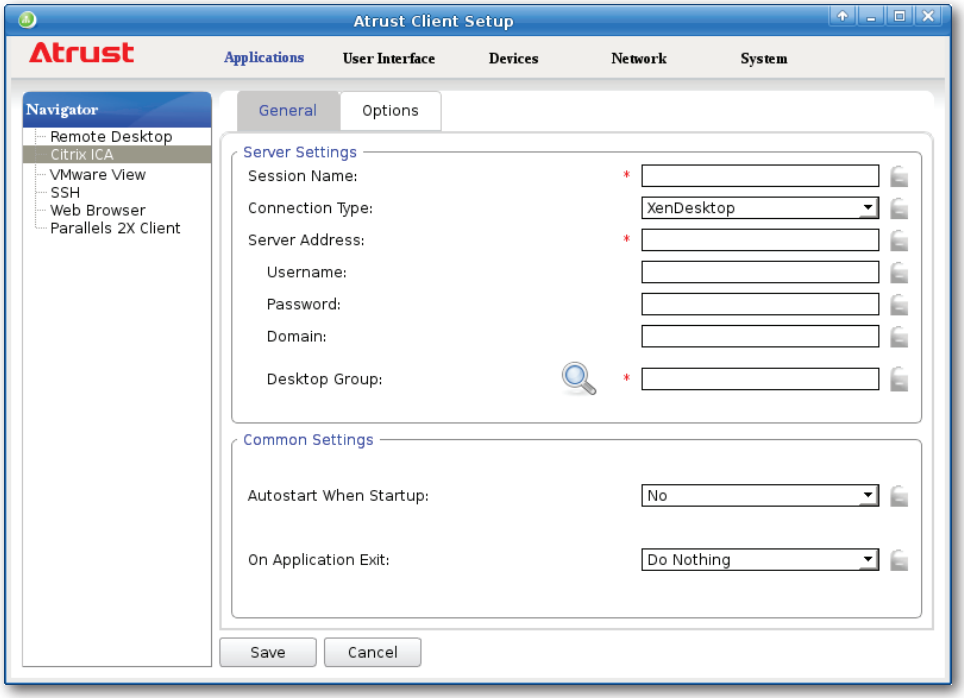


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, click the Connection Type drop-down menu to select **XenDesktop**.



5. Type the session name, the IP address / URL / FQDN of the server through which virtual desktops are accessible, and the desired desktop group.

NOTE

- You can use the Search icon to help you discover available desktop groups for a given set of credentials.

6. Click **Save** to confirm. The customized access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

Connection Type: XenApp

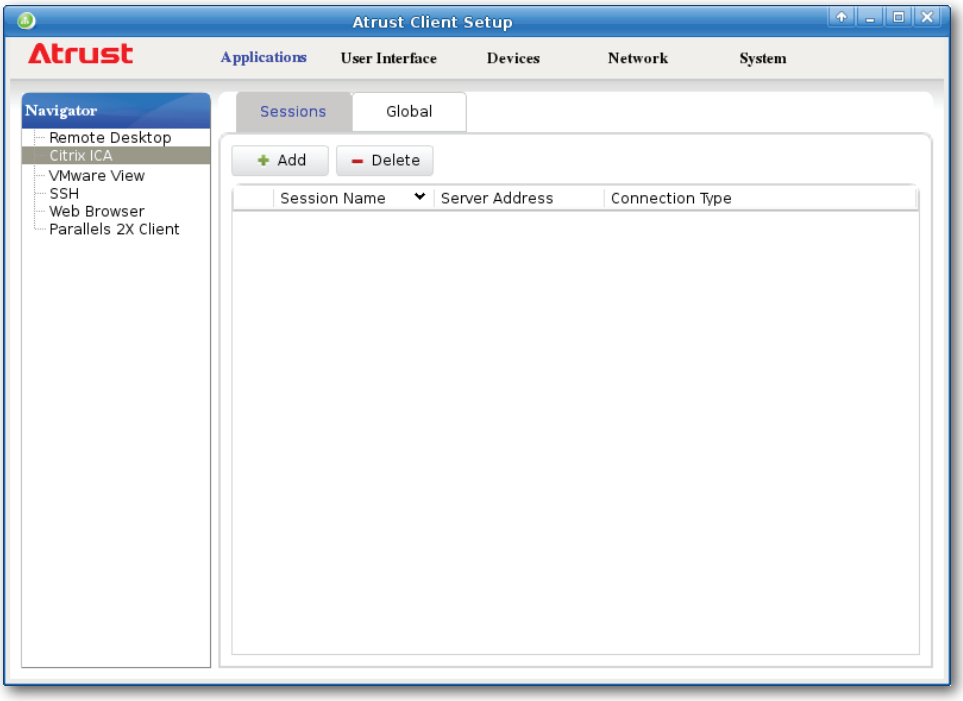
To quickly configure ICA connection settings for the connection type of XenApp, please do the following:

NOTE

- You can refer to the following table for Citrix products and recommended connection types:

Citrix Product	Recommended Connection Type
XenApp 6.5 or earlier	XenApp / Web Logon
XenDesktop 5.6 or earlier	XenDesktop / Web Logon
Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)	StoreFront / Web Logon
VDI-in-a-Box	VDI-in-a-Box / Web Logon

1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

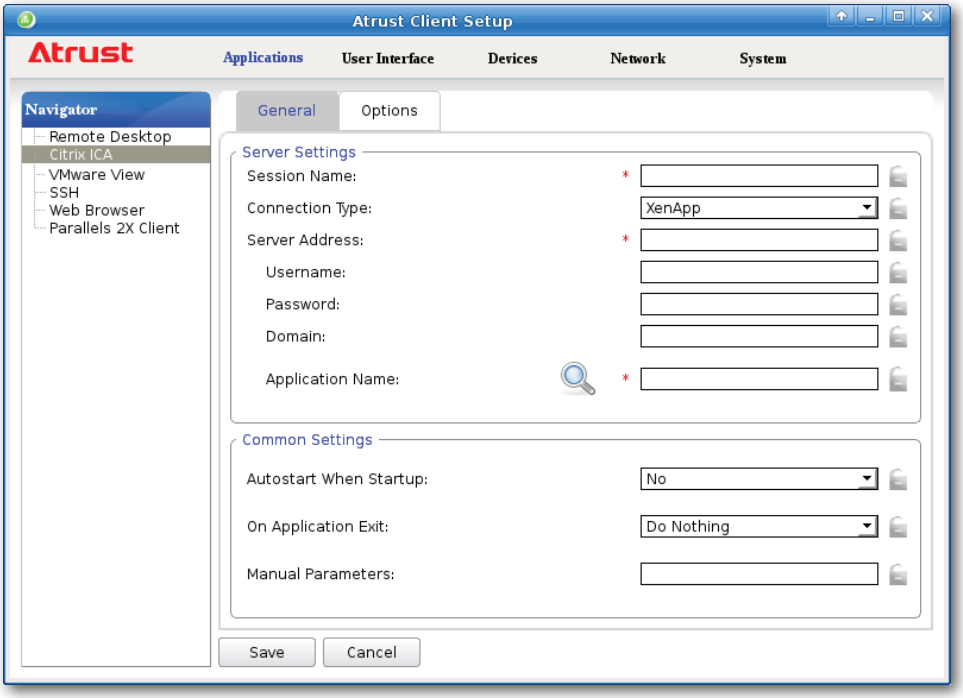


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, click the Connection Type drop-down menu to select **XenApp**.



5. Type the session name, the IP address / URL / FQDN of the server through which virtual applications are accessible, and the desired application name.

NOTE

- You may need to provide the ***XML port number*** as well for your server address (for example, XA65P.CTX.poc:**8080**), depending on your server-side configuration.

NOTE

- You can use the Search icon to help you discover available applications for a given set of credentials.

6. Click **Save** to confirm. The customized access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

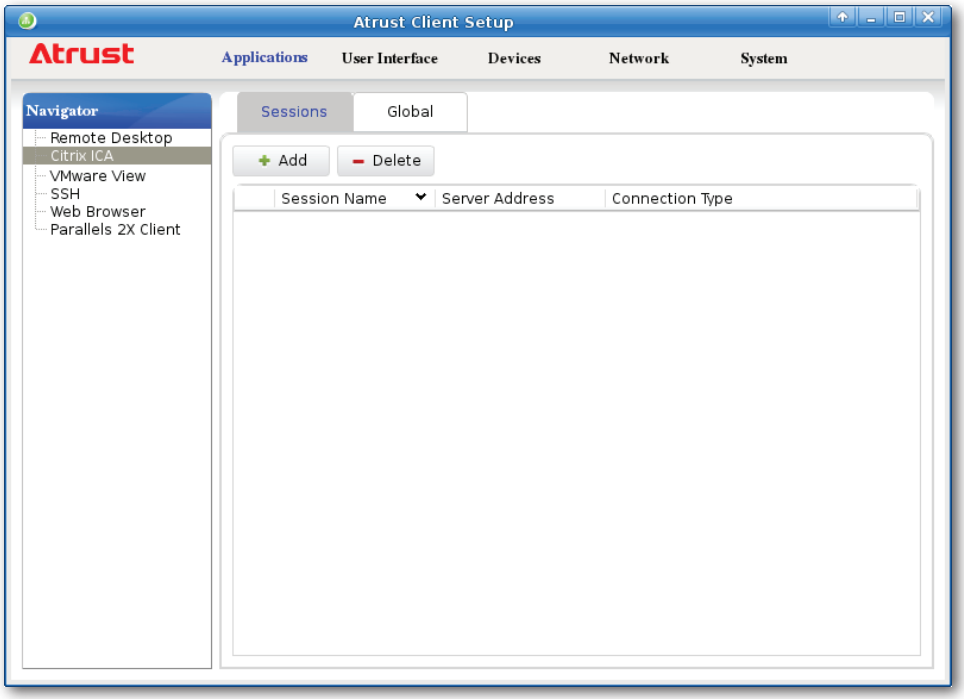
Connection Type: Server Connection

To quickly configure ICA connection settings for the connection type of Server Connection, please do the following:

NOTE

- This connection type is used to connect to XenApp server for ***administration*** and supports ***only*** *XenApp 6.5 and earlier*.

1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.

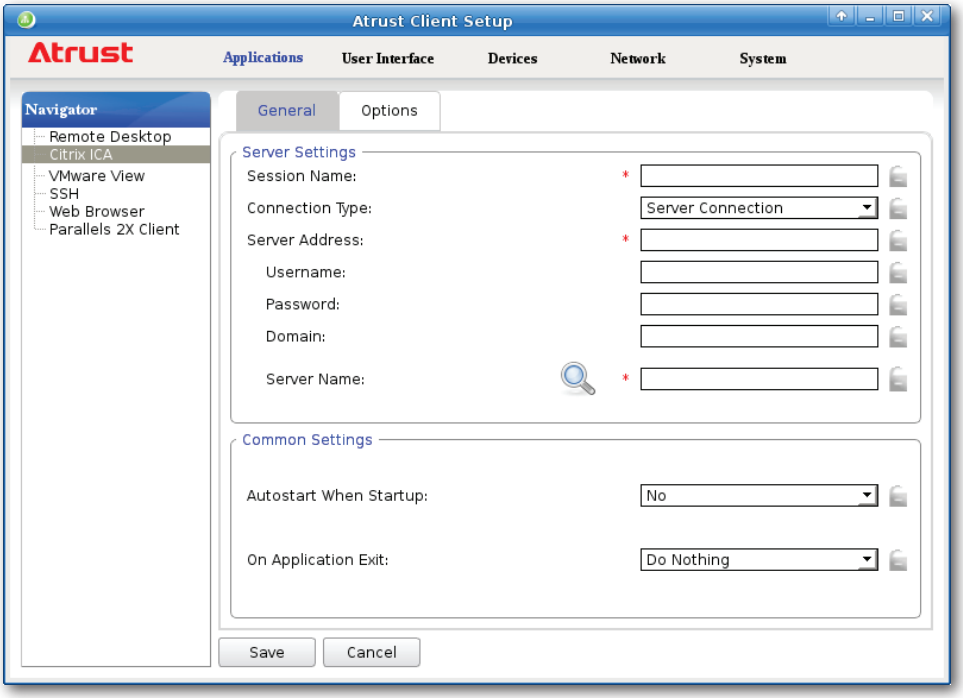


NOTE

- If you haven't created any entry, the ICA Connection list will be empty.

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

4. On **General** sub-tab, click the Connection Type drop-down menu to select **Server Connection**.



5. Type the session name, server address, and server name.

NOTE

- You may need to provide the ***XML port number*** as well for your server address (for example, 192.168.77.10:**8080**), depending on your server-side configuration.

NOTE

- Only connections to XenApp servers are supported by this connection type.
- You can use the Search icon to help you detect the server name.

6. Click **Save** to confirm. The customized access shortcuts are automatically created on the local desktop and START menu.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "3.6.11 Configuring Advanced ICA Connection Settings" on page 182.

3.6.7 Switching the Citrix Receiver Version

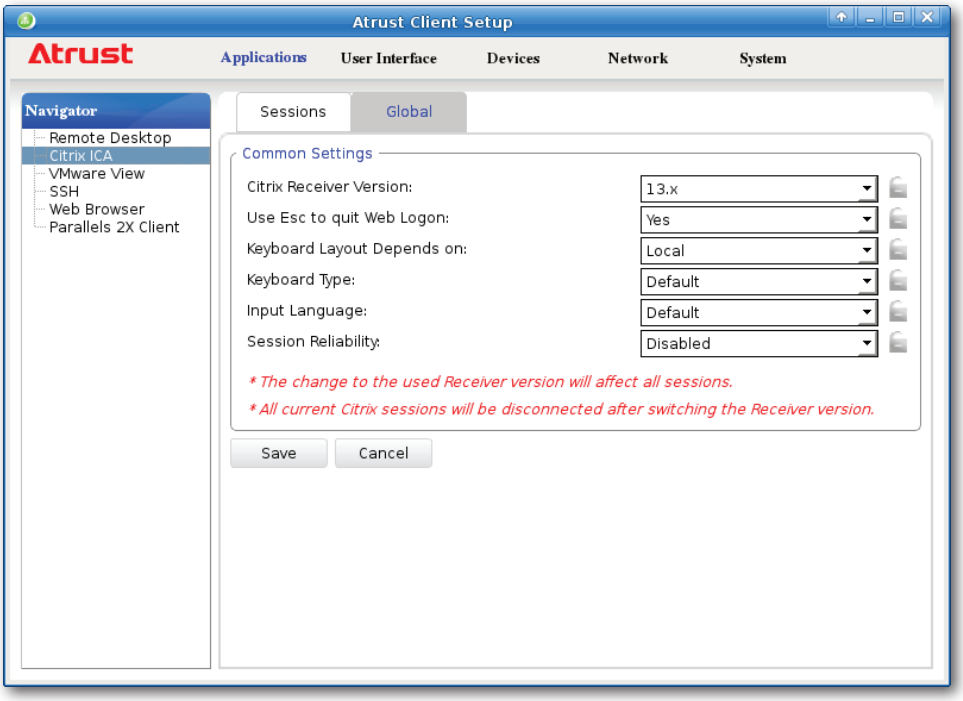
Two versions of Citrix Receiver are switchable in case that an older version of Citrix Receiver is required for your Citrix environment.

To change the version of Citrix Receiver, please do the following:

NOTE

- This is a global setting; the change will affect all Citrix connections.

1. On Atrust Client Setup, click **Applications** > **Citrix ICA** > **Global**.
2. Click the drop-down menu to select the desired Citrix Receiver version. Two options are available: **12.x** and **13.x**.



TIP

- The default Citrix Receiver version is **13.x**.
- You can refer to the following table for Citrix products and recommended Citrix Receiver version:

Citrix Product	Recommended Receiver Version
XenApp earlier than 6.5	12.x
XenDesktop earlier than 5.6	12.x
Virtual Apps and Desktops (XenApp / XenDesktop 7.x or later)	13.x

3. Click **Save** to apply.

3.6.8 Enabling or Disabling Esc to Quit on the Web Logon Screen

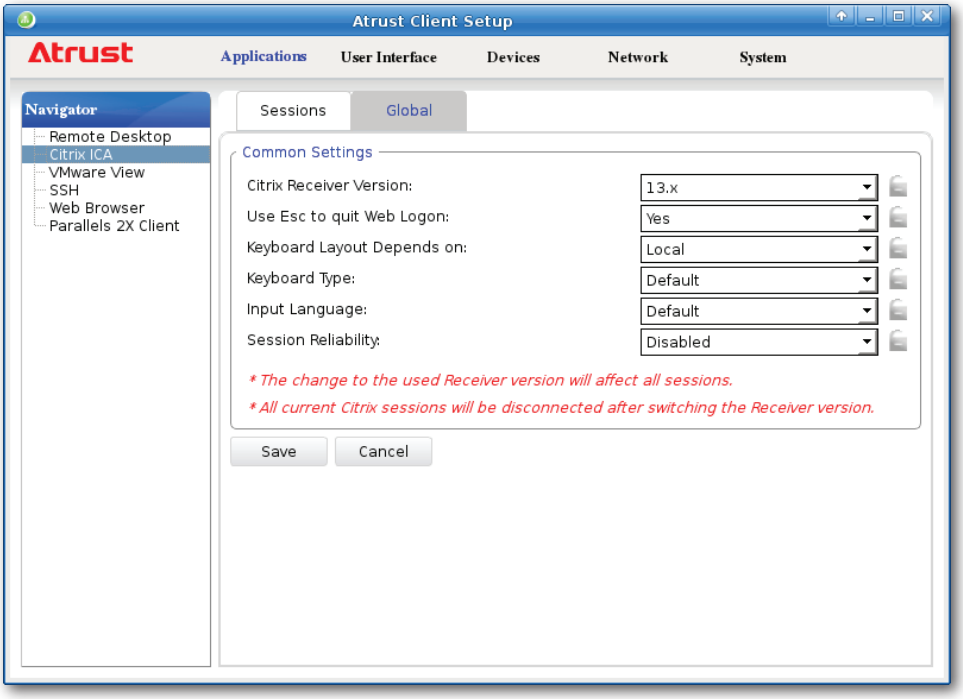
You can choose whether to allow the use of **Esc** key to quit the Web Logon screen:

- If **Yes** is selected, you can use both **Esc** and **Alt** + **F4** to quit the Web Logon screen.
- If **No** is selected, only **Alt** + **F4** works.

To enable or disable Esc to Quit on the Web Logon screen, please do the following:

> **NOTE**
>
> - This is a global setting; the change will affect all Citrix connections.

1. On Atrust Client Setup, click **Applications** > **Citrix ICA** > **Global**.
2. Click the drop-down menu to select **Yes** or **No** to enable or disable Esc to Quit.

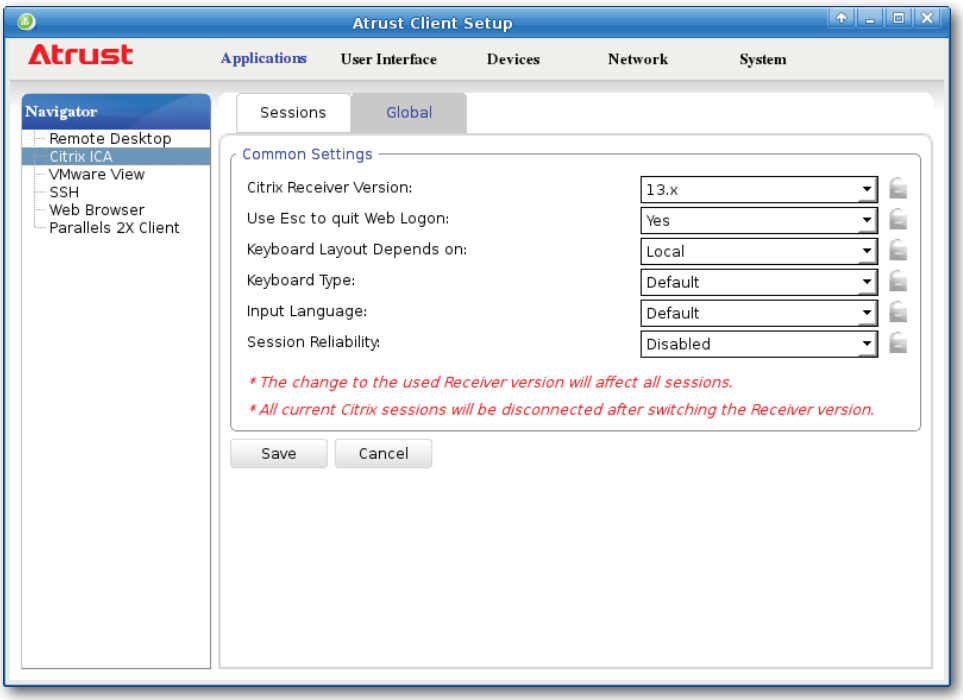


3. Click **Save** to apply.

3.6.9 Configuring Keyboard Layout and Type for Citrix ICA Sessions

To set the used keyboard layout and type for all Citrix ICA sessions, please do the following:

1. On Atrust Client Setup, click **Applications** > **Citrix ICA** > **Global**.
2. Click drop-down menus to select what determines the keyboard layout and the desired keyboard type.



NOTE

- These are global settings; the changes will affect all ICA sessions.

3. Click **Save** to apply.

3.6.10 Accessing Citrix Services

For Connection Types of StoreFront, VDI-in-a-Box, XenDesktop, XenApp, and Server Connection

To access Citrix services, please do the following:

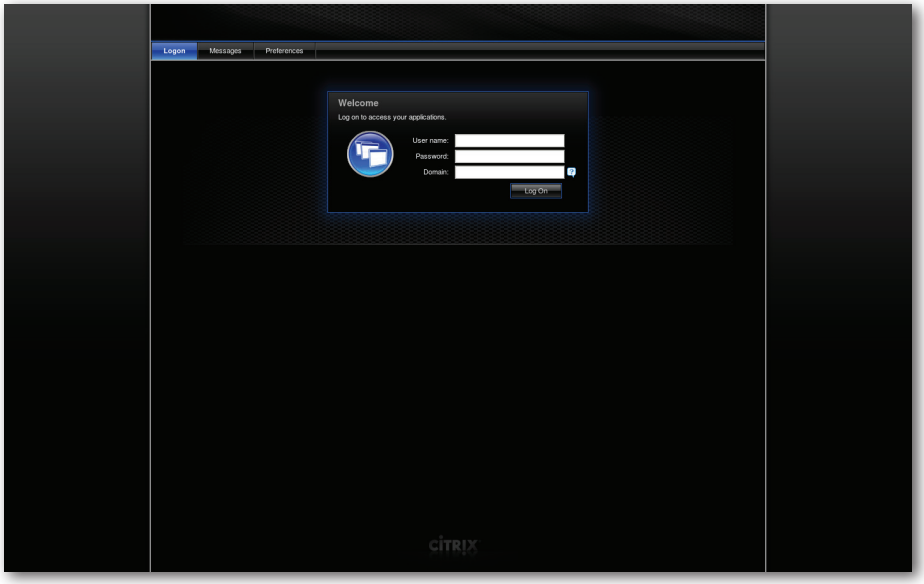
1. Double click the created (customized) shortcut on the desktop, and then provide your credentials if needed.
2. Depending on your connection type and settings, you can find:
   - Desktop or application launched directly on the screen
   - Access shortcuts of desktops or applications shown on the desktop or a window on the desktop

For Connection Type of Web Logon

To access Citrix services, please do the following:

1. Double click the created (customized) shortcut on the desktop.
2. The Web browser is launched in ***full-screen*** with the Citrix Logon screen.

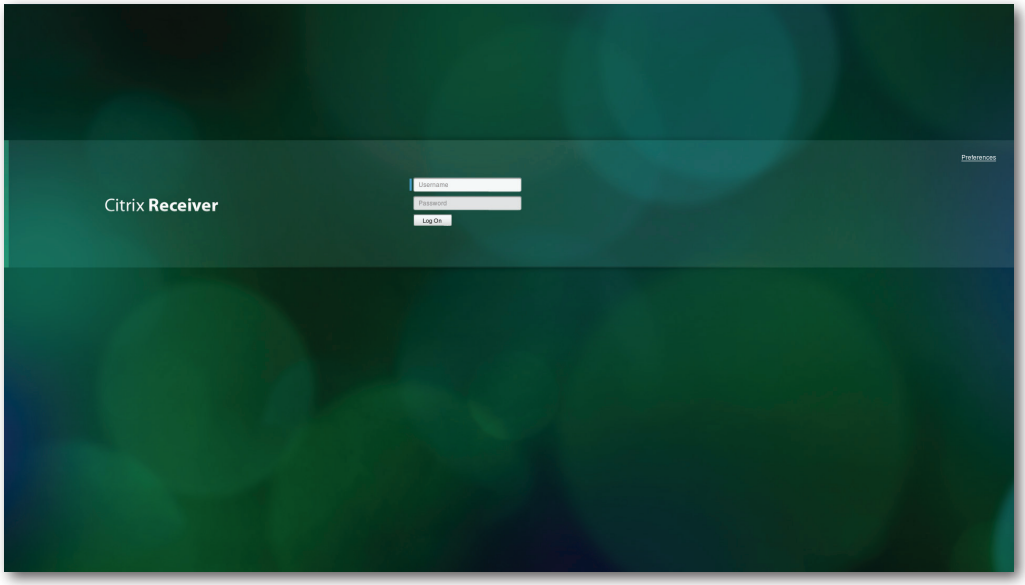
Citrix Logon Screen Example: XenApp 6.0 Fundamentals



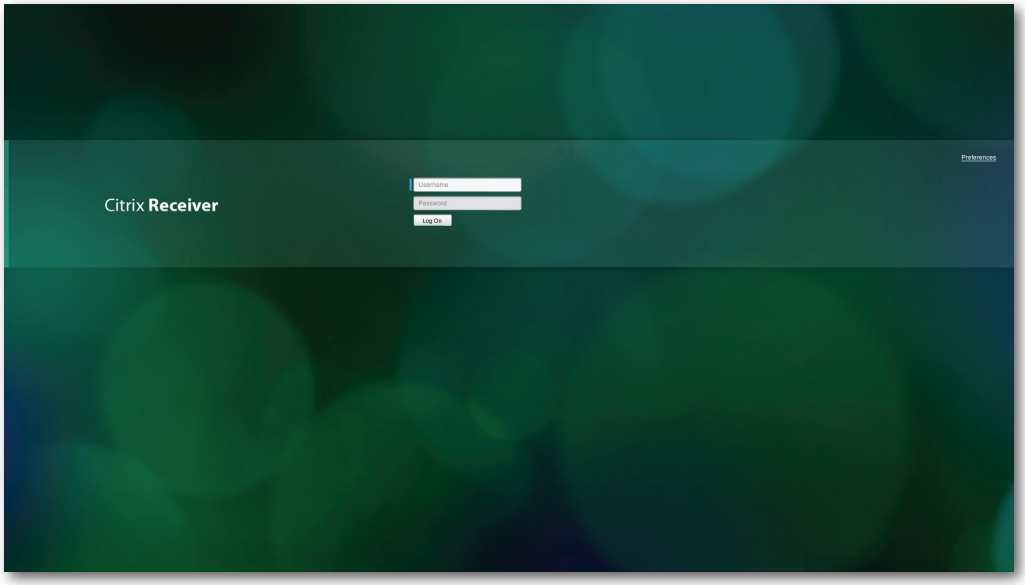
Citrix Logon Screen Example: XenApp 6.5 Platinum

Citrix Logon Screen Example: XenDesktop 5.6 Platinum

Citrix Logon Screen Example: VDI-in-a-Box



Citrix Logon Screen Example: XenApp and XenDesktop 7.5 Platinum



3. Type in the required credentials, and then click **Log On**.

NOTE

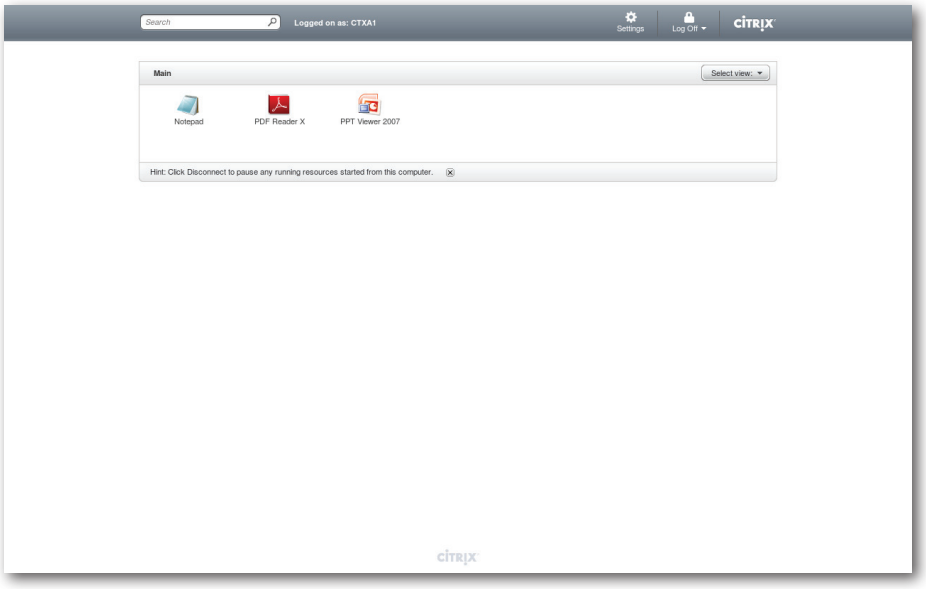
- If your XenApp server doesn't belong to any domain, type in the server name in the Domain field instead.

4. On the Desktop or Application Selection screen, click to select the desired desktop or application(s).

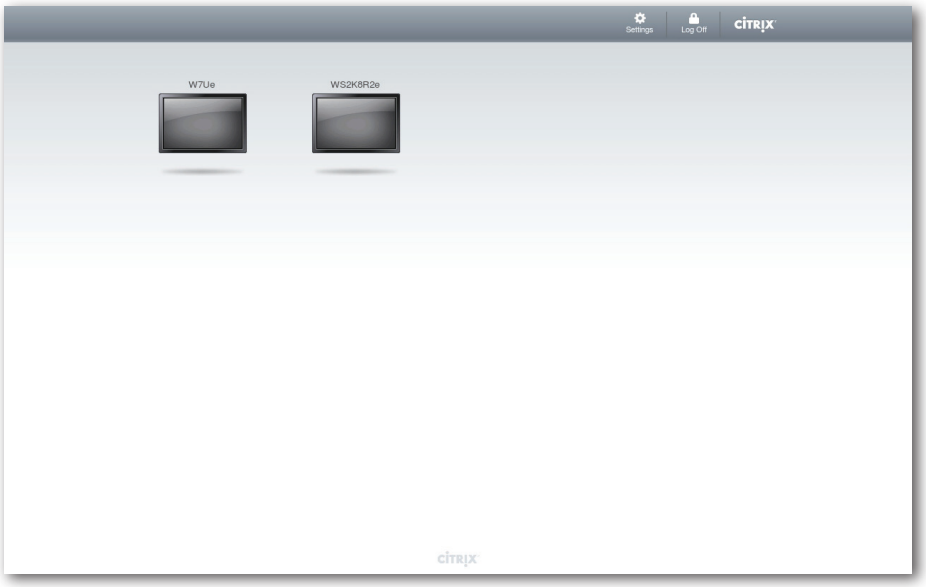
NOTE

- You might enter the virtual desktop directly if only one type of virtual desktop is assigned to the provided credentials.

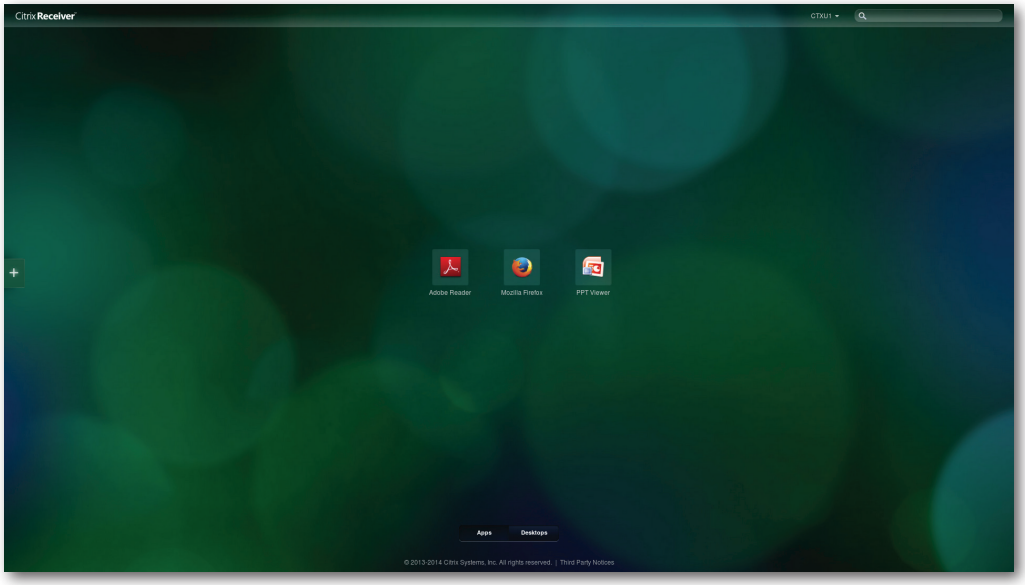
Selection Screen Example: XenApp 6.5 Platinum



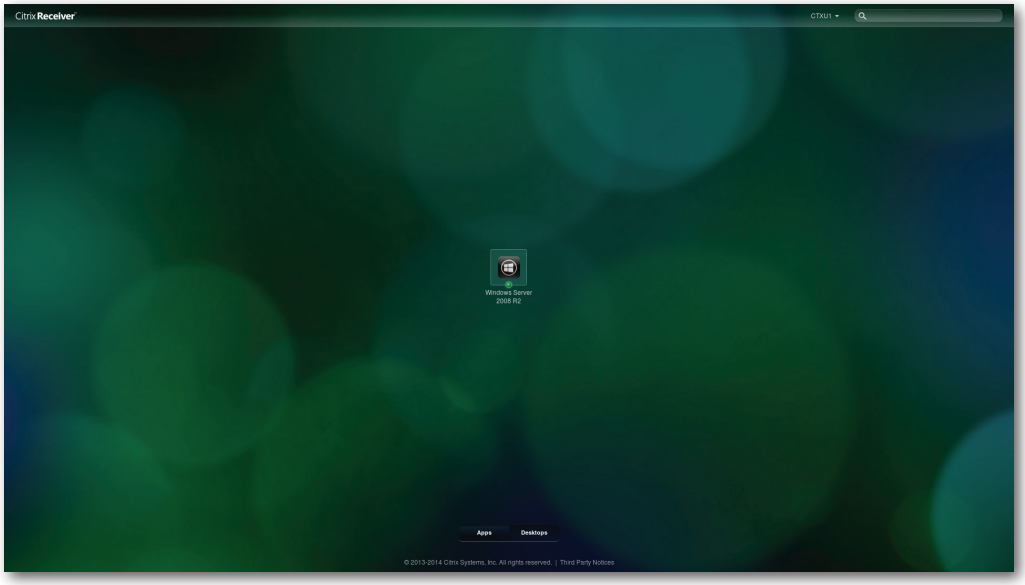
Selection Screen Example: XenDesktop 5.6 Platinum



Selection Screen Example: XenApp 7.5 Platinum

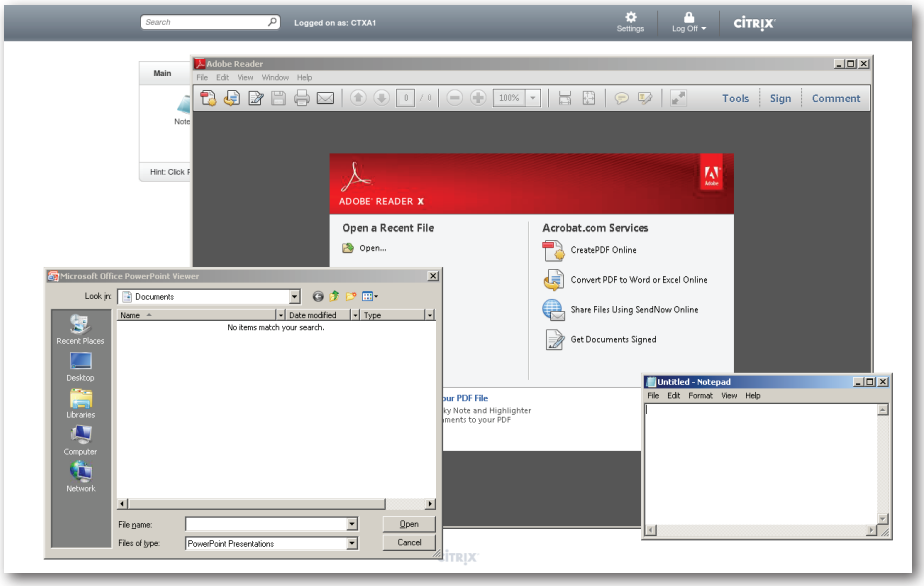


Selection Screen Example: XenDesktop 7.5 Platinum

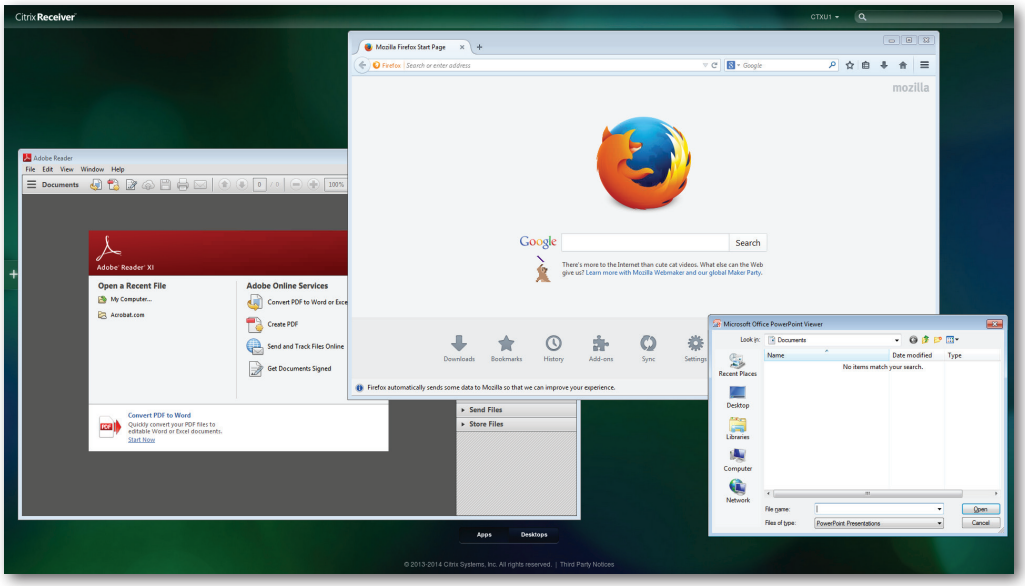


5. The selected virtual desktop or application(s) will be displayed on the screen.

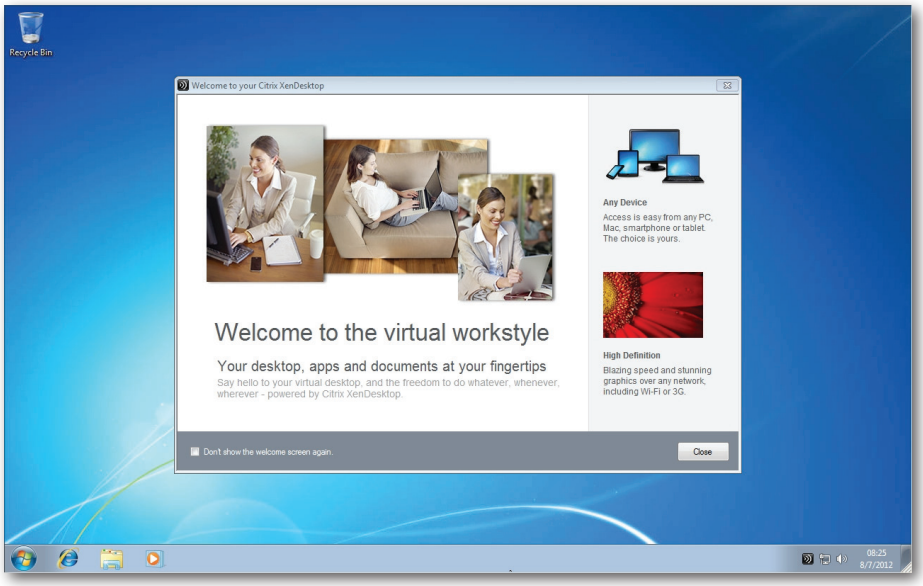
Virtual Application Examples
PowerPoint Viewer, Adobe Reader, and Notepad



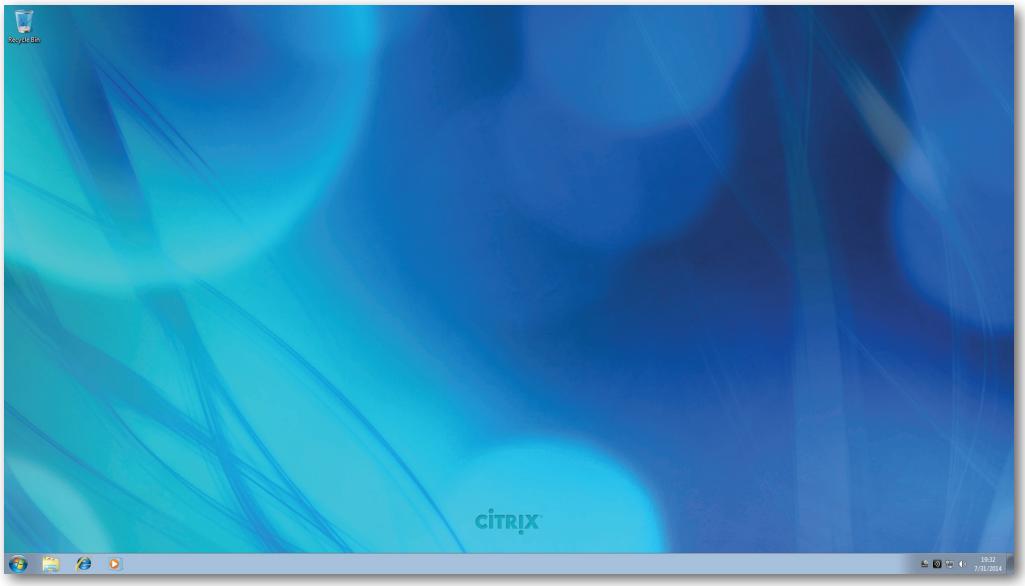
Virtual Application Examples
Adobe Reader, Mozilla Firefox, and PowerPoint Viewer



Virtual Desktop Example
Windows 7 Ultimate



Virtual Desktop Example
Windows Server 2008 R2



3.6.11 Configuring Advanced ICA Connection Settings

The tables below provide a description of each setting item for ICA connections. Please refer to these tables to configure advanced settings and customize shortcuts on the local desktop and START menu for service access.

NOTE

- Please note that available settings vary with the selected connection type.

Settings for the Connection Type of Web Logon

NOTE

- For descriptions of available settings for the connection type of StoreFront, please refer to "Settings for the Connection Type of StoreFront" on page 187.
- For descriptions of available settings for the connection type of VDI-in-a-Box, please refer to "Settings for the Connection Type of VDI-in-a-Box" on page 192.
- For descriptions of settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 197.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 202.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 207.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name of browser sessions for Citrix service access.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when Web Logon is selected.

Six connection types are available:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:

<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
<tr><td>Server Address</td><td>Type in the IP address / URL / FQDN of the server through which Citrix services are accessible.

Refer to the table below for details:

<table>
<tr><th>Citrix Product</th><th>Component to Connect</th><th>Connection Address</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>Web Interface</td><td>IP / URL / FQDN</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>Web Interface</td><td>IP / URL / FQDN</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp and XenDesktop 7.5 or later)</td><td>StoreFront</td><td>IP / URL / FQDN plus sub-path

For example —
FQDN: X75.CTX.poc
Sub-path: /Citrix/StoreWeb (default)
Connection Address:
X75.CTX.poc/Citrix/StoreWeb</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>When all Citrix sessions are closed</td><td>Select what to do next when all Citrix sessions are closed.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Return to Web Logon</td><td>Stay on the Web Logon screen.</td></tr><tr><td>Quit Web Logon</td><td>Exit the Web Logon screen.</td></tr></table>
NOTE: If only one virtual application or desktop is opened and then closed, your option here would apply.</td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a browser session for Citrix service access automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table><tr><th>No.</th><th>Mode</th><th>Description</th></tr><tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr><tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr><tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr></table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.</td></tr>
</table>

<table>
<tr>
<td>On Application Exit</td>
<td>Select what to do when a browser session for Citrix service access is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr>
<tr><td>Restart Application</td><td>Opens a browser session again for service access.</td></tr>
<tr><td>Reboot</td><td>Restarts your thin client.</td></tr>
<tr><td>Shutdown</td><td>Turns off your thin client.</td></tr>
</table>
</td>
</tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) and to select access type in a Citrix ICA session. Three options are available: **No**, **Read Only**, and **Read Write**. If **Read Only** or **Read Write** is selected, the locally attached USB drive(s) will become available in launched Citrix ICA sessions. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a virtual desktop.
Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.

Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
USB Redirection Settings	
Item	**Description**
USB Storage	Please refer to "Advanced Quick Connection Settings for Citrix ICA Sessions" on page 64 for detailed instructions on these similar settings.
Printers	
Redirect Connected USB Devices	
Plugged USB Devices	
Redirection Rules	

Settings for the Connection Type of StoreFront

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 182.
- For descriptions of settings for the connection type of VDI-in-a-Box, please refer to "Settings for the Connection Type of VDI-in-a-Box" on page 192.
- For descriptions of settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 197.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 202.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 207.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when StoreFront is selected.

Six connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:
<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Server Address</td><td>Type in the IP address / URL / FQDN of the server through which virtual desktops or applications are accessible (where a StoreFront is hosted).</td></tr>
<tr><td>Store Name</td><td>Type in the store name of your Citrix environment if required.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.</td></tr>
<tr><td>Access Type</td><td>Click the drop-down menu to select the access type. Two options are available: Specified and All.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Specified</td><td>• Specific desktop/application, or
• Access shortcuts in a window</td></tr><tr><td>All</td><td>• Access shortcuts on the desktop</td></tr></table></td></tr>
<tr><td>Desktop Group / Application</td><td>Type in the name of the desktop group / application or use the Search icon in front of the field to discover available desktop groups / applications.</td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a Citrix ICA session automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:
<table><tr><th>No.</th><th>Mode</th><th>Description</th></tr><tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr><tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr><tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr></table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.</td></tr>
</table>

<table>
<tr><td>On Application Exit</td><td>Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr><tr><td>Restart Application</td><td>Opens an ICA session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
<tr><td>Prompt for Credentials on Application Restart</td><td>This setting item is available only when Restart Application is selected for On Application Exit. Click to select whether to prompt for credentials or not when an ICA session restarts.</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Color Depth	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **16 Bit**, **24 Bit**, and **Automatic**.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Four options are available: **Full Screen**, **1280x1024**, **1024x768**, and **800x600**.
Window Mode	Click the drop-down menu to select the desired window mode. Two options are available: **Regular Window** and **Seamless Window**.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a virtual desktop.

Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.
Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
Enable Automatic Reconnect	Check/Uncheck to enable/disable automatic reconnecting after an ICA session was interrupted. **NOTE:** Automatic reconnecting (Auto Client Reconnect) may not work for a XenDesktop ICA session. This is a known issue. For more details, please visit Citrix websites at support.citrix.com or www.citrix.com.
Number of Retries	Click the drop-down menu to select the number of retries, ranging from 1 to 10.
Delay between Retries	Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.
Enable Audio	Check/Uncheck to enable/disable sound in an ICA session.
Audio Quality	Click the drop-down menu to choose the desired sound quality in an ICA session. Three options are available: **High Quality**, **Medium Quality**, and **Low Quality**.

Option	Description
High Quality	Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.
Medium Quality	Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.
Low Quality	Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.

<table>
<tr><td>Enable Audio Input</td><td>Check/Uncheck to enable/disable audio input in an ICA session.</td></tr>
<tr><td>Windows Key Combination</td><td>Click the drop-down menu to select where to apply Windows Key Combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">Connection Dialog Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Show Remember Field</td><td>Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.</td></tr>
<tr><td colspan="2">USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>USB Storage</td><td rowspan="5">Please refer to “Advanced Quick Connection Settings for Citrix ICA Sessions” on page 64 for detailed instructions on these similar settings.</td></tr>
<tr><td>Printers</td></tr>
<tr><td>Redirect Connected USB Devices</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
</table>

Settings for the Connection Type of VDI-in-a-Box

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 182.
- For descriptions of settings for the connection type of StoreFront, please refer to "Settings for the Connection Type of StoreFront" on page 187.
- For descriptions of settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 197.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 202.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 207.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when VDI-in-a-Box is selected.

Six connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:
<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
</table>

Server Address	Type in the IP address / URL / FQDN of the server through which virtual desktops are accessible.
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server.
Desktop Group / Application	Type in the name of the desktop group or use the Search icon in front of the field to discover available desktop groups.

Common Settings

Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when your mt182L is started up (Autostart mode). **NOTE:** There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session. Available actions include: • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client
3	Quick Connection	The client will enter Atrust Quick Connection screen after system startup.

NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.

<table>
<tr><td>On Application Exit</td><td>Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr><tr><td>Restart Application</td><td>Opens an ICA session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
<tr><td>Prompt for Credentials on Application Restart</td><td>This setting item is available only when Restart Application is selected for On Application Exit. Click to select whether to prompt for credentials or not when an ICA session restarts.</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Color Depth	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **16 Bit**, **24 Bit**, and **Automatic**.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Four options are available: **Full Screen**, **1280x1024**, **1024x768**, and **800x600**.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a virtual desktop.

Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.
Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
Enable Automatic Reconnect	Check/Uncheck to enable/disable automatic reconnecting after an ICA session was interrupted. **NOTE:** Automatic reconnecting (Auto Client Reconnect) may not work for a XenDesktop ICA session. This is a known issue. For more details, please visit Citrix websites at support.citrix.com or www.citrix.com.
Number of Retries	Click the drop-down menu to select the number of retries, ranging from 1 to 10.
Delay between Retries	Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.
Enable Audio	Check/Uncheck to enable/disable sound in an ICA session.
Audio Quality	Click the drop-down menu to choose the desired sound quality in an ICA session. Three options are available: **High Quality**, **Medium Quality**, and **Low Quality**.

Option	Description
High Quality	Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.
Medium Quality	Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.
Low Quality	Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.

<table>
<tr><td>Enable Audio Input</td><td>Check/Uncheck to enable/disable audio input in an ICA session.</td></tr>
<tr><td>Windows Key Combination</td><td>Click the drop-down menu to select where to apply Windows Key Combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">Connection Dialog Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Show Remember Field</td><td>Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.</td></tr>
<tr><td colspan="2">USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>USB Storage</td><td rowspan="5">Please refer to “Advanced Quick Connection Settings for Citrix ICA Sessions” on page 64 for detailed instructions on these similar settings.</td></tr>
<tr><td>Printers</td></tr>
<tr><td>Redirect Connected USB Devices</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
</table>

Settings for the Connection Type of XenDesktop

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 182.
- For descriptions of settings for the connection type of StoreFront, please refer to "Settings for the Connection Type of StoreFront" on page 187.
- For descriptions of settings for the connection type of VDI-in-a-Box, please refer to "Settings for the Connection Type of VDI-in-a-Box" on page 192.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 202.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 207.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when XenDesktop is selected.

Six connection types are available:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:

<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
</table>

Server Address	Type in the IP address / URL / FQDN of the server through which virtual desktops are accessible (where a Web Interface is hosted).
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server.
Desktop Group	Type in the name of the desktop group or use the Search icon in front of the field to discover available desktop groups.

Common Settings

Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when your mt182L is started up (Autostart mode). **NOTE:** There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session. Available actions include: • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client
3	Quick Connection	The client will enter Atrust Quick Connection screen after system startup.

NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.

<table>
<tr><td>On Application Exit</td><td>Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr><tr><td>Restart Application</td><td>Opens an ICA session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
<tr><td>Prompt for Credentials on Application Restart</td><td>This setting item is available only when Restart Application is selected for On Application Exit. Click to select whether to prompt for credentials or not when an ICA session restarts.</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Color Depth	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **16 Bit**, **24 Bit**, and **Automatic**.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Four options are available: **Full Screen**, **1280x1024**, **1024x768**, and **800x600**.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a virtual desktop.

Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.
Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
Enable Automatic Reconnect	Check/Uncheck to enable/disable automatic reconnecting after an ICA session was interrupted. **NOTE:** Automatic reconnecting (Auto Client Reconnect) may not work for a XenDesktop ICA session. This is a known issue. For more details, please visit Citrix websites at support.citrix.com or www.citrix.com.
Number of Retries	Click the drop-down menu to select the number of retries, ranging from 1 to 10.
Delay between Retries	Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.
Enable Audio	Check/Uncheck to enable/disable sound in an ICA session.
Audio Quality	Click the drop-down menu to choose the desired sound quality in an ICA session. Three options are available: **High Quality**, **Medium Quality**, and **Low Quality**.

Option	Description
High Quality	Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.
Medium Quality	Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.
Low Quality	Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.

<table>
<tr><td>Enable Audio Input</td><td>Check/Uncheck to enable/disable audio input in an ICA session.</td></tr>
<tr><td>Windows Key Combination</td><td>Click the drop-down menu to select where to apply Windows Key Combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">Connection Dialog Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Show Remember Field</td><td>Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.</td></tr>
<tr><td colspan="2">USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>USB Storage</td><td rowspan="5">Please refer to “Advanced Quick Connection Settings for Citrix ICA Sessions” on page 64 for detailed instructions on these similar settings.</td></tr>
<tr><td>Printers</td></tr>
<tr><td>Redirect Connected USB Devices</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
</table>

Settings for the Connection Type of XenApp

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 182.
- For descriptions of settings for the connection type of StoreFront, please refer to "Settings for the Connection Type of StoreFront" on page 187.
- For descriptions of settings for the connection type of VDI-in-a-Box, please refer to "Settings for the Connection Type of VDI-in-a-Box" on page 192.
- For descriptions of available settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 197.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 207.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when XenApp is selected.

Six connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:
<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Server Address</td><td>Type in the IP address / URL / FQDN of a XenApp server.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.</td></tr>
<tr><td>Application Name</td><td>Type in the application name or use the Search icon in front of the field to discover available applications.</td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a Citrix ICA session automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>

NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.</td></tr>
</table>

<table>
<tr><td>On Application Exit</td><td>Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr><tr><td>Restart Application</td><td>Opens an ICA session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
<tr><td>Prompt for Credentials on Application Restart</td><td>This setting item is available only when Restart Application is selected for On Application Exit. Click to select whether to prompt for credentials or not when an ICA session restarts.</td></tr>
<tr><td>Manual Parameters</td><td>Type in parameters for extended parameter passing.</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Color Depth	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **16 Bit**, **24 Bit**, and **Automatic**.
Window Size	This item is available only when **Regular Window** is selected. Click the drop-down menu to select the desired window size of a Citrix ICA session. Four options are available: **Full Screen**, **1280x1024**, **1024x768**, and **800x600**.
Window Mode	Click the drop-down menu to select the desired window mode. Two options are available: **Regular Window** and **Seamless Window**.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.

Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a delivered application.
Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.
Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
Network Protocol	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: **TCP/IP**, **TCP/IP + HTTP server location**, and **SSL/TLS + HTTPS server location**.
Enable Automatic Reconnect	Check/Uncheck to enable/disable automatic reconnecting after an ICA session was interrupted.
Number of Retries	Click the drop-down menu to select the number of retries, ranging from 1 to 10.
Delay between Retries	Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.
Enable Audio	Check/Uncheck to enable/disable sound in an ICA session.

<table>
<tr><td>Audio Quality</td><td>Click the drop-down menu to choose the desired sound quality in an ICA session. Three options are available: High Quality, Medium Quality, and Low Quality.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>High Quality</td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr><tr><td>Medium Quality</td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr><tr><td>Low Quality</td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr></table></td></tr>
<tr><td>Enable Audio Input</td><td>Check/Uncheck to enable/disable audio input in an ICA session.</td></tr>
<tr><td>Windows Key Combination</td><td>Click the drop-down menu to select where to apply Windows Key Combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>USB Storage</td><td rowspan="5">Please refer to “Advanced Quick Connection Settings for Citrix ICA Sessions” on page 64 for detailed instructions on these similar settings.</td></tr>
<tr><td>Printers</td></tr>
<tr><td>Redirect Connected USB Devices</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
</table>

Settings for the Connection Type of Server Connection

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 182.
- For descriptions of settings for the connection type of StoreFront, please refer to "Settings for the Connection Type of StoreFront" on page 187.
- Fore descriptions of settings for the connection type of VDI-in-a-Box, please refer to "Settings for the Connection Type of VDI-in-a-Box" on page 192.
- For descriptions of available settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 197.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 202.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when Server Connection is selected.

Six connection types are available:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).</td></tr>
<tr><td>StoreFront</td><td>Provides access to virtual desktops and applications through a StoreFront.</td></tr>
<tr><td>VDI-in-a-Box</td><td>Provides access to virtual desktops through VDI-in-a-Box.</td></tr>
<tr><td>XenDesktop</td><td>Provides access to virtual desktops for an earlier version of XenDesktop.</td></tr>
<tr><td>XenApp</td><td>Provides access to virtual applications for an earlier version of XenApp.</td></tr>
<tr><td>Server Connection</td><td>Provides access to servers for administration (XenApp servers only).</td></tr>
</table>

Refer to the table below for Citrix products and recommended connection types:

<table>
<tr><th>Citrix Product</th><th>Recommended Connection Type</th></tr>
<tr><td>XenApp 6.5 or earlier</td><td>XenApp / Web Logon</td></tr>
<tr><td>XenDesktop 5.6 or earlier</td><td>XenDesktop / Web Logon</td></tr>
<tr><td>Virtual Apps and Desktops (XenApp/XenDesktop 7.5 or later)</td><td>StoreFront / Web Logon</td></tr>
<tr><td>VDI-in-a-Box</td><td>VDI-in-a-Box / Web Logon</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Server Address</td><td>Type in the IP address / URL / FQDN of the XenApp server.

NOTE: Server Connection only supports connections to XenApp servers.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.</td></tr>
<tr><td>Server Name</td><td>Type in the name of the server.</td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a Citrix ICA session automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>

NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.</td></tr>
</table>

<table>
<tr><td>On Application Exit</td><td>Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Local Linux desktop.</td></tr><tr><td>Restart Application</td><td>Opens an ICA session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
<tr><td>Prompt for Credentials on Application Restart</td><td>This setting item is available only when Restart Application is selected for On Application Exit. Click to select whether to prompt for credentials or not when an ICA session restarts.</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Use Toolbar	Click the drop-down menu to enable/disable the Citrix (Desktop Viewer) Toolbar.
Color Depth	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **16 Bit**, **24 Bit**, and **Automatic**.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Four options are available: **Full Screen**, **1280x1024**, **1024x768**, and **800x600**.
Device Mapping	
Item	**Description**
Mapping Local USB Storage	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session. **NOTE:** You need to enable local USB storage drive(s) as well. See section "3.4.3 Configuring Settings for USB Storage Devices" on page 94 for details.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE:** This setting item is not applicable to your mt182L. However, if you use a serial-based barcode scanner, and attach it to your mt182L with a serial-to-USB adapter, you need to enable this setting in order to use the local barcode scanner in a virtual server desktop.

Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions. **NOTE:** To enable locally attached printer(s), please refer to section "3.4.8 Adding a Local Printer" on page 99 for detailed instructions.
Connection Settings	
Item	**Description**
Rendering Type	Click the drop-down menu to select resources rendering on the endpoint or the server. Two options are available: **Server Rendering** and **Client Rendering**. **NOTE:** The **Client Rendering** option may not be available on your system.
HDX RealTime WebCam	This item is available only when **Client Rendering** is selected. When **Yes** is selected, a locally attached webcam can be used in an ICA session.
Use H264 Compression	Click to enable/disable H.264 compression support on the client, allowing session data are sent from the server side using H.264 format encoding.
Network Protocol	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: **TCP/IP**, **TCP/IP + HTTP server location**, and **SSL/TLS + HTTPS server location**.
Enable Automatic Reconnect	Check/Uncheck to enable/disable automatic reconnecting after an ICA session was interrupted. **NOTE:** Automatic reconnecting (Auto Client Reconnect) may not work for a XenDesktop ICA session. This is a known issue. For more details, please visit Citrix websites at support.citrix.com or www.citrix.com.
Number of Retries	Click the drop-down menu to select the number of retries, ranging from 1 to 10.
Delay between Retries	Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.
Enable Audio	Check/Uncheck to enable/disable sound in an ICA session.

<table>
<tr><td>Audio Quality</td><td>Click the drop-down menu to choose the desired sound quality in an ICA session. Three options are available: High Quality, Medium Quality, and Low Quality.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>High Quality</td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr><tr><td>Medium Quality</td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr><tr><td>Low Quality</td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr></table></td></tr>
<tr><td>Enable Audio Input</td><td>Check/Uncheck to enable/disable audio input in an ICA session.</td></tr>
<tr><td>Windows Key Combination</td><td>Click the drop-down menu to select where to apply Windows Key Combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">USB Redirection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>USB Storage</td><td rowspan="5">Please refer to “Advanced Quick Connection Settings for Citrix ICA Sessions” on page 64 for detailed instructions on these similar settings.</td></tr>
<tr><td>Printers</td></tr>
<tr><td>Redirect Connected USB Devices</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
</table>

3.6.12 Configuring Basic VMware View Connection Settings

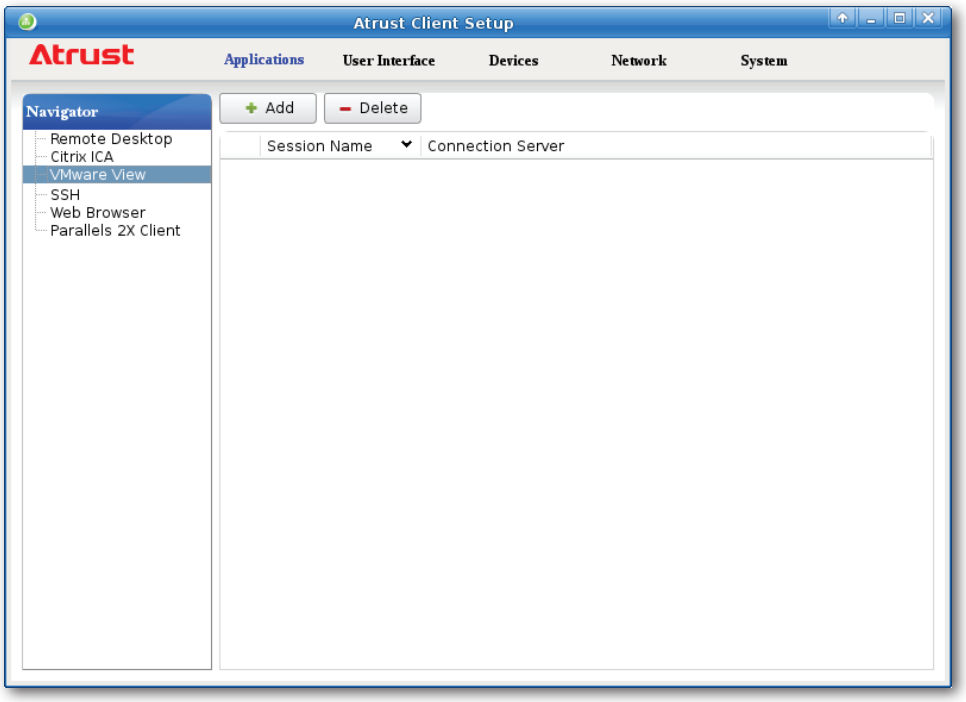
The **VMware View** setting enables you to configure View connection settings for VMware View or Horizon View services and create shortcuts on the local desktop and START menu for service access. You can access on-demand services for work simply through these shortcuts.

NOTE

- For more information on VMware desktop virtualization solutions, please visit VMware website at www.vmware.com.

To quickly configure VMware View connection settings, please do the following:

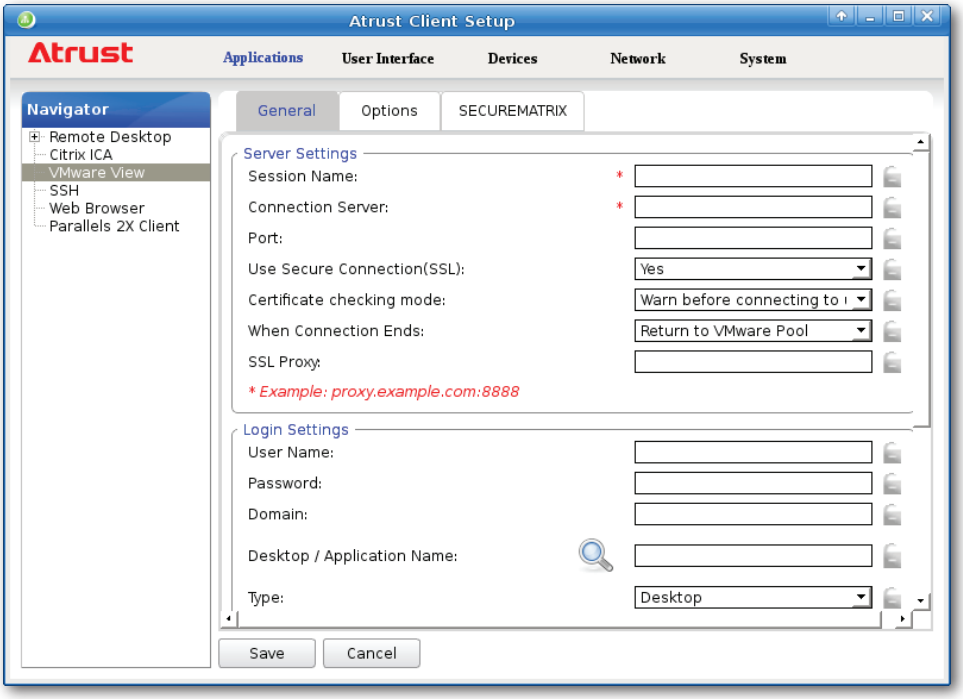
1. On Atrust Client Setup, click **Applications** > **VMware View**.
2. The View Connection list appears in the Configuration area.



NOTE

- If you haven't created any entry, the View Connection list will be empty.

3. Click **Add** on the top of the View Connection list to add a new entry of View connection.



4. Type in the desired session name and the computer name or IP address of the View Connection Server, and then click **Save** to confirm.

> **NOTE**
>
> - These are the only required fields for the creation of a service access shortcut on the desktop. Other data can be provided during the period of service access. Depending on your needs, you might choose to type in more other data.

5. The new entry is added to the View Connection list and the access shortcuts are automatically created on the local desktop and START menu.

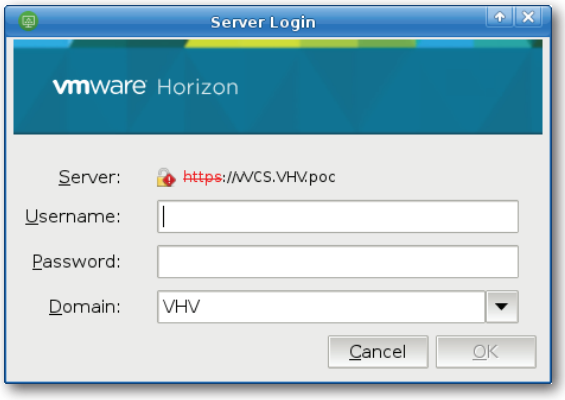
3.6.13 Accessing VMware View or Horizon View Services

To access VMware View or Horizon View services, please do the following:

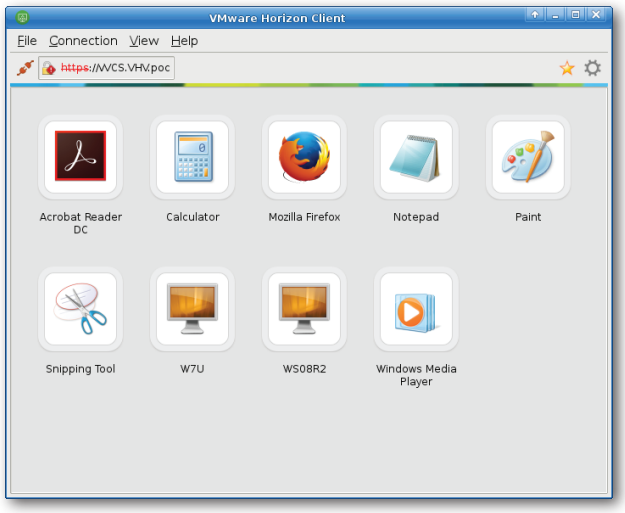
1. Double click the created (customized) access shortcut on the desktop.

> **NOTE**
>
> - A window might appear with a certificate message about the remote server. Consult the IT administrator for details and ensure the connection is secure ***first***. To import a security certificate, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73. To bypass, click **Connect Insecurely**.

2. A Welcome window might appear. Click **OK** to continue.
3. A window appears prompting for the credentials. Enter your user name, password, click the Domain drop-down menu to select the domain, and then click **OK**.



4. A window appears with available desktops and/or applications for the provided credentials.

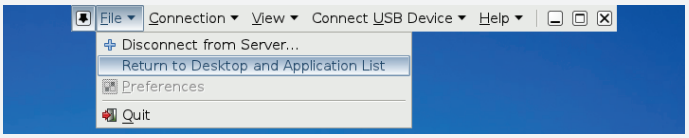


5. Double click to select the desired desktop or application.

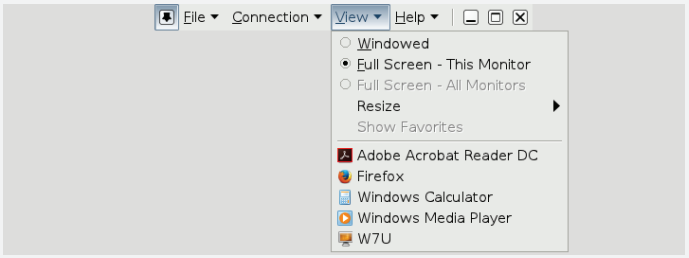
6. The selected desktop or application will be displayed on the screen.

NOTE

- Your desktop or application will be displayed in full screen. You can:
  - ✧ Click **File** > **Return to Desktop and Application List** on the top tool bar to recall the Desktop and Application list.



  - ✧ Click **View** on the top tool bar to switch to a virtual desktop or application.



3.6.14 Configuring Advanced View Connection Settings

The table below provides a description of each setting item for View connections. Please refer to this table to configure advanced settings and customize shortcuts on the local desktop and START menu for service access.

General Sub-tab

Server Settings	
Item	**Description**
Session Name	Type in the name for VMware View or Horizon View sessions.
Connection Server	Type in the computer name or IP address of the View Connection Server. **NOTE:** For more information on View Connection Server, please visit VMware website at www.vmware.com.
Port	Type in the port number used to communicate with the View Connection Server. To use the default value, simply leave it blank.
Use secure connection (SSL)	Check/Uncheck to enable/disable secure connection.
Certificate Checking Mode	Click the drop-down menu to select if to check server identity certificates and if to connect to untrusted servers. Three options are available: **Do not verify server identity certificates**, **Warn before connecting to untrusted servers**, and **Never connect to untrusted servers**.
When Connection Ends	Click the drop-down menu to select what to do when the connection ends. Two options are available: **Return to VMware Pool** and **Quit VMware Client**.

Option	**Description**
Return to VMware Pool	When the connection ends, return to the Desktop and Application list for given credentials.
Quit VMware Client	When the connection ends, close VMware Client. To access virtual desktops and applications, you need to provide the credentials again.

SSL Proxy	Type in the URL / IP address (including a port number) of an SSL proxy if any.
Login Settings	
Item	**Description**
Username	Type in the user name for authentication.
Password	Type in the password for authentication.
Domain	Type in the domain name of the View Connection Server.
Desktop / Application Name	Type in the desktop / application name. Or, leave it blank for users to select one. **NOTE:** You can use the Search icon to help you discover available desktops or applications for a given set of credentials.

<table>
<tr><td>Type</td><td>Click the drop-down menu to select the correct type.

NOTE: Select Desktop for a desktop name given in the previous setting; Application for an application name.</td></tr>
<tr><td>Verify before Access</td><td>Click the drop-down menu to select whether to verify the entitlement to the virtual desktop or application provided in the previous setting item:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Yes</td><td>Verify the entitlement to the virtual desktop or application provided in the previous setting item. Stop if the given credentials do not pass this verification.</td></tr><tr><td>No</td><td>If the given credentials are not entitled to the virtual desktop or application provided in the previous setting item, just ignore that error and provide the Desktop and Application list available for that credentials.</td></tr></table></td></tr>
<tr><td>Remember Credentials for the next login</td><td>Click the drop-down menu to select whether to remember the logon credentials.</td></tr>
<tr><td>Preferred Display Protocol</td><td>Click the drop-down menu to select the desired display protocol. Three options are available: Manual, Microsoft RDP, and PCoIP.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Manual</td><td>Manually select the desired display protocol.</td></tr><tr><td>Microsoft RDP</td><td>Use Microsoft RDP as the display protocol.</td></tr><tr><td>PCoIP</td><td>Use VMware PCoIP as the display protocol.</td></tr></table></td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Non-Interactive Mode</td><td>Select Yes or No to allow or disallow the Non-Interactive mode. The default is to use the Non-Interactive mode.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Yes</td><td>The Non-Interactive mode is used. Users are not allowed to re-select different settings if the settings have been specified in View connection settings.</td></tr><tr><td>No</td><td>The Interactive mode is used. Users are allowed to re-select different settings even if the settings have been specified in View connection settings.</td></tr></table></td></tr>
</table>

<table>
<tr>
<td>Autostart When Startup</td>
<td>
Select whether to open a VMware View or Horizon View session automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired VMware View session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired VMware View or Horizon View session and perform the configured action after exiting the session.

Available actions include:
• Returning to the local desktop
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.
</td>
</tr>
<tr>
<td>On Application Exit</td>
<td>
Select what to do when a VMware View or Horizon View session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Returns to the local desktop.</td></tr>
<tr><td>Restart Application</td><td>Opens a VMware View or Horizon View session again.</td></tr>
<tr><td>Reboot</td><td>Restarts your thin client.</td></tr>
<tr><td>Shutdown</td><td>Turns off your thin client.</td></tr>
</table>
</td>
</tr>
</table>

Options Sub-tab

<table>
<tr><th colspan="2">Window Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Resolution</td><td>Click the drop-down menu to select the desired display size of a View session. Three options are available: Full Screen, Large Window, and Small Window.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Full Screen</td><td>Opens the selected View session in full screen.</td></tr><tr><td>Large Window</td><td>Opens the selected View session in a large window.</td></tr><tr><td>Small Window</td><td>Opens the selected View session in a small window.</td></tr></table></td></tr>
<tr><td>Window Mode</td><td>Click the drop-down menu to select the window mode. Two options are available: Regular Window and Seamless Window.</td></tr>
<tr><td>Use Toolbar</td><td>Click the drop-down menu to select if the Toolbar is accessible in a session.</td></tr>
<tr><th colspan="2">USB Redirection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Mass Storage</td><td rowspan="6">Please refer to “Advanced Quick Connection Settings for VMware View Sessions” on page 66 for detailed instructions on these similar settings.</td></tr>
<tr><td>Smart Card</td></tr>
<tr><td>Human Interface Device</td></tr>
<tr><td>Printer</td></tr>
<tr><td>Plugged USB Devices</td></tr>
<tr><td>Redirection Rules</td></tr>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Printer Mapping</td><td>Click to enable/disable printer mapping for VMware View connections.

NOTE: You need to add a local or network printer for your mt182L first, and then enable this feature here to use that mapped printer in a virtual desktop session.

NOTE: For detailed instructions on how to add a local or network printer for your thin client, please refer to section “3.4.8 Adding a Local Printer” on page 99 or “3.4.9 Adding a Network Printer” on page 102.

NOTE: Even you disable printer mapping, your printer might still be redirected to a virtual desktop session if Printer Redirection is enabled (see above settings in this table).</td></tr>
</table>

SECUREMATRIX Sub-tab

Connection Settings	
Item	**Description**
Use SECUREMATRIX	Check to use SECUREMATRIX authentication.
GSB Server Address	Type the server address of GSB server, the server for SECUREMATRIX authentication service.
Username	Type your user name (Login ID).

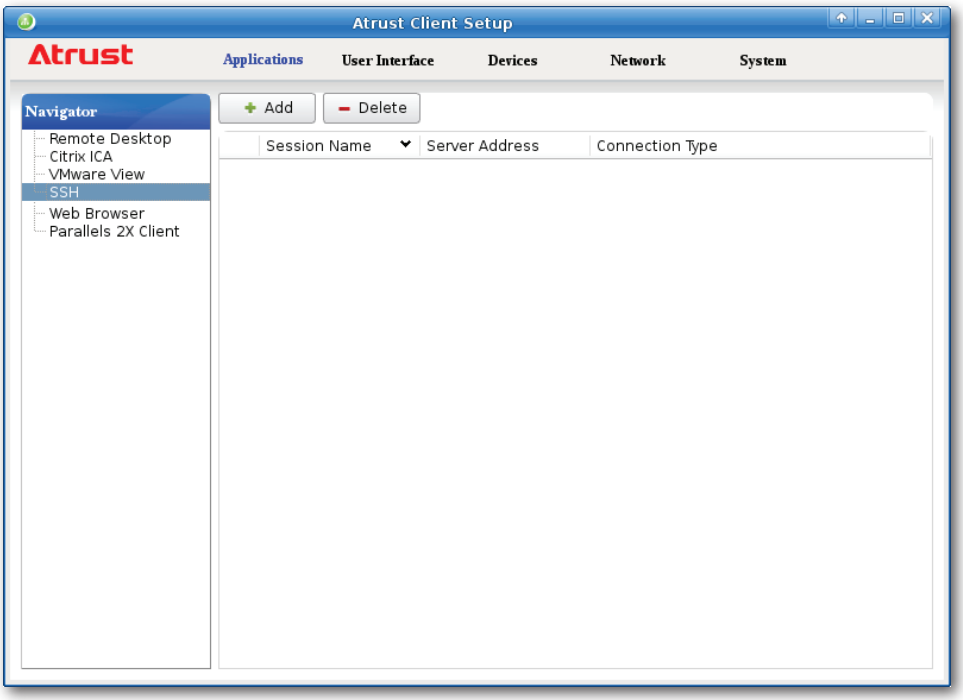
NOTE

- For details, please refer to "A.3 Using SECUREMATRIX Authentication for VMware Connections" on page 252.

3.6.15 Configuring SSH Connection Settings

To configure SSH (Secure SHell) connection settings, please do the following:

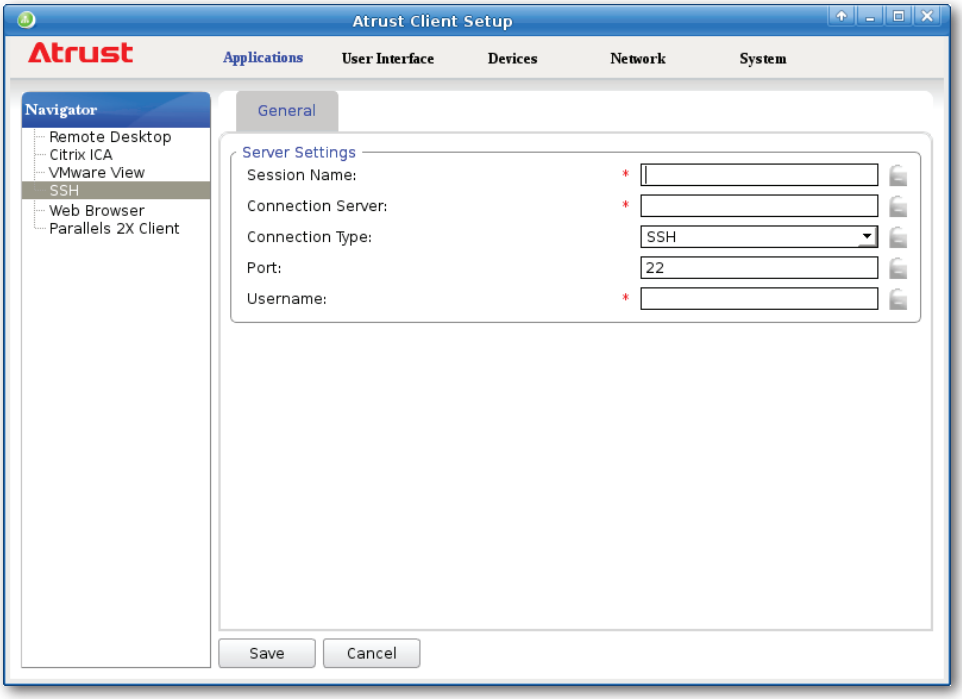
1. On Atrust Client Setup, click **Applications** > **SSH**.
2. The SSH Connection list appears in the Configuration area.



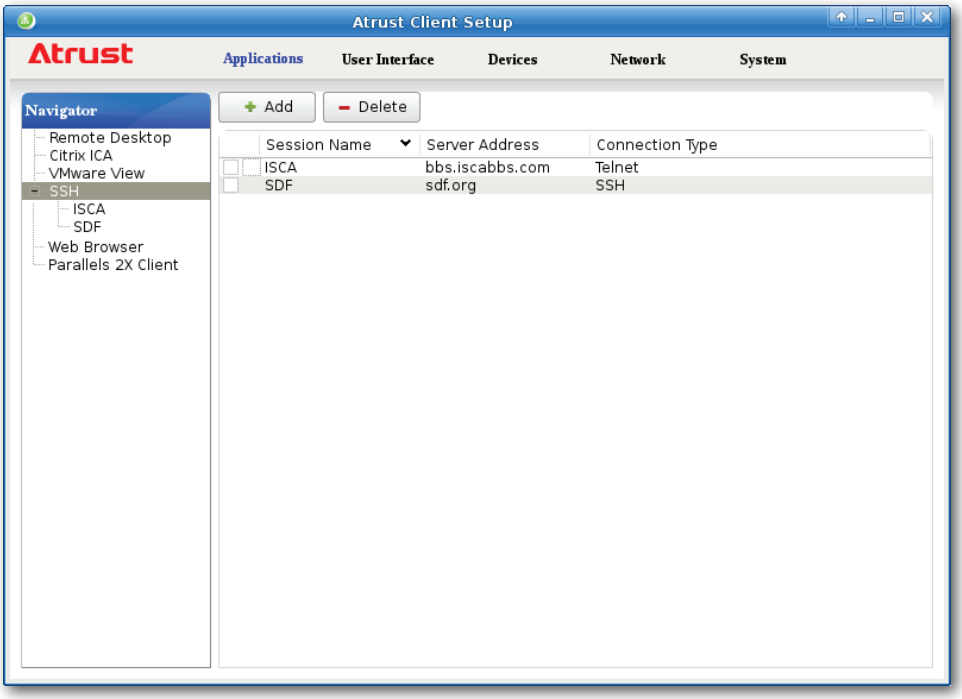
NOTE

- If you haven't created any entry, the SSH Connection list will be empty.

3. Click **Add** on the top of the SSH Connection list to add a new entry of SSH connection.



4. Click the drop-down menu to select the desired connection type. Two types are available: **SSH** and **Telnet**.
5. Type in the desired session name, the computer name or IP address of the remote server, the user name, and then click **Save** to confirm.
6. The new entry is added to the SSH Connection list and the access shortcuts are automatically created on the local desktop and START menu.

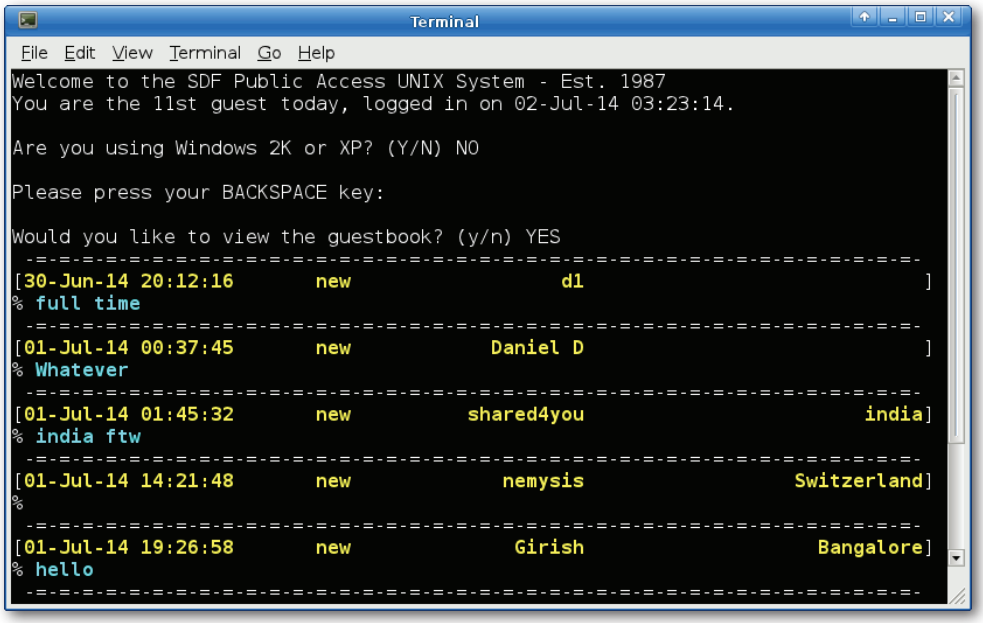


3.6.16 Launching SSH and Telnet Sessions

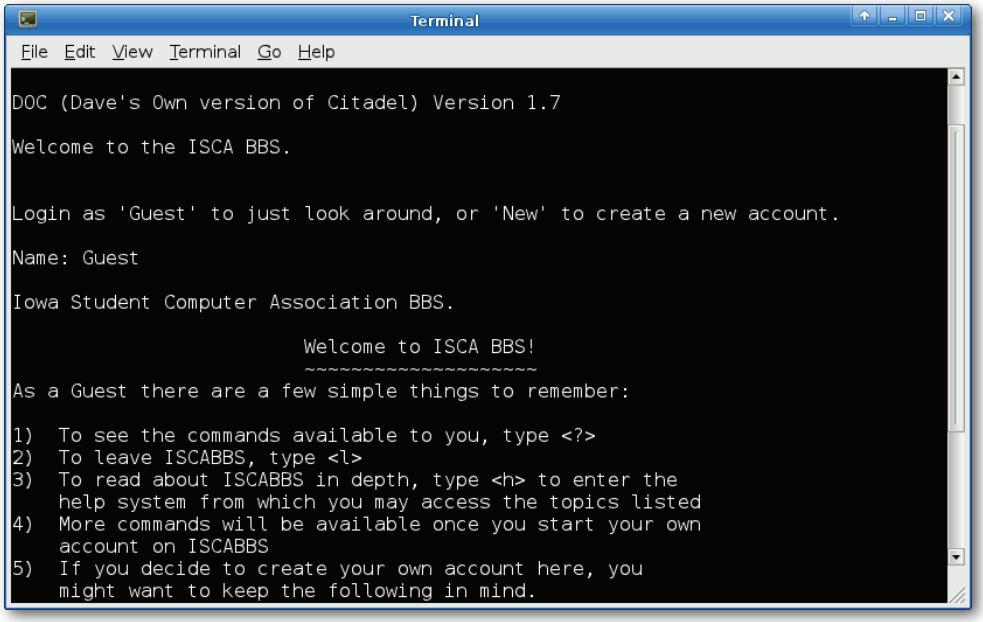
To launch an SSH or Telnet session, please do the following:

1. Double click the created shortcut on the local desktop.
2. The SSH or Telnet session starts in the opened window.

Example: SSH Session



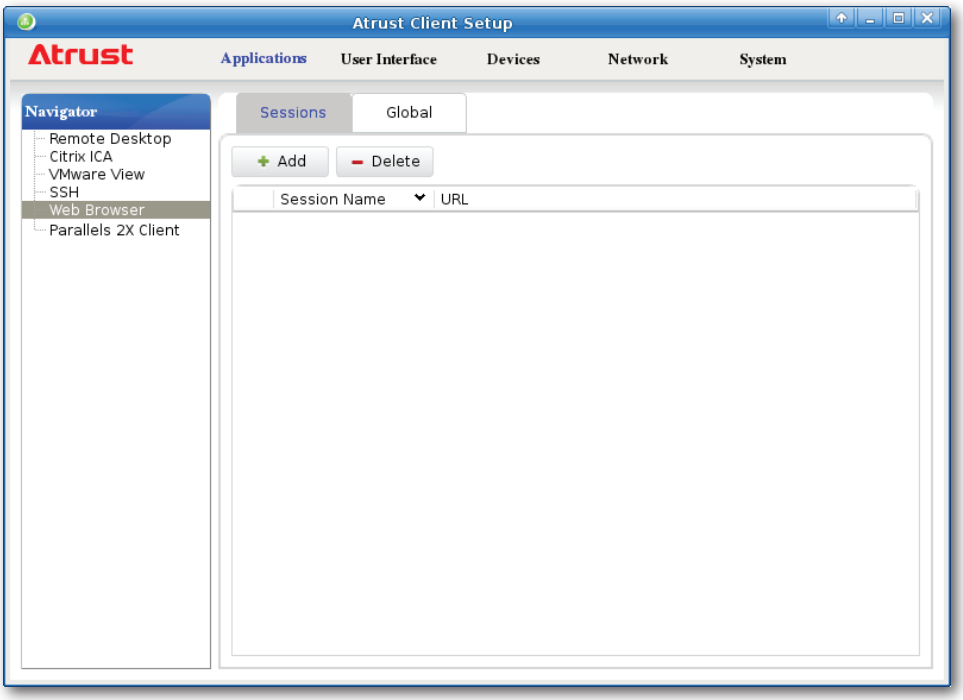
Example: Telnet Session



3.6.17 Configuring Basic Settings for Browser Sessions

To configure basic settings for a browser session, please do the following:

1. On Atrust Client Setup, click **Applications** > **Web Browser**.
2. The Web Page Access list appears in the Configuration area.

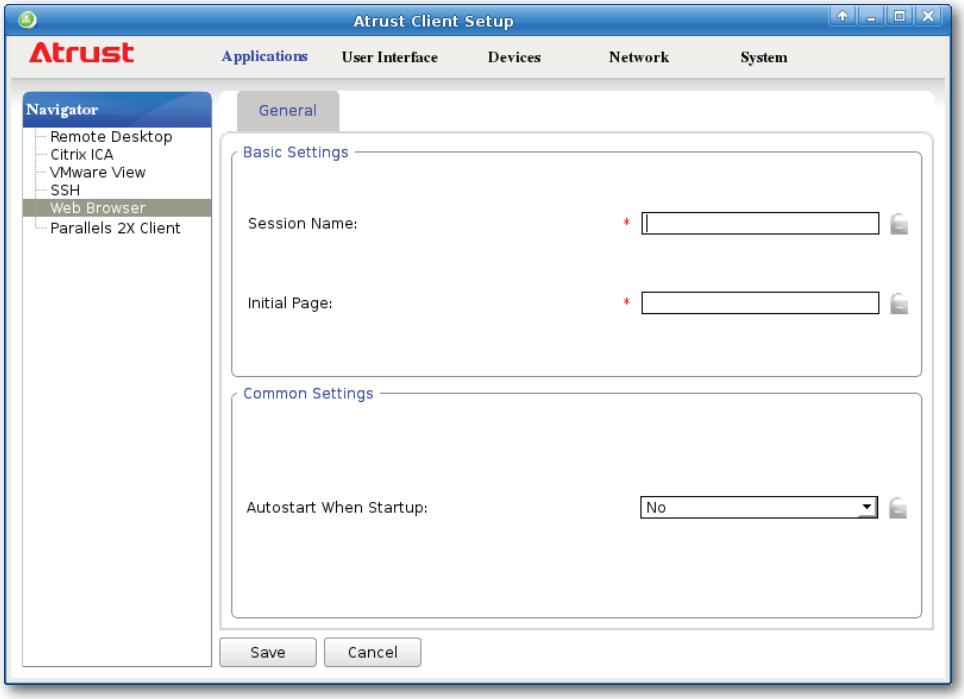


NOTE

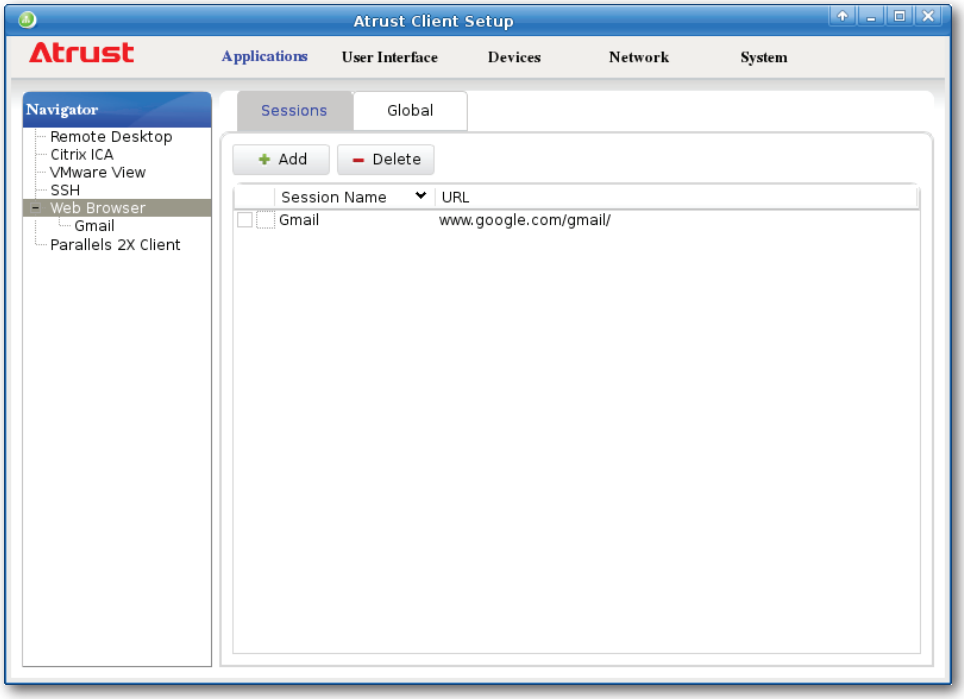
- If you haven't created any entry, the Web Page Access list will be empty.

3. Click **Add** on the top of the Web Page Access list to add a new entry.

4. Type in the desired session name, the URL of the web page, and then click **Save** to confirm.



5. The new entry is added to the Web Page Access list and the access shortcuts are automatically created on the local desktop and START menu.

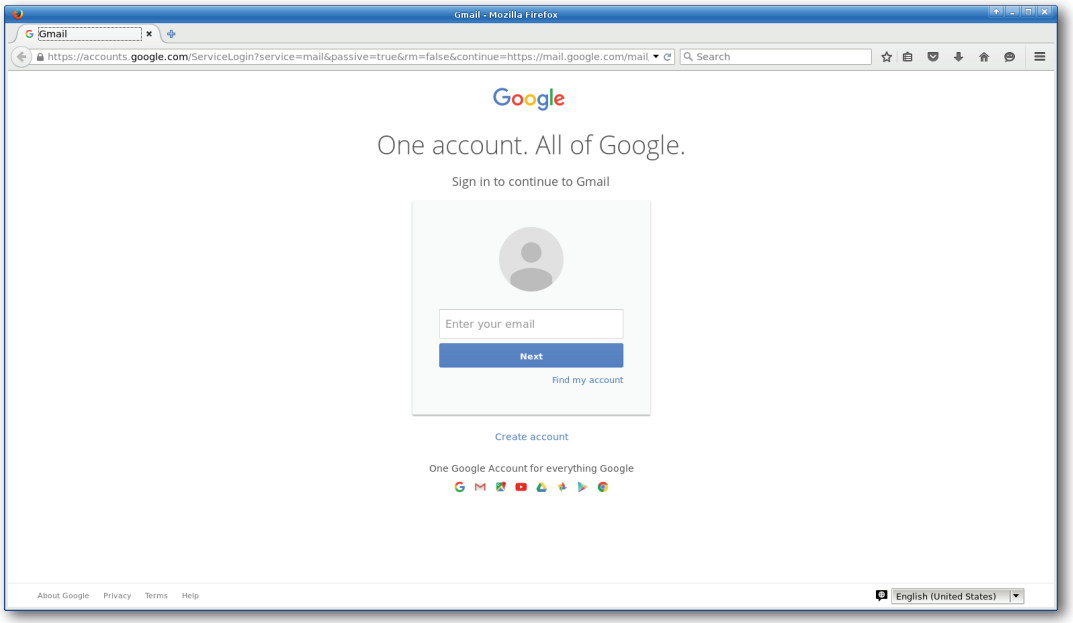


3.6.18 Launching Browser Sessions

To launch a browser session, please do the following:

1. Double click the created shortcut on the local desktop or START menu.
2. The session starts in the opened browser.

Example: Gmail Login Session



3.6.19 Configuring Advanced Settings for Browser Sessions

The tables below provide a description of each setting item for browser sessions. Please refer to these tables to configure advanced settings and customize for Web access.

General Sub-tab

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for browser sessions.</td></tr>
<tr><td>Initial Page</td><td>Type in the URL of the Web page.</td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a browser session automatically or not when your mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired browser session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired browser session.</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The default. The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>

NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.</td></tr>
</table>

Global Sub-tab

Common Settings	
Item	**Description**
Home Page	Set the desired home page for the web browser.

3.6.20 Configuring Basic RAS / RDP Connection Settings

The **Parallels 2X Client** setting allows you to configure RAS / RDP connection settings and create shortcuts on the local desktop and START menu for service access. You can access remote desktops or applications for work simply through these shortcuts.

NOTE

- For more information on RAS (Remote Application Server) and RDP (Remote Desktop Protocol), please visit Parallels website at www.parallels.com.

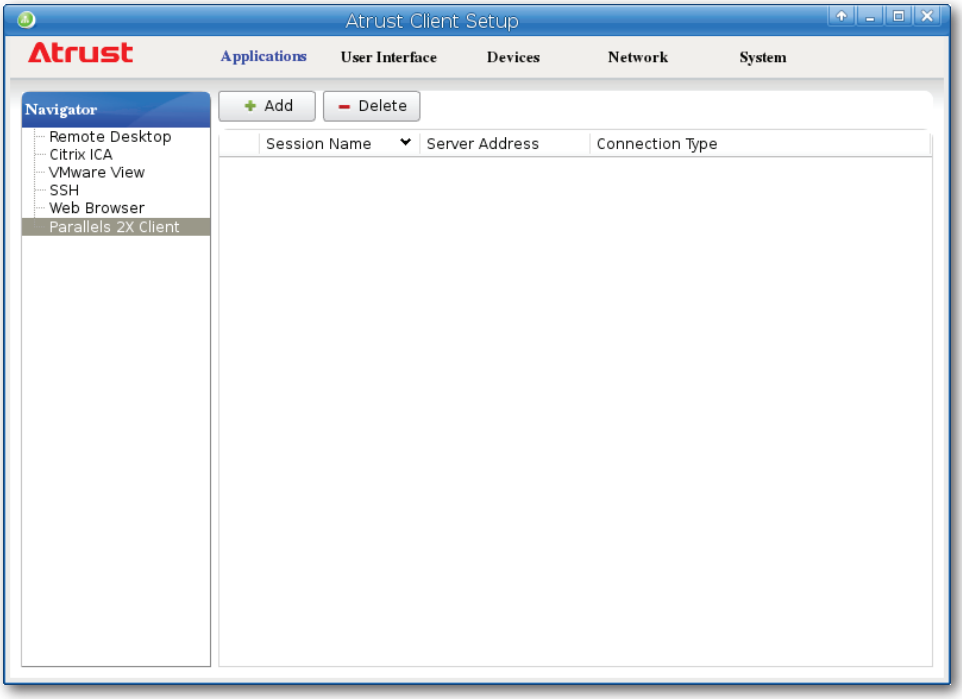
Two connection types are available:

Connection Type	Description	Page
Parallels Remote Application Server	Select to access remote desktops and applications via Parallels Remote Application Server.	229
Standard RDP	Select to access remote desktops via standard Microsoft Remote Desktop Services.	231

Connection Type: Parallels Remote Application Server

To quickly configure RAS connection settings for this connection type, please do the following:

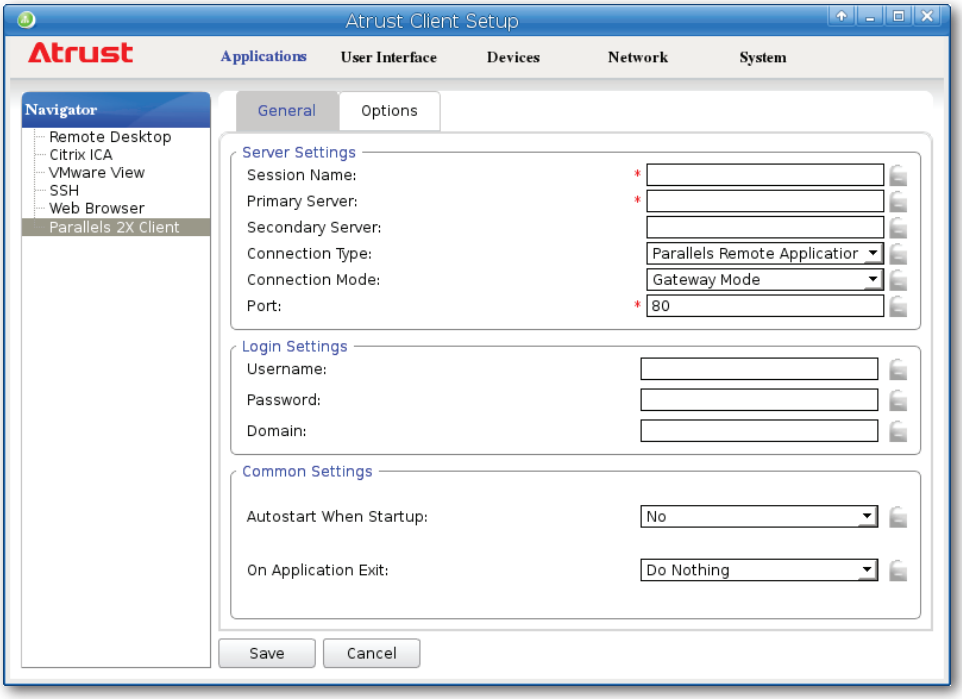
1. On Atrust Client Setup, Click **Applications** > **Parallels 2X Client**.
2. The RAS / RDP Connection list appears in the Configuration area.



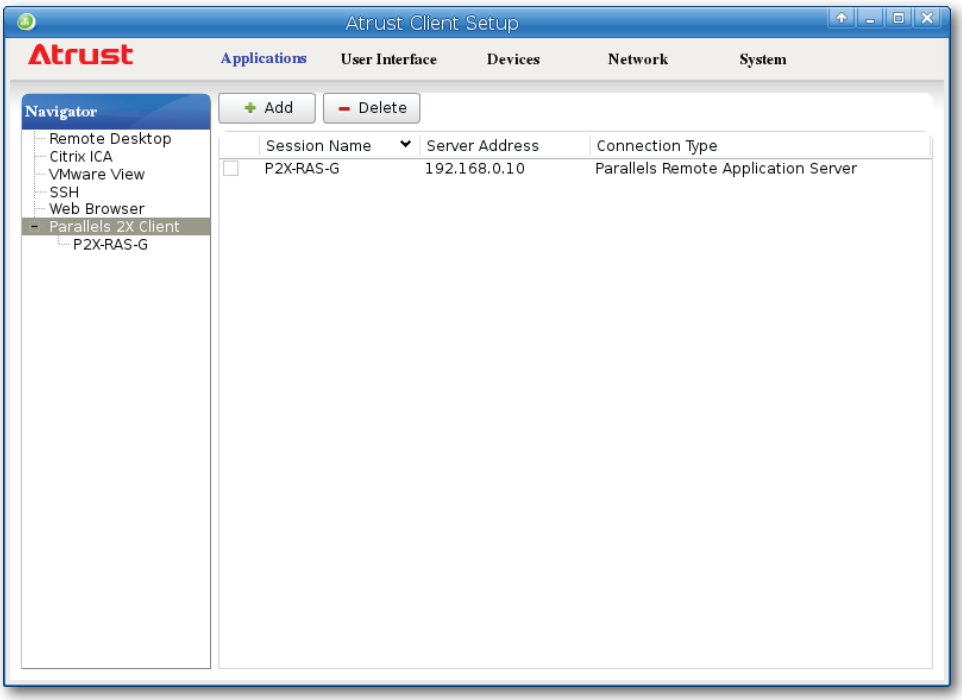
NOTE

- If you haven't created any entry, the RAS / RDP Connection list will be empty.

3. Click **Add** on the top of the RAS / RDP Connection list to create a new entry of RAS connection.



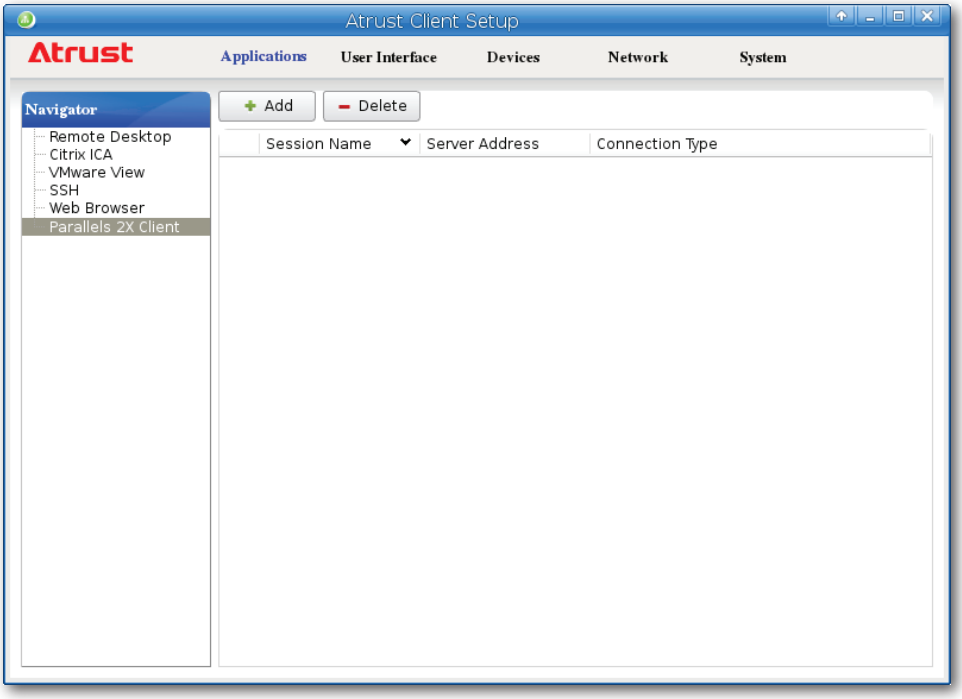
4. On **General** sub-tab, ensure that **Parallels Remote Application Server** is selected for the connection type, type in the session name and the primary server address under the Server Settings section.
5. Click **Save** to confirm.
6. The new entry is added to the RAS / RDP Connection list and the access shortcuts are automatically created on the local desktop and START menu.



Connection Type: Standard RDP

To quickly configure RDP connection settings for this connection type, please do the following:

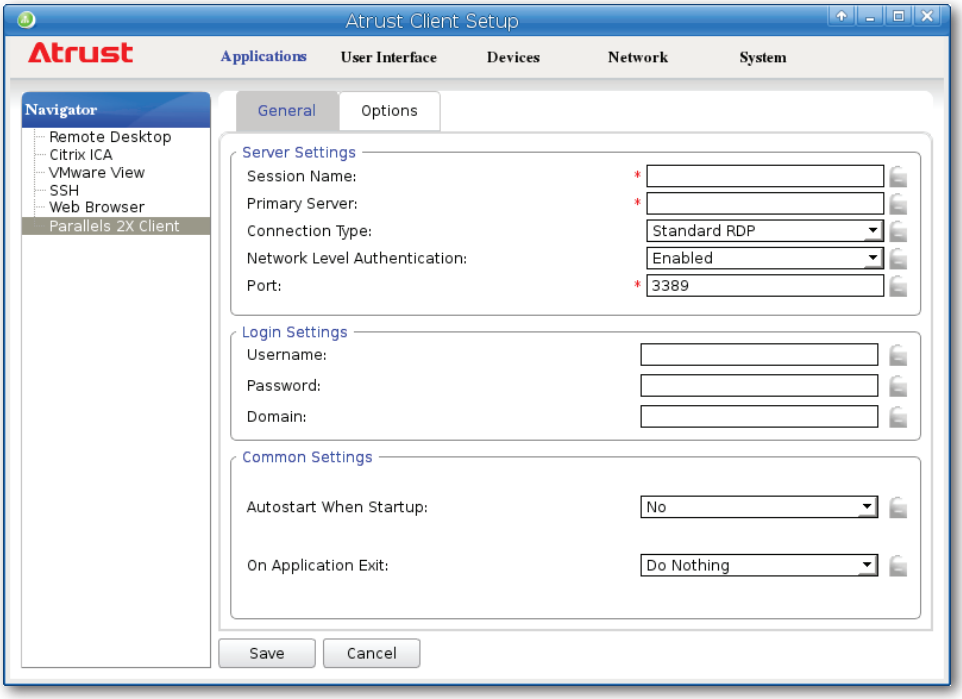
1. On Atrust Client Setup, Click **Applications** > **Parallels 2X Client**.
2. The RAS / RDP Connection list appears in the Configuration area.



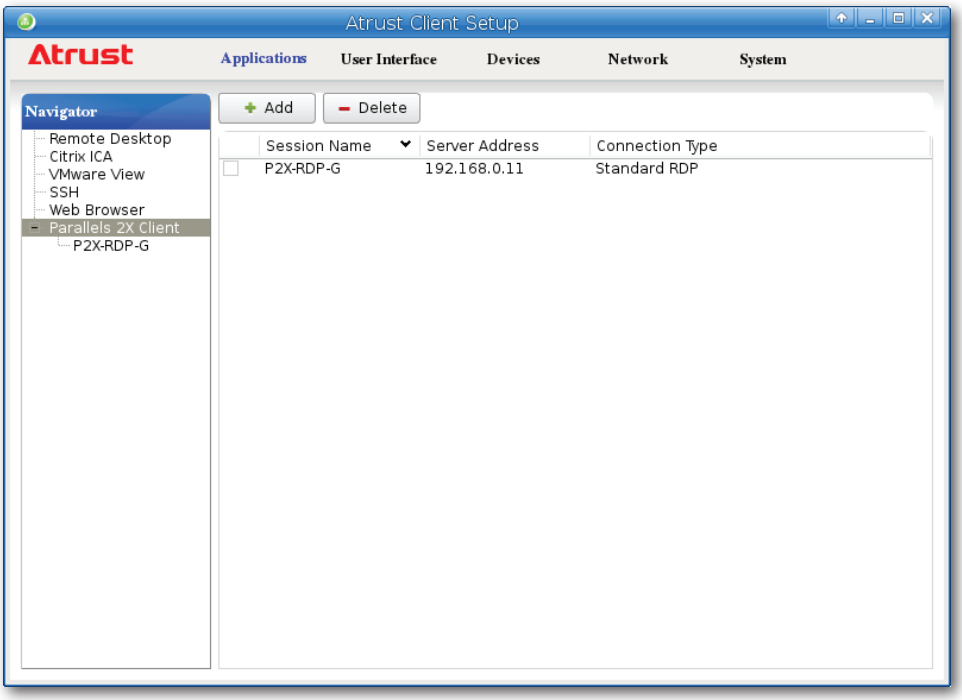
NOTE

- If you haven't created any entry, the RAS / RDP Connection list will be empty.

3. Click **Add** on the top of the RAS / RDP Connection list to create a new entry of RDP connection.



4. On **General** sub-tab, ensure that **Standard RDP** is selected for the connection type, type in the session name and the primary server address under the Server Settings section.
5. Click **Save** to confirm.
6. The new entry is added to the RAS / RDP Connection list and the access shortcuts are automatically created on the local desktop and START menu.

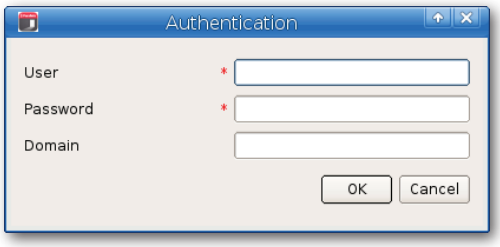


3.6.21 Accessing Remote Desktops or Applications

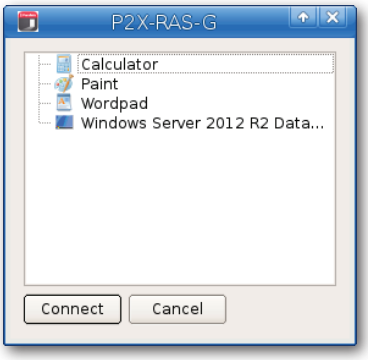
Connection Type: Parallels Remote Application Server

To access remote desktops or applications, please do the following:

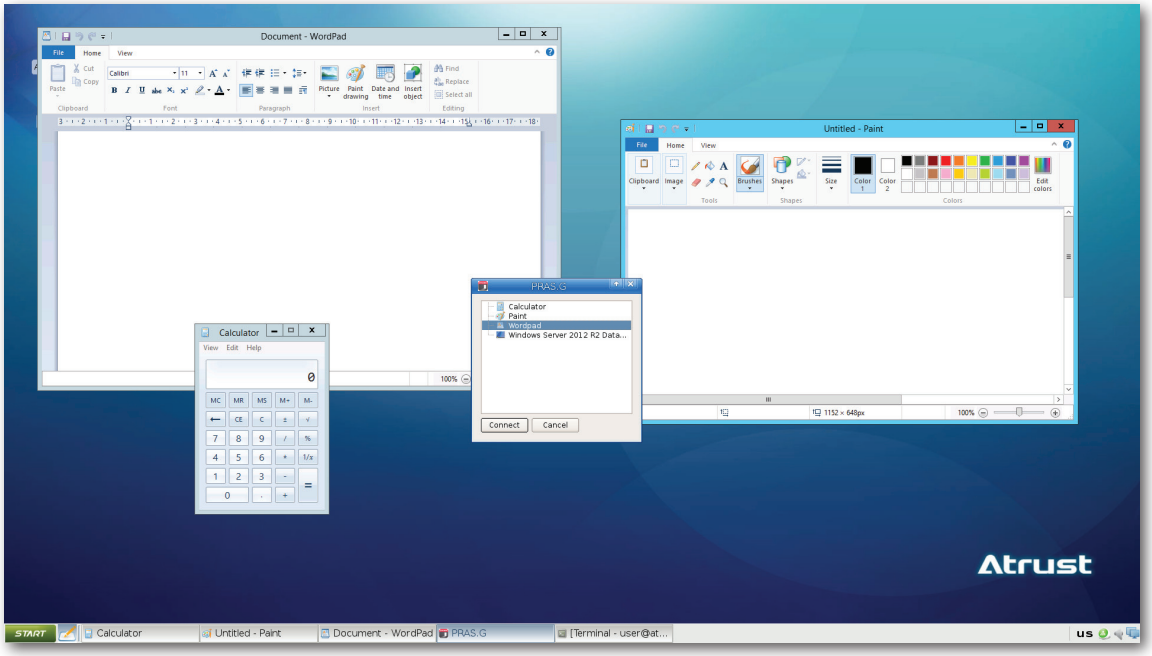
1. Double click the created shortcut on the desktop.
2. On the opened window, provide your credentials as required, and then click **OK**.

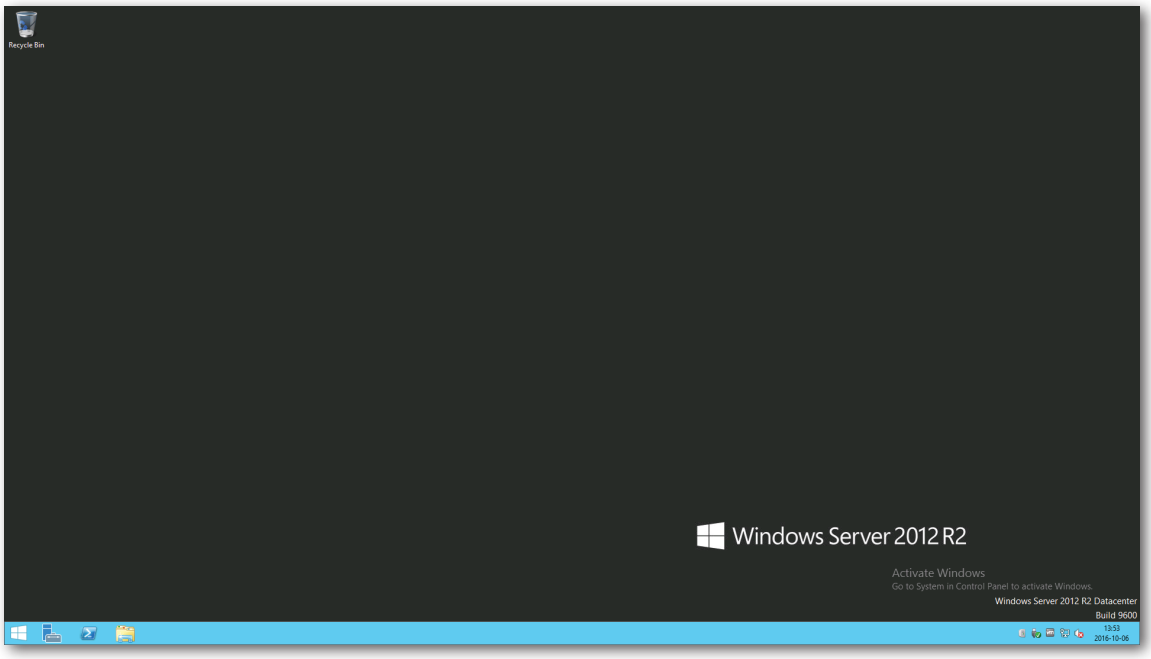


3. A window appears with available applications and desktops.



4. Click to select the desired application or desktop, and then click **Connect** to confirm.
5. The application or desktop will be displayed on the screen.





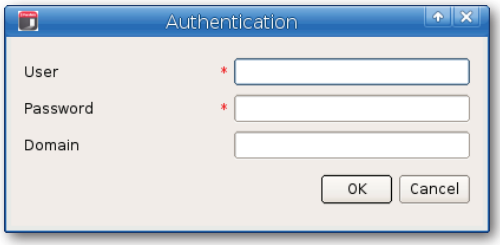
NOTE

- The desktop will be displayed in full screen.

Connection Type: Standard RDP

To access remote desktops, please do the following:

1. Double click the created shortcut on the desktop.
2. On the opened window, provide your credentials as required, and then click **OK**.



3. The desktop will be displayed in full screen.

3.6.22 Configuring Advanced RAS / RDP Connection Settings

The tables below provide a description of each setting item for RAS / RDP connections. Please refer to these tables to configure advanced settings and customize shortcuts on local desktop and START menu for service access.

NOTE

- Please note that available settings vary with the selected connection type.

Settings for the Connection Type of Parallels Remote Application Server

NOTE

- For descriptions of settings for the connection type of Standard RDP, please see "Settings for the Connection Type of Standard RDP" on page 241.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for RAS (Remote Application Server) sessions.</td></tr>
<tr><td>Primary Server</td><td>Type in the computer name or IP address of the server through which to deliver an RAS session.</td></tr>
<tr><td>Secondary Server</td><td>Type in the 2nd computer name or IP address of the server (if available) in case that the primary server fails to deliver a session.</td></tr>
<tr><td>Connection Type</td><td>This table only provides descriptions for available settings when Parallels Remote Application Server is selected.

Two connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Parallels Remote Application Server</td><td>Select to access remote desktops and applications via Parallels Remote Application Server.</td></tr><tr><td>Standard RDP</td><td>Select to access remote desktops via standard Microsoft Remote Desktop Services.</td></tr></table></td></tr>
</table>

<table>
<tr><td>Connection Mode</td><td>Click the drop-down menu to select the desired connection mode. Four options are available:

Option — Description

Gateway Mode — Connected with the RAS (Remote Application Server) Secure Client Gateway and data tunneled through the first available connection.

NOTE: This mode is ideal for servers which are only reachable via the gateway and do not require a high level of security.

Direct Mode — First connected to the RAS (Remote Application Server) Secure Client Gateway for the best available Server and then connected directly with that particular Server.

NOTE: This is best used when the client and the server are on the same network.

Gateway SSL Mode — Connected with the RAS (Remote Application Server) Secure Client Gateway securely and data encypted and tunneled through the first available connection.

Direct SSL Mode — First connected to the RAS (Remote Application Server) Secure Client Gateway using SSL for the best available server and then connect directly with that particular Server.

NOTE: This is best when the client and the server are on the same network and high security safeguards are required.</td></tr>
<tr><td>Port</td><td>The port used by default will be given automatically after you select a connection type and mode. Type a different one if needed.</td></tr>
<tr><td colspan="2">Login Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.

NOTE: Domain is a collection of computers on a network that share a common database and security policy. Leave this field blank if the server doesn’t belong to any domain.</td></tr>
</table>

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>
Select whether to open an RAS session automatically or not when mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired RAS session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired RAS session and perform the configured action after exiting the session.

Available actions include:
• Not to do anything
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The default. The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.
</td></tr>
<tr><td>On Application Exit</td><td>
Select what to do when a Parallel 2X session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Not to do anything.</td></tr>
<tr><td>Restart Application</td><td>Launches an RAS session again.</td></tr>
<tr><td>Reboot</td><td>Restarts your mt182L.</td></tr>
<tr><td>Shutdown</td><td>Turns off your mt182L.</td></tr>
</table>
</td></tr>
</table>

Options Sub-tab

Window Settings	
Item	**Description**
Color Depth	Click the drop-down menu to select the desired color depth for an RAS session. Five options are available: **8 Bit**, **15 Bit**, **16 Bit**, **24 Bit**, and **32 Bit**. **NOTE:** If RemoteFX is enabled in **Graphics Acceleration**, only 32 bit per pixel could be selected here. **NOTE:** You can configure the upper limit of the color depth for an RAS session on the host server. In this case, no matter which color depth you choose here, the value cannot exceed the defined limit.
Graphics Acceleration	Click the drop-down menu to set graphics acceleration. Four options are available: **None**, **Basic**, **RemoteFX**, and **RemoteFX Adaptive**. **NOTE:** Windows® RemoteFX™ is a technology that offers a rich user experience over a network for remote desktop users. **NOTE:** If **RemoteFX** is selected here, 32 bit per pixel color depth will be chosen automatically in **Color Depth**.
Use all monitors for desktop session	Check to use connected and secondary monitors as extended screens.
Span desktop across all monitors	Check to span the launched desktop across all connected monitors.
Published Applications	
Item	**Description**
Use primary monitor only	Check to display launched applications on the primary monitor only. Other monitors connected will not be used and users cannot move application windows to those monitors too.
Optimization Settings	
Item	**Description**
Connection Quality	Select the option that best describes the quality of your network connection. Three options are available: **LAN (Very Fast)**, **Broadband (Fast)**, and **Modem (Slow)**. **NOTE:** Selection here will determine the defaults of items in this section as listed below.
Desktop background	Check to use the desktop background.
Font smoothing	Check to use ClearType® technology to make fonts clear and smooth.
Show window contents while dragging	Check to show window contents while dragging a window.
Menu and window animation	Check to show menu and window animation.
Themes	Check to allow non-classic themes.

<table>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>USB Storage Mapping</td><td>Click the drop-down menu to enable/disable USB storage mapping.

When Enable is selected, users can access the local USB storage devices, such as a USB flash drive and memory card reader, in an RAS session.

NOTE: Atrust Client Setup also allows you to enable or disable the use of locally attached USB storage devices. You need to enable locally attached USB storage devices first in order to use them in an RAS session. The default is enabled.

NOTE: To configure the use of USB storage devices, please refer to section “3.4.3 Configuring Settings for USB Storage Devices” on page 94.</td></tr>
<tr><td>Printer Mapping</td><td>Click the drop-down menu to enable/disable printer mapping.

When Enable is selected, users can access a local or network printer in an RAS session.

NOTE: You need to add a local or network printer for your mt182L first, and then enable this feature here to use that printer in an RAS session.

NOTE: For detailed instructions on how to add a local or network printer for your mt182L, please refer to section “3.4.8 Adding a Local Printer” on page 99 or “3.4.9 Adding a Network Printer” on page 102.</td></tr>
<tr><td>Serial Port Mapping</td><td>Click the drop-down menu to enable/disable serial port mapping.

When Enable is selected, users can access a serial device, such as a barcode scanner, in an RAS session.</td></tr>
<tr><td>Smart Card Mapping</td><td>Click the drop-down menu to enable/disable smart card mapping.

When Enable is selected, users can access smart cards through a smart card reader in an RAS session.</td></tr>
<tr><td>Clipboard Mapping</td><td>Click the drop-down menu to enable/disable Clipboard mapping.</td></tr>
<tr><th colspan="2">Local Resources Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Remote Audio Playback</td><td>Click the drop-down menu to configure the audio playback setting in an RAS session. Three options are available: Play on this computer, Play on remote computer, and Do not play.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Play on this computer</td><td>Allows audio playback in an RAS session using locally attached audio devices.</td></tr>
<tr><td>Do not play</td><td>Disables audio playback in an RAS session using locally attached audio devices.</td></tr>
<tr><td>Play on remote computer</td><td>Allows audio playback in an RAS session using audio devices attached to the remote computer.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td>Remote Audio Recording</td><td>Click the drop-down menu to configure the audio playback setting in an RAS session. Two options are available: Recording from this computer and Do not record.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Recording from this computer</td><td>Allows audio recording in an RAS session using locally attached audio devices.</td></tr><tr><td>Do not record</td><td>Disables audio recording in an RAS session using locally attached audio devices.</td></tr></table></td></tr>
<tr><td>Windows key combination</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><td colspan="2">Proxy Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Use Proxy Server</td><td>Check this item if a proxy server is used and then specify the details.</td></tr>
<tr><td>Proxy Type</td><td>Click the drop-down menu to select the type of the proxy server according to the used protocol.

Four options are available: SOCKS 4, SOCKS 4A, SOCKS 5, and HTTP 1.1.</td></tr>
<tr><td>Proxy Host</td><td>Specify the IP address of the proxy server.</td></tr>
<tr><td>Proxy Port</td><td>Specify the port used for proxy service.</td></tr>
<tr><td>Use Proxy Credentials</td><td>Check if user authentication is required for a proxy server and then specify the credentials.</td></tr>
<tr><td>Username</td><td>Type the user / account name of the proxy server.</td></tr>
<tr><td>Password</td><td>Type the password of the user account.</td></tr>
<tr><td colspan="2">Additional Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Compression</td><td>Click the drop-menu to enable / disable the compression for the data traffic.</td></tr>
</table>

Settings for the Connection Type of Standard RDP

NOTE

- For descriptions of settings for the connection type of Parallels Remote Application Server, please refer to "Settings for the Connection Type of Parallels Remote Application Server" on page 235.

General Sub-tab

Server Settings	
Item	**Description**
Session Name	Type in the name for RDP sessions.
Primary Server	Type in the computer name or IP address of the server through which to deliver an RDP session.
Connection Type	This table only provides descriptions for available settings when **Standard RDP** is selected. Two connection types are available: **Option** / **Description** Parallels Remote Application Server: Select to access remote desktops and applications via Parallels Remote Application Server. Standard RDP: Select to access remote desktops via standard Microsoft Remote Desktop Services.
Network Level Authentication	Select to enable/disable Network Level Authentication. **NOTE:** Network Level Authentication is the authentication method used to enhance the server security by requiring that the user be authenticated before the logon screen is displayed and a session is created. This is a more secure authentication method that can help protect the remote computer from malicious users and software.
Port	The port used by default will be given automatically after you select a connection type and mode. Type a different one if needed.
Login Settings	
Item	**Description**
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server. **NOTE:** Domain is a collection of computers on a network that share a common database and security policy. Leave this field blank if the server doesn't belong to any domain.

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>
Select whether to open an RDP session automatically or not when mt182L is started up (Autostart mode).

NOTE: There are three similar but different modes for your mt182L and only one mode will take effect if all are enabled. Three modes and the order of priority are listed as follows:

<table>
<tr><th>No.</th><th>Mode</th><th>Description</th></tr>
<tr><td>1</td><td>Appliance</td><td>The client will start up directly with the desired Remote Desktop session and perform the configured action after exiting the session.

Available actions include:
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>2</td><td>Autostart</td><td>The client will start up directly with the desired RDP session and perform the configured action after exiting the session.

Available actions include:
• Not to do anything
• Re-launching a new session
• Restarting the thin client
• Turning off the thin client</td></tr>
<tr><td>3</td><td>Quick Connection</td><td>The default. The client will enter Atrust Quick Connection screen after system startup.</td></tr>
</table>
NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.
</td></tr>
<tr><td>On Application Exit</td><td>
Select what to do when an RDP session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do Nothing</td><td>Not to do anything.</td></tr>
<tr><td>Restart Application</td><td>Launches an RDP session again.</td></tr>
<tr><td>Reboot</td><td>Restarts your mt182L.</td></tr>
<tr><td>Shutdown</td><td>Turns off your mt182L.</td></tr>
</table>
</td></tr>
</table>

Options Sub-tab

<table>
<tr><th colspan="2">Window Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Color Depth</td><td>Click the drop-down menu to select the desired color depth for an RDP session. Five options are available: 8 Bit, 15 Bit, 16 Bit, 24 Bit, and 32 Bit.

NOTE: If RemoteFX is enabled in Graphics Acceleration, only 32 bit per pixel could be selected here.

NOTE: You can configure the upper limit of the color depth for an RDP session on the host server. In this case, no matter which color depth you choose here, the value cannot exceed the defined limit.</td></tr>
<tr><td>Resolution</td><td>Click the drop-down menu to select the desired display resolution on an RDP session. Four options are available: Fullscreen, Large Window, Medium Window, and Small Window.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Fullscreen</td><td>Opens an RDP session in full screen with the same display resolution as the local desktop.</td></tr><tr><td>Large Window</td><td>Opens an RDP session in a large display resolution.</td></tr><tr><td>Medium Window</td><td>Opens an RDP session in a medium display resolution.</td></tr><tr><td>Small Window</td><td>Opens an RDP session in a small display resolution.</td></tr></table>
NOTE: To configure the display resolution of the local desktop, please refer to section “3.3.3 Configuring Display Settings” on page 80.</td></tr>
<tr><td>Graphics Acceleration</td><td>Click the drop-down menu to set graphics acceleration. Four options are available: None, Basic, RemoteFX, and RemoteFX Adaptive.

NOTE: Windows® RemoteFX™ is a technology that offers a rich user experience over a network for remote desktop users.

NOTE: If RemoteFX is selected here, 32 bit per pixel color depth will be chosen automatically in Color Depth.</td></tr>
<tr><td>Use all monitors for desktop session</td><td>Check to use connected and secondary monitors as extended screens.</td></tr>
<tr><td>Span desktop across all monitors</td><td>Check to span the launched desktop across all connected monitors.</td></tr>
<tr><th colspan="2">Published Applications</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Use primary monitor only</td><td>Check to display launched applications on the primary monitor only. Other monitors connected will not be used and users cannot move application windows to those monitors too.</td></tr>
</table>

Optimization Settings	
Item	**Description**
Connection Quality	Select the option that best describes the quality of your network connection. Three options are available: **LAN (Very Fast)**, **Broadband (Fast)**, and **Modem (Slow)**. **NOTE:** Selection here will determine the defaults of items in this section as listed below.
Desktop background	Check to use the desktop background.
Font smoothing	Check to use ClearType® technology to make fonts clear and smooth.
Show window contents while dragging	Check to show window contents while dragging a window.
Menu and window animation	Check to show menu and window animation.
Themes	Check to allow non-classic themes.
Connection Settings	
Item	**Description**
USB Storage Mapping	Click the drop-down menu to enable/disable USB storage mapping. When **Enable** is selected, users can access the local USB storage devices, such as a USB flash drive and memory card reader, in an RDP session. **NOTE:** Atrust Client Setup also allows you to enable or disable the use of locally attached USB storage devices. You need to enable locally attached USB storage devices first in order to use them in an RDP session. The default is enabled. **NOTE:** To configure the use of USB storage devices, please refer to section "3.4.3 Configuring Settings for USB Storage Devices" on page 94.
Printer Mapping	Click the drop-down menu to enable/disable printer mapping. When **Enable** is selected, users can access a local or network printer in an RDP session. **NOTE:** You need to add a local or network printer for your mt182L first, and then enable this feature here to use that printer in an RDP session. **NOTE:** For detailed instructions on how to add a local or network printer for your mt182L, please refer to section "3.4.8 Adding a Local Printer" on page 99 or "3.4.9 Adding a Network Printer" on page 102.
Serial Port Mapping	Click the drop-down menu to enable/disable serial port mapping. When **Enable** is selected, users can access a serial device, such as a barcode scanner, in an RDP session.
Smart Card Mapping	Click the drop-down menu to enable/disable smart card mapping. When **Enable** is selected, users can access smart cards through a smart card reader in an RDP session.
Clipboard Mapping	Click the drop-down menu to enable/disable Clipboard mapping.

<table>
<tr><th colspan="2">Local Resources Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Remote Audio Playback</td><td>Click the drop-down menu to configure the audio playback setting in an RDP session. Three options are available: Play on this computer, Play on remote computer, and Do not play.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Play on this computer</td><td>Allows audio playback in an RDP session using locally attached audio devices.</td></tr><tr><td>Do not play</td><td>Disables audio playback in an RDP session using locally attached audio devices.</td></tr><tr><td>Play on remote computer</td><td>Allows audio playback in an RDP session using audio devices attached to the remote computer.</td></tr></table></td></tr>
<tr><td>Remote Audio Recording</td><td>Click the drop-down menu to configure the audio playback setting in a Remote Desktop session. Two options are available: Recording from this computer and Do not record.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Recording from this computer</td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr><tr><td>Do not record</td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr></table></td></tr>
<tr><td>Windows key combination</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On the local computer, On the remote server, and In full screen mode only.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>On the local computer</td><td>Applies to the local desktop only.</td></tr><tr><td>On the remote server</td><td>Applies to the virtual desktop only.</td></tr><tr><td>In full screen mode only</td><td>Applies to the virtual desktop only when the desktop is running in the full-screen mode.</td></tr></table></td></tr>
<tr><th colspan="2">Proxy Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Use Proxy Server</td><td>Check this item if a proxy server is used and then specify the details.</td></tr>
<tr><td>Proxy Type</td><td>Click the drop-down menu to select the type of the proxy server according to the used protocol.

Four options are available: SOCKS 4, SOCKS 4A, SOCKS 5, and HTTP 1.1.</td></tr>
<tr><td>Proxy Host</td><td>Specify the IP address of the proxy server.</td></tr>
<tr><td>Proxy Port</td><td>Specify the port used for proxy service.</td></tr>
</table>

Use Proxy Credentials	Check if user authentication is required for a proxy server and then specify the credentials.
Username	Type the user / account name of the proxy server.
Password	Type the password of the user account.
Additional Settings	
Item	**Description**
Compression	Click the drop-menu to enable / disable the compression for the data traffic.

Appendices

This chapter provides instructions on advanced settings, maintenance, and upgrade for your mt182L thin client.

A.1 Resetting Your mt182L to the Factory Default

How to restore factory default settings for your mt182L 249

A.2 Updating Firmware for Your mt182L

Four ways to update firmware for your mt182L 250

A.3 Using SECUREMATRIX Authentication for VMware Connections

Enabling SECUREMATRIX authentication 252
Using SECUREMATRIX authentication 254
Changing Your Password Pattern 257

A.4 Auto Setup Flowchart

Sequence of actions in Auto Setup mode 259

A.1 Resetting Your mt182L to the Factory Default

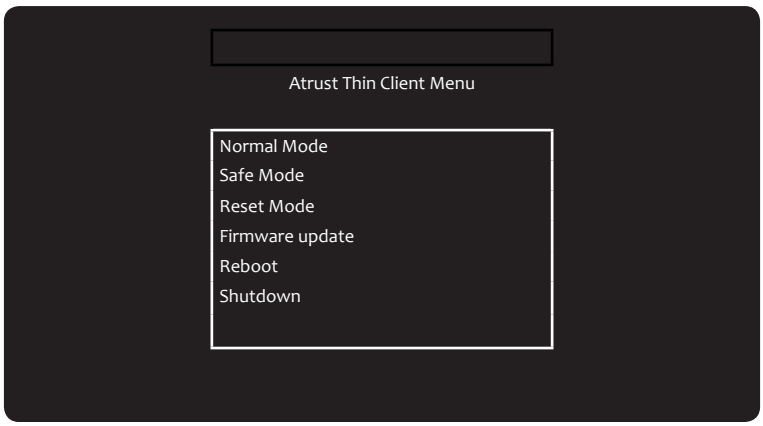
To reset your mt182L to the factory default, please do the following:

WARNING

- Resetting your mt182L to the factory default will erase all current settings in Atrust Client Setup and restore all settings to defaults.

1. Restart your mt182L.

1. During the POST (Power-on Self-Test) period, press **Esc** on the keyboard to enter Atrust Thin Client Menu.



NOTE

- You might need to wait about 15 seconds for this menu to appear on the screen.
- Six options are available on Atrust Thin Client Menu: **Normal Mode**, **Safe Mode**, **Reset Mode**, **Firmware update**, **Reboot**, and **Shutdown**. See the table below for the description of each option:

Menu Option	Description
Normal Mode	Boots up your mt182L as the normal startup procedure.
Safe Mode	Clears and resets the current screen resolution setting.
Reset Mode	Resets your mt182L to the factory default.
Firmware update	Updates firmware for your mt182L through the network.
Reboot	Reboots your mt182L.
Shutdown	Shuts down your mt182L.

2. Use arrow keys on the keyboard to select **Reset Mode**, and then press **Enter** on the keyboard to continue.
3. A message appears prompting for confirmation. Click **y** on the keyboard to confirm.
4. After completion, press **Enter** on the keyboard to restart your system.

A.2 Updating Firmware for Your mt182L

Four ways are available to update firmware for your mt182L:

Method	Description
Atrust Thin Client Menu	Downloads firmware from a remote computer and updates firmware for your thin client.
USB Flash Drive	Updates firmware with a USB flash drive created by Recovery USB Disk Creator.
Atrust Client Setup	Initiates firmware update locally on the thin client with the help of Atrust Client Setup.
Atrust Device Manger	Initiates firmware update remotely on the remote computer with Atrust Device Manager.

Using Atrust Thin Client Menu

To update firmware using Atrust Thin Client Menu, please do the following:

1. Connect your thin client to the network, and then restart it.
2. During the POST (Power-On Self-Test) period, press **Esc** on the keyboard to enter Atrust Thin Client Menu.
3. Select **Firmware update** and then follow the on-screen instructions to complete the task.

NOTE

- You need to specify the IP address of the firmware server over the network. A firmware server is the server where Atrust Device Manager is installed and client firmware files are imported through Atrust Device Manager.
- For more information about Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

Using a USB Flash Drive

To update firmware using a USB flash drive created by Recovery USB Disk Creator, please do the following:

NOTE

- For instructions on how to create a USB flash drive using Recovery USB Disk Creator, please refer to the Quick Guide for USB Creator.

1. Plug the USB flash drive, and then restart your thin client.
2. During the POST period, press **F7** to enter the Boot Device menu.
3. Select the USB flash drive on that menu to enter Atrust Thin Client Recovery System screen.
4. Follow the on-screen instructions to complete the task.

Using Atrust Client Setup

To update firmware using Atrust Client Setup, please refer to section "3.2.7 Updating Firmware from the Management Computer" on page 56.

Using Atrust Device Manager

To update firmware using Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

A.3 Using SECUREMATRIX Authentication for VMware Connections

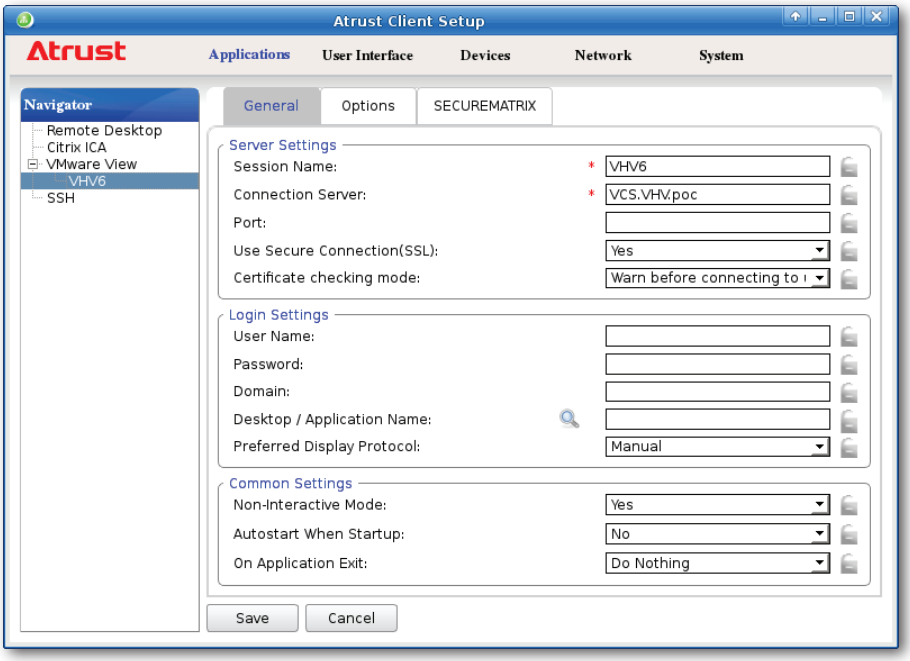
Enabling SECUREMATRIX Authentication for Custom VMware Connections

To enable SECUREMATRIX authentication for a custom VMware connection, please do the following:

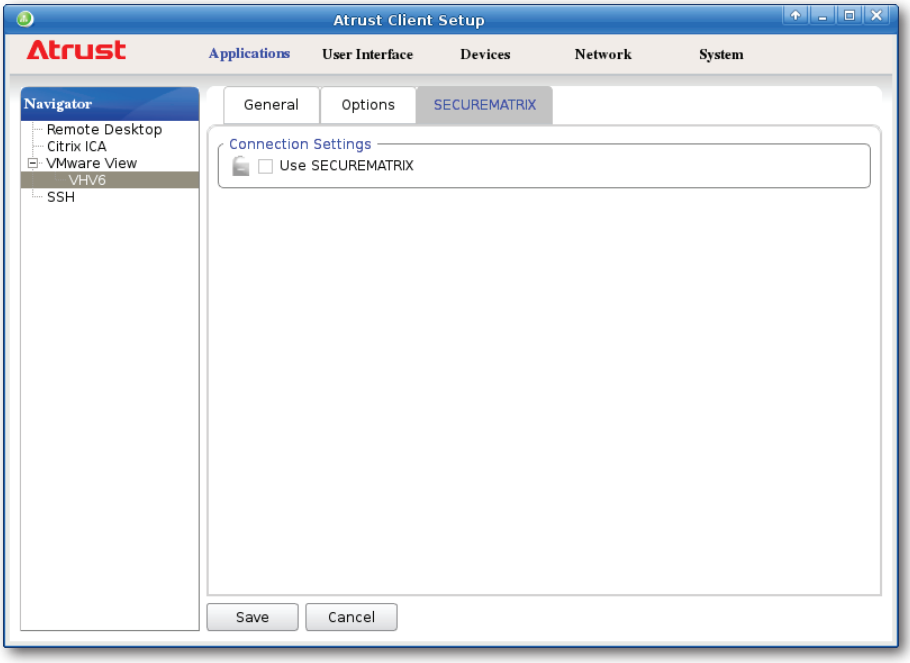
NOTE

- SECUREMATRIX authentication is not available in Quick Connection mode.

1. On the local desktop, click **START** > **Settings** > **Atrust Client Setup** to launch Atrust Client Setup.
2. Click **Applications** > **VMware > Add** to create a new entry of connection settings.
3. On the General tab, type the desired session name and the server address of View Connection Server.



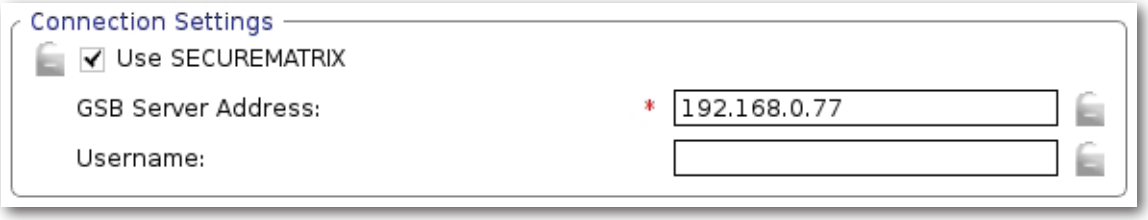
4. On the SECUREMATRIX tab, click to check **Use SECUREMATRIX**.



NOTE

- By default, SECUREMATRIX authentication is disabled.

5. Two fields appear for you to provide SECUREMATRIX related information. Type the server address of GSB server (the server for SECUREMATRIX authentication service).



6. Configure other connection settings if needed, and then click **Save** to confirm.
7. The access shortcuts will be created on the local desktop and START menu.

Using SECUREMATRIX Authentication in VMware Connections

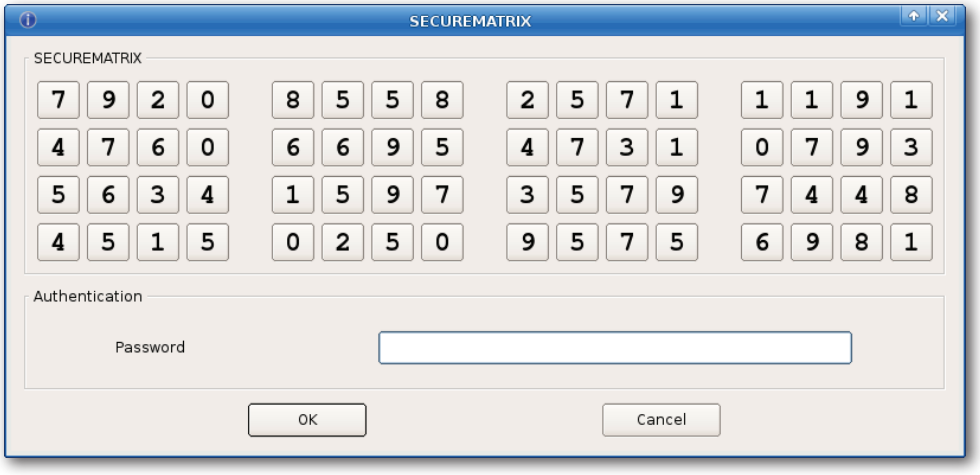
When SECUREMATRIX is enabled in your VMware connection, follow the steps and instructions below to use SECUREMATRIX authentication:

1. Click the shortcut on the local desktop or START menu.
2. A window appears to prompt for the Login ID of SECUREMATRIX authentication.

3. Type your Login ID, and then click **OK** to confirm.

> **NOTE**
>
> - To change your password pattern, click **Change Password**. For details, please see "Changing Your Password Pattern for SECUREMATRIX Authentication" on page 257.

4. The SECUREMATRIX window appears prompting for the password.

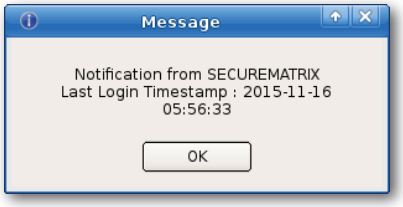


5. Type numbers under your ***password pattern*** using the keyboard or click numbers directly on the window, and then click **OK** to confirm.

TIP

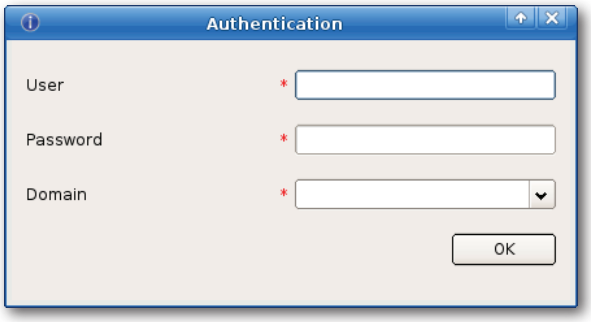
- For example, if your ***password pattern*** is shown as below, type or click numbers, **0**, **0**, **4**, **5**, **1**, **3**, **6**, **2**, in sequence.

6. A message appears when SECUREMATRIX authentication is completed. Click **OK** to continue.

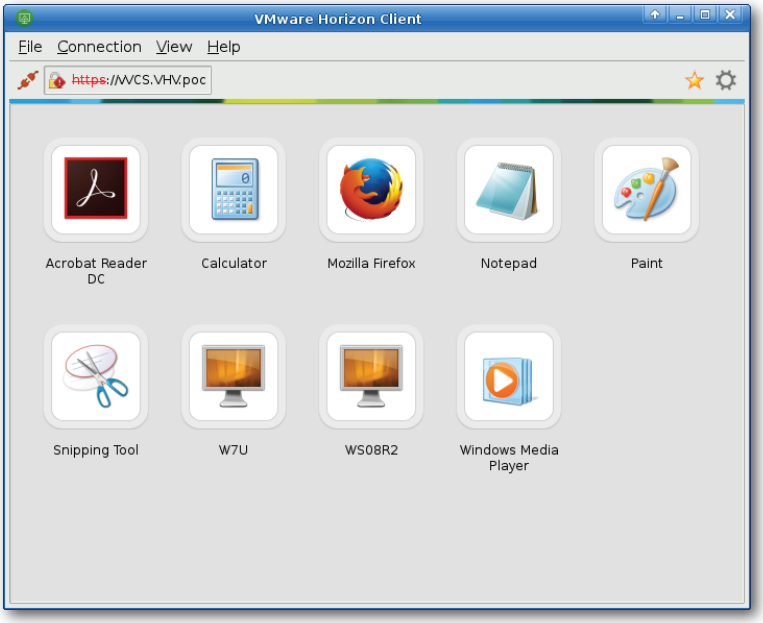


7. A message appears prompting to provide credentials for access to VMware virtual desktops and applications. Click **OK** to continue.

8. Type your credentials on the opened window, and then click **OK** to continue.



9. The Desktop and Application list appears. Double-click to select the desired desktop or application.

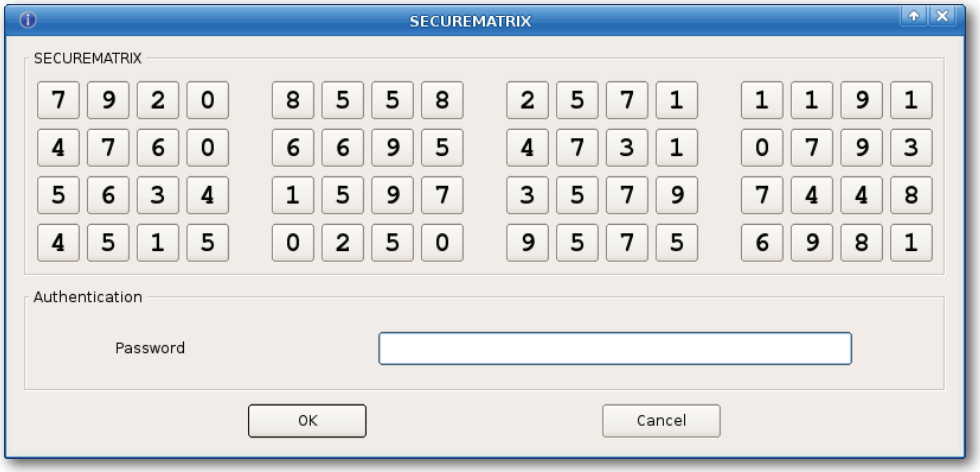

VMware Horizon Client
File Connection View Help
https://WCS.VHV.poc
Acrobat Reader DC
Calculator
Mozilla Firefox
Notepad
Paint
Snipping Tool
W7U
WS08R2
Windows Media Player

Changing Your Password Pattern for SECUREMATRIX Authentication

To change your password pattern for SECUREMATRIX authentication, please do the following:

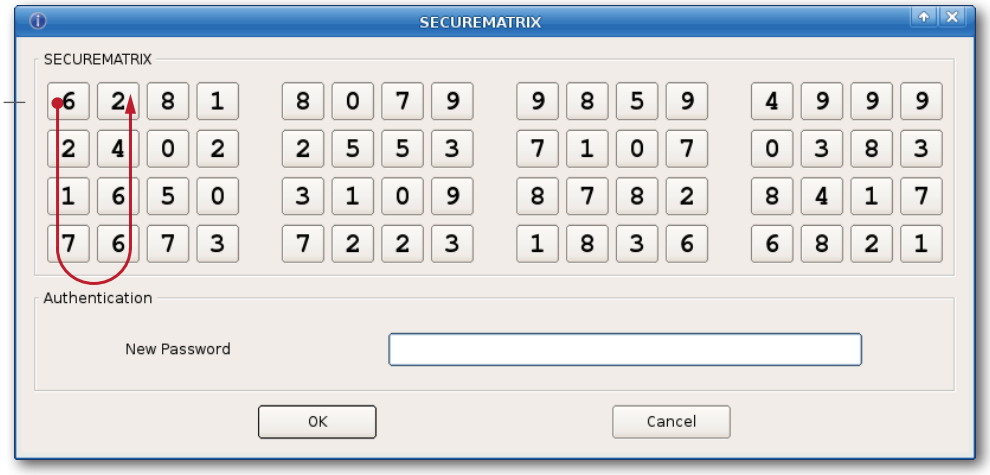
1. On the window prompting for the Login ID as shown, type your Login ID, and then click **Change Password**.

2. Type or click numbers under your ***old password pattern***, and then click **OK** to continue.

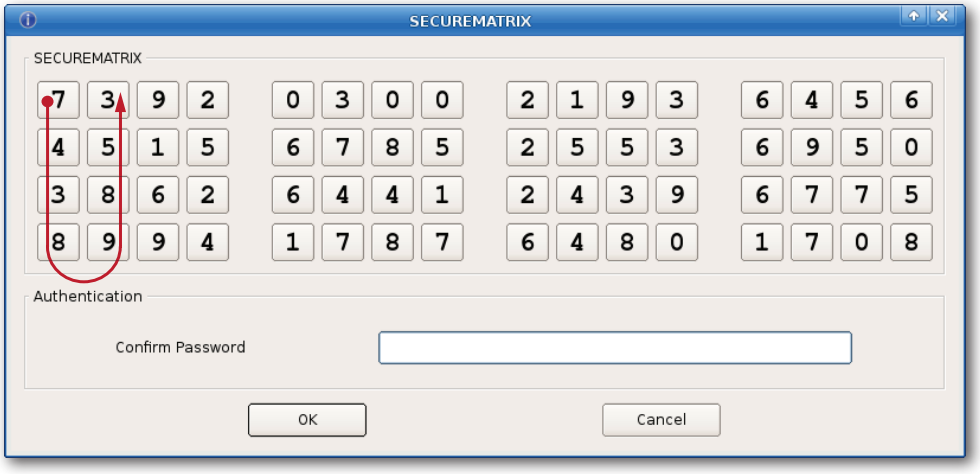


3. Type or click numbers under your ***new password pattern***, and then click **OK** to continue.

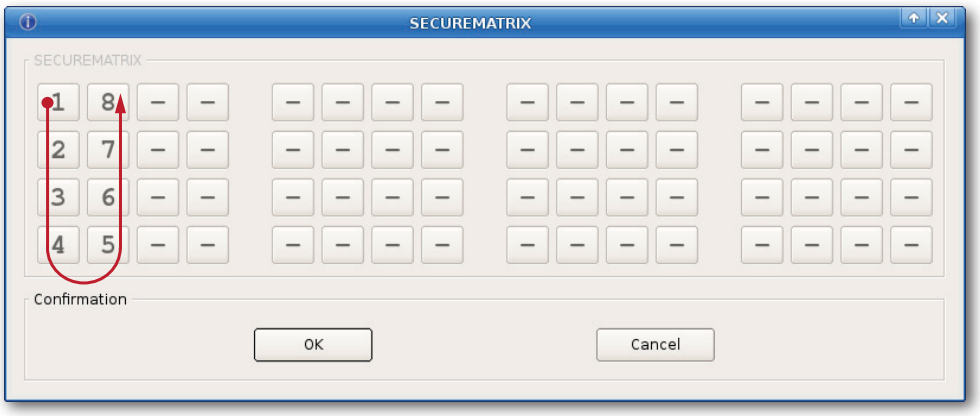
Your new password pattern, for example



4. Type or click numbers under your ***new password pattern*** again, and then click **OK** to continue.



5. A window appears showing your ***new password pattern*** in numerical order and prompting for confirmation. Click **OK** to confirm.



A.4 Auto Setup Flowchart

Please see ***next page*** for sequence of actions in Auto Setup mode.

For details, please refer to User's Guide for Auto Setup.

FLOWCHART

START

Power on / Restart thin client

Auto Setup enabled
- No → Factory default configurations
- Yes

Network connected
- No → Ever got and kept ***Global*** and ***MAC*** configurations
  - Yes → Apply previous configurations → Ready for use
  - No → Factory default configurations
- Yes

Auto Setup environment ready
- No → Ever got and kept ***Global*** and ***MAC*** configurations
- Yes

Get preset configurations & Apply basic ***Global*** and ***MAC **** configurations

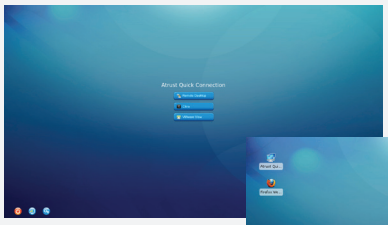
* **MAC** configuration will be applied *if any* but not a necessary element in Auto Setup; **Global** one is required.

User authentication enabled
- No → Apply complete ***Global*** and ***MAC **** configurations → Ready for use
- Yes

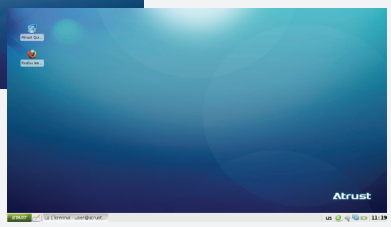
User authentication passed
- Yes → Apply complete ***Global***, ***MAC ****, and ***User*** configurations → Ready for use
- No → Deny access

SCREENS

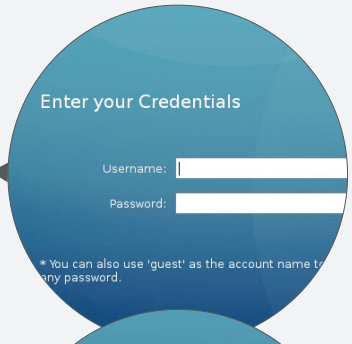
Unportable thin clients start with Quick Connection screen



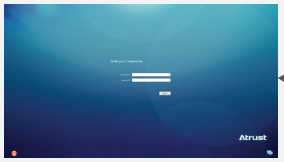
Portable thin clients start with Local Desktop

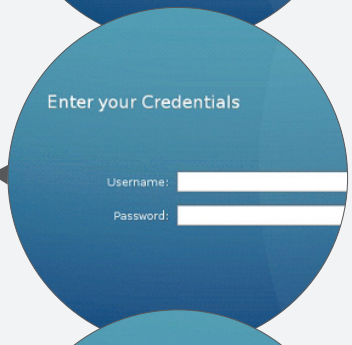


Logon screen with guest-enabled user authentication

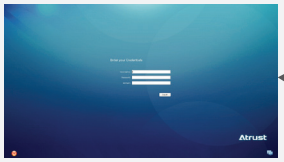


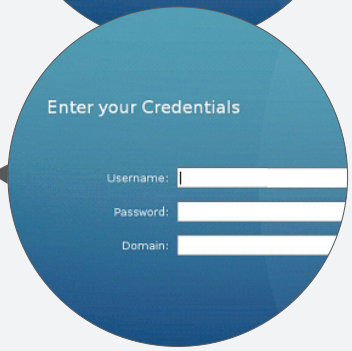
Logon screen with guest-disabled user authentication





Logon screen with Active Directory authentication





When Auto Setup is enabled, user environment might vary with preset configurations.

AUTO SETUP REQUIREMENTS

- Auto Setup enabled endpoint devices
- Auto Setup environment and mechanism
- Network connectivity
- Target virtualization services for use

Specifications

Atrust mt182L mobile thin client

Processor	Intel® Atom® x5-E8000, Quad-core, 1.04 GHz, up to 2.0 GHz		
System Memory	2 GB		
Flash Memory	4 GB		
Display	Type: 14", FHD 1920 x 1080		
Keyboard / Touchpad	Keyboard: full layout including the numeric keypad Touchpad: 2-button Glide pad		
Sound	Built-in speakers		
I/O interfaces	Left side: 1 x DC IN 1 x HDMI 1 x USB-C (USB 3.1 Gen 1) 1 x Audio combo jack	Right side: 2 x USB-A (USB 3.1 Gen 1) 1 x USB-C (USB 3.1 Gen 1)	Display and base: 2 x Built-in microphone 1 x Webcam 2 x Built-in speaker 1 x Fingerprint sensor
Networking	USB-to-LAN adapter: USB-A (USB 3.1), 10/100/1000 Mb Ethernet Wi-Fi 802.11 ac/a/b/g/n (M.2 interface) Bluetooth 4.2		
AC Adapter	INPUT: 100-240 V, 50-60 Hz OUTPUT: 19 V, 3.42 A, 65 W		
Battery	Built-in Rechargeable battery 3290 mAh		
Operating system	Atrust Linux		
Supported Protocols	Microsoft RDP with RemoteFX / Citrix ICA with HDX / VMware PCoIP		
Management	Atrust Client Setup / Atrust Device Manager		
Security	Kensington security slot		
Dimensions	(W)322 x (D)222 x (H)15.95 mm		
Weight	1.20 kg (approx.)		
Environment	Operating Temperature: 0° C ~ 35° C Non-operating Temperature: -20° C ~ 60° C Operating Humidity (Rh): 10% ~ 90% (non-condensing) Non-operating Humidity (Rh): 5% ~ 95%		

UM-mt182L-ENJP-20031910

Atrust