

Mobile Thin Client Solution Atrust mt182L

Topics Covered:

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



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.

ΝΟΤΕ

• A note provides important information for a specific situation.



• 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

WARNINGUse 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.

vi

Table of Contents

Copyright and Trademark Statements

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

1 Overview 1

- Introduction 3 1.1
- 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

Configuring Client Settings 3 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**

- 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
- Configuring the Access Privileges and Passwords of Atrust Client Setup 3.2.4

45

47

77

78

64

48

3.2.5 Configuring the Login Password for the Local Desktop 52

i

- 3.2.6 Configuring Shadow Settings for Remote Assistance 54 56
- 3.2.7 Updating Firmware from the Management Computer 58
- Enabling or Disabling the Appliance Mode 3.2.8 3.2.9 Enabling or Disabling Auto Setup 62
- 3.2.10 Configuring the Quick Connection Mode
- 62 Configuring Advanced Quick Connection Settings 3.2.11
- 3.2.12 Managing the Use of Power
- 68 Enabling or Disabling the Command-line Functions 3.2.13
- 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
- Enabling or Disabling Auto Registration 3.2.17
- 3.2.18 Viewing System and Network Information

3.3 Configuring User Interface Settings 79

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

3.4	3.3.3 3.3.4 3.3.5 3.3.6 3.3.7 3.3.8 3.3.9 Config 3.4.1 3.4.2	Configuring Display Settings80Customizing Desktop and System Language SettingsHiding or Showing Quick Access Shortcuts86Using a Custom Wallpaper87Adjusting Keyboard Settings88Adjusting Mouse Settings90Configuring Screensaver Settings91uring External Device Settings93Devices Tab Overview93Available Settings at a Glance94	83	
	3.4.3 3.4.4 3.4.5 3.4.6 3.4.7 3.4.8 3.4.9	Configuring Settings for USB Storage Devices94Manually Mount and Eject Attached USB Storage Devices96Disabling or Enabling Attached Audio Devices96Using Audio Devices97Muting or Unmuting the Sound98Adding a Local Printer99Adding a Network Printer102	5	95
3.5	Config	uring Network Settings 103		
	3.5.1 3.5.2 3.5.3 3.5.4 3.5.5 3.5.6	Network Tab Overview103Available Settings at a Glance104Configuring Wired Network Settings105Configuring IEEE 802.1X Authentication108Establishing and Stopping a VPN connection109Configuring Virtual Private Network Settings113		
	3.5.7 3.5.8 3.5.9 3.5.10 3.5.11 3.5.12 3.5.13	Creating the Mapping of IP Addresses to Names of Hosts Configuring the Failover Cluster List 116 Changing the Host Name of Your Thin Client 118 Enabling or Disabling the Wireless Interface 119 Configuring the Trigger Threshold for Roaming Establishing and Stopping a Wireless Connection Configuring Wireless Connection Settings 124	120 121	114
2.4	3.5.14	Configuring Proxy Settings for Web-based Access to Serv	ices	125
3.6	3.6.1 3.6.2 3.6.3 3.6.4 3.6.5 3.6.6 3.6.7	uring Service Access Settings127Applications Tab Overview127Available Settings at a Glance128Configuring Basic RDP Connection Settings129Accessing Remote Desktop Services138Configuring Advanced RDP Connection Settings159Switching the Citrix Receiver Version172	144	
	3.6.8	Enabling or Disabling Esc to Quit on the Web Logon Scre		173
	3.6.9 3.6.10	Configuring Keyboard Layout and Type for Citrix ICA Sess Accessing Citrix Services 175	sions	174
	3.6.11	Configuring Advanced ICA Connection Settings	182	
	3.6.12 3.6.13 3.6.14	Configuring Basic VMware View Connection Settings Accessing VMware View or Horizon View Services Configuring Advanced View Connection Settings	212 214 216	
	3.6.15	Configuring SSH Connection Settings 221		
	3.6.16 3.6.17 3.6.18	Launching SSH and Telnet Sessions223Configuring Basic Settings for Browser Sessions226	224	
	3.6.19	Configuring Advanced Settings for Browser Sessions	227	
	3.6.20	Configuring Basic RAS / RDP Connection Settings Accessing Remote Desktops or Applications 233	228	
	3.6.21 3.6.22	Configuring Advanced RAS / RDP Connection Settings	235	
Appendices	5	247		

A.1 Resetting Your mt182L to the Factory Default 249A.2 Updating Firmware for Your mt182L 250

- A.3 Using SECUREMATRIX Authentication for VMware Connections 252
- A.4 Auto Setup Flowchart 259

Specifications 261

×

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

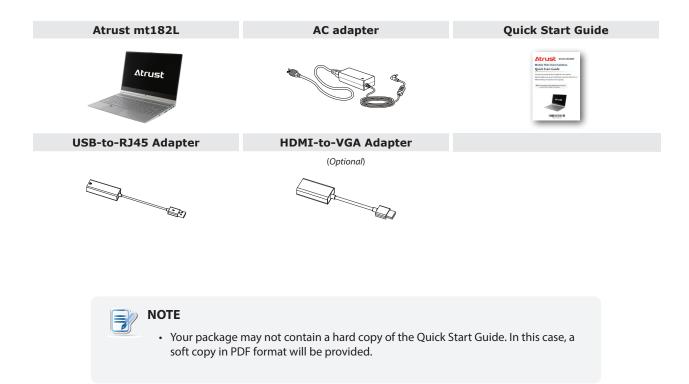
1.2 Features

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

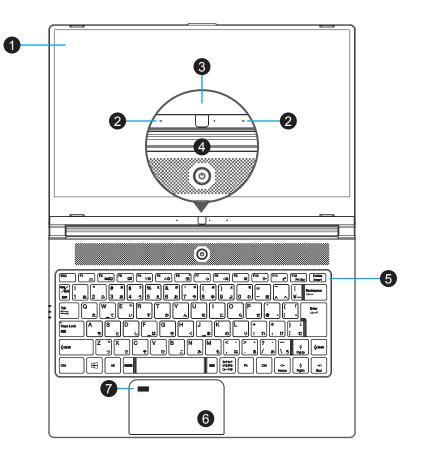
1.3 Package Contents

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.



1.4 Exterior Components

Display and Base Components



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

Fn Key Combinations

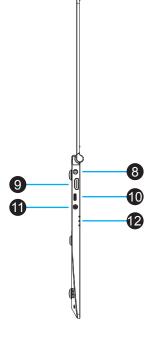
With the combination of **Fn** plus another specific key (most with one printed symbol on it), you can quickly adjust hardware settings to suit your needs.

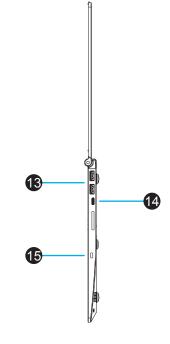
$ \begin{array}{c} \text{ESC} & \fbox{P1} \\ \\$
$\begin{bmatrix} Tab \\ \overset{W}{\overset{H}{{H}}}{\overset{H}{{}}}{\overset{H}}{\overset{H}{\\{H}}{{}}}}{}}{}}{}}}}}}}}$
$ \begin{bmatrix} C_{\text{appe Lock}} \\ \texttt{S} \\ \texttt{5} \\ \texttt{E} \\ \texttt{Cape Lock} \\ \texttt{5} \\ \texttt{E} \\ \texttt{Cape Lock} \\ \texttt{5} \\ \texttt{5} \\ \texttt{Cape Lock} \\ \texttt{5} \\ \texttt{5} \\ \texttt{6} \\ \texttt{6}$
$ \begin{array}{c} \begin{array}{c} \begin{array}{c} \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \end{array} \\ \end{array} \\ \end{array} \\ \begin{array}{c} \\ \\ \\ \end{array} \\ $
Ctri Image: State in the s

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

Combination	Description	Combination	Description
Fn + (F1 <u>**</u>)	Fn + F1 Use to switch the brightness of the keyboard backlight.	Fn + F∂ t t	Fn + F9 Use to mute / unmute the sound.
	Fn + F2 Use to switch the use of displays.	Fn + (^{F1∅} →	Fn + F10 Use to enable / disable the Airplane mode.
Fn + F3	Fn + F3 Use to enable / disable the touchpad.	Fn + Fig z [*]	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 + A FgUp	Use to work as PgUp key.
Fn + F6 o	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 ⊂(<i>i</i>)	Fn + F8 Use to increase the volume of the built-in speakers.	Fn + ⊨⊳ End	Use to work as End key.

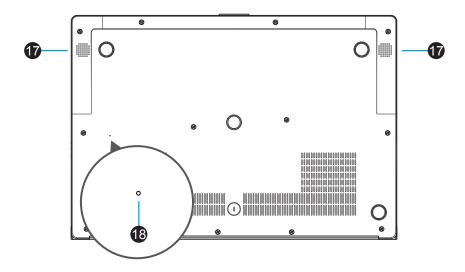
Left and Right Side Components





No.	Sign	Component	Description
8		DC IN	Connects to an AC adapter.
9	нәті	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.
	Ċ	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.
12	[1 +]	Battery LED	Glows orange when the battery is being charged.Glows blue when the battery is fully charged.
	,Ci	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	-88-	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.

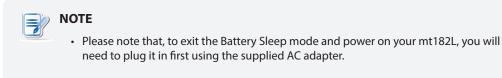
1.5 Before Getting Started

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.



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



 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
		The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session.
1	Appliance	Available actions include:
T	Аррпансе	Re-launching a new session
		Restarting the thin client
		• Turning off the thin client
	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)
2		 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

TIP

on the desktop to enter Atrust Quick Connection screen.



 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
 - (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	 Click to configure audio settings. 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 <i>System Sleep mode</i> manually (Fn + F12 or 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.

3	Atrust Client Setup							
Atrust	Applications	User Interface	Devices	Network	System			
Navigator Ethernet VPN Hosts Host Name Wreless Proxy	IP Type: DNS DNS Type: Wake On LAI Wake On LAI	N	cation	DHCP Dynamic Enabled	DNS (via DHCP			

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

		Atrust Client	Setup			↑ _ □ ×
\trust	Applications	User Interface	Devices	Network	System	
vigator Ethernet VPN Hosts Host Name Wireless Proxy		- Delete Priority int-F9-L 20 GGBR14 20 GGBR14 20 GGBR14 20 GGBR14 20 GGBR14 20 20 a 2.46 20 a 2.46 20 20 a 2.46 20 20 20 20 20 20 20 20 20 20	Scan Signal 000 100 100 100 94 94 94 91 81 80 74 70 68 80 74 72 70 68 64 62 62 55 54 54	 Security Insecure WPA 	Status	Comment -

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

ltrust	Applications	User Interface	Devices	Network	System	
vigator	Connectio	ns Wireless				
Ethernet VPN	+ Add	– Delete	Q. Scan	🖉 Connect		
Hosts	- Add	- Delete	S scan	Connect		
Host Name Wireless	SSIE	Priori	ty Signal	 Security 	Status	Comment 📤
Proxy	HP-P	rint-F9-L 20	100	Insecure		
ноху	✓ IT-AP	02 20	100	WPA		
	- SMC	WGBR14 20	100	WPA		
	roan	ning24 20	100	WPA		
	roan	ning5 20	100	WPA		
	Dem	o-AP01 20	97	WPA 802.1x		
		Portable 20	94	WPA		
		NK_F36B 20	94	WPA		
	MIX2		91	WPA		
		nia_2.4G 20	81	WPA		
		o-AP02 20	81	WPA		
	KiKi-ł		80	WPA		
		t001 20	80	WPA		
		NK_EF01 20	74	WPA		
		erylife_5G 20	72	WPA		
	IT-AF		70	WPA		
		1000N 20	70	WPA		_
		er~HerH 20	68	WPA		
	MIX5		64	WPA		
	IT-AP		62	WPA		
		ON-69B0 20	60	WPA		
		ON-9920 20	55	WPA		
		.091 20	54 54	WPA		-
	III min	home 20	54	WPA		, , Č

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

	🕘 Wi	reless Network Auth	entication Required	•	
		n required by wireless r ired to access the wire	network. Passwords or en less network.	cryption	
	Wireless Secu	irity:	WPA & WPA2 Personal	•	
	Key:	*			
	Show char	acter		_	
			Connect Ca	ancel	
	-			_	
	_			_	
NOTE					
recorded	d for future a	access. In this cas	work before, the p e, you don't need t establishment of a	to provide	
• Consult	your netwo	rk administrator f	for required inform	nation on a	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**.

SSID	Priority	Signal	Security	Status 🔺	Comment
 IT-AP02	20	100	WPA	connected	Connected before
 sophia_2.4G	20	92	WPA		
 roaming5	20	87	WPA		
 roaming24	20	100	WPA		
 guest001	20	87	WPA		
 dlink_DWR-113	20	38	WPA		
 dir-810-5g	20	45	WPA		
 dir-810-2g	20	94	WPA		
 amphenol_S	20	72	WPA		

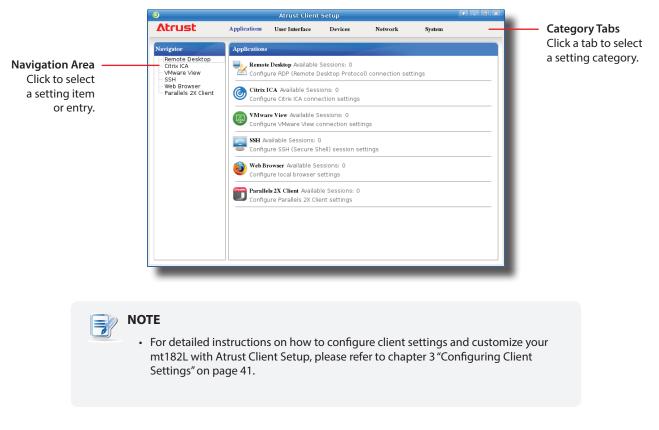
8. Close Atrust Client Setup.

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



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

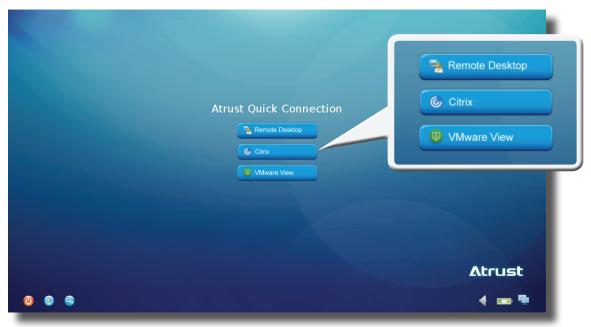
	٥		Atrust Client	Setup				
	Δtrust	Applications U	User Interface	Devices	Network	System		
Time Zone	Savigator Time Zone Password Primware Update Auto Satup Oulck Connection Power Management Save Power Management or Management Power Management Po	General Time Zone Time Zone: NTP NTP Server Ac	ddress		(GMT) Co	ordinated Unive		Time Zone drop-down menu

System

- 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**.

Remote Destkop Connection
Session name: <quick connection=""></quick>
Computer:
User name:
Password:
Domain:
Connect
To return to the previous screen, press Esc . Use Alt + Tab to select and restore a hidden or minimized application or desktop session.
 NOTE To discover available Windows MultiPoint Server systems over your network, please do the following:
1. Click 👯 on the left of the Computer field.
 Click was solutile left of the computer field. Upon completion, a window appears with the search result.
Confirm Dialog Windows MultiPoint Servers' list, please select one that you want to connect: EE-SV1 (192.168.11.108) OK
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 Citrix 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



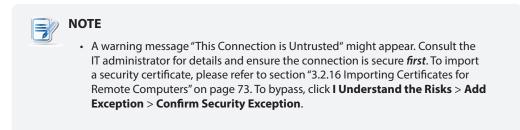
• For newer versions of XenDesktop and XenApp, you may need to further specify the sub-path of the server. Refer to the following table for details:

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
		IP / URL / FQDN plus sub-path
Virtual Apps and Desktops (XenApp and XenDesktop 7.5 or later)	StoreFront	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.



The following are some examples of Citrix Logon screens.

XenDesktop 5.6 Platinum:



Citrix Logon Screen



• To return to Atrust Quick Connection screen, press Esc.

XenApp 6.0 Fundamentals:



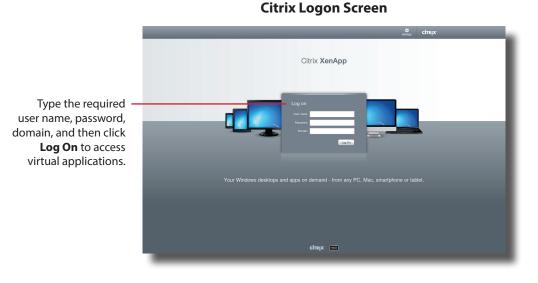
Citrix Logon Screen

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

NOTE

3

- 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:



• To return to Atrust Quick Connection screen, press Esc.

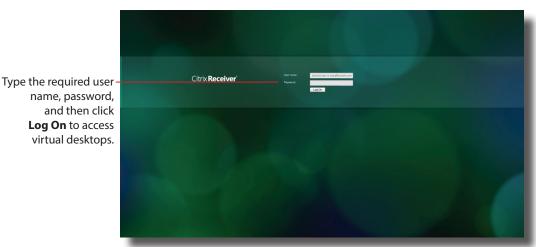
• If your XenApp server doesn't belong to any domain, type the computer name of the server in the Domain field.

Getting Started 24 Learning the Basics

VDI-in-a-Box:



XenApp and XenDesktop 7.5 Platinum:



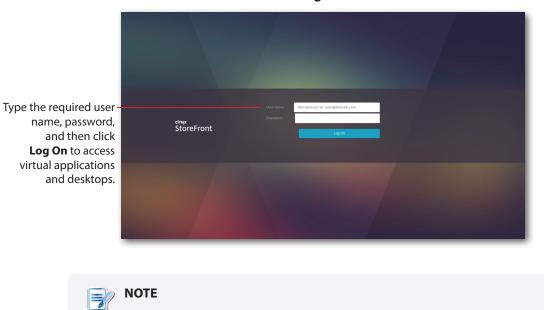




• To return to Atrust Quick Connection screen, press Esc.

Citrix Logon Screen

Virtual Apps and Desktops 7 1808.2:

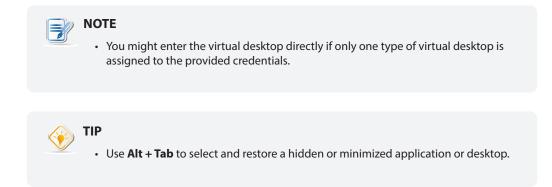


• To return to the Quick Connection screen, press **Esc**.

Citrix Logon Screen

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).



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.

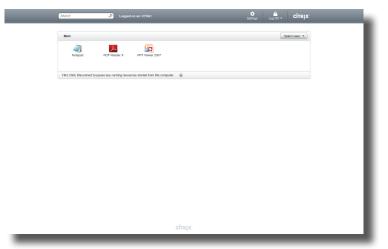


Virtual Desktop Example: Windows 7 Ultimate

XenApp 6.5 Platinum:

1. The Application Selection screen appears after logon.

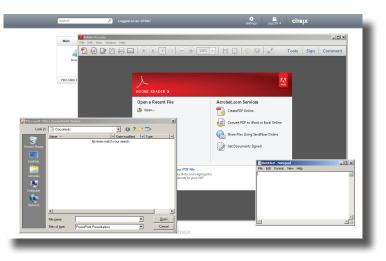
Application Selection Screen



- 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



ΝΟΤΕ

- 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





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

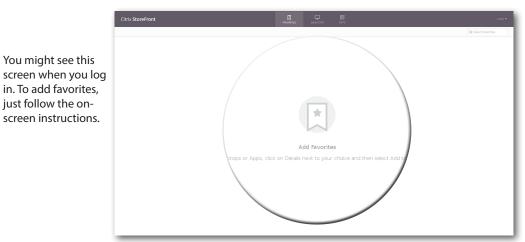


NOTE

- 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.

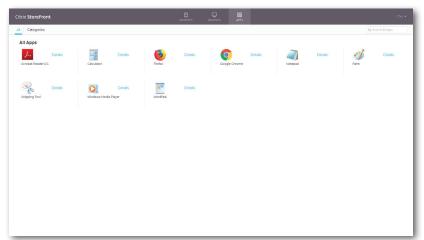


Favorites Screen

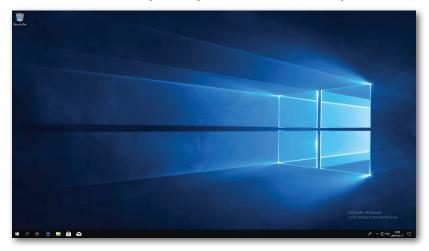
Desktop Selection Screen

Citrix StoreFront	R R BB	ctiau 🗸
		Q Search Desktops
Details Details Details Windows Server 2012 R2		

Application Selection Screen



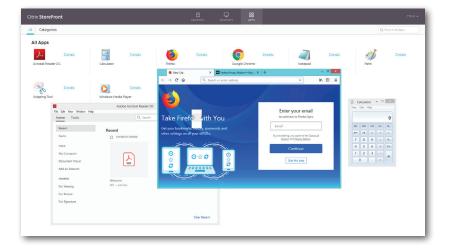
- 2. Click to select the desired application or desktop.
- 3. The selected application or desktop will be displayed on the screen.



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 VMware View 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**.

		🐵 VMware Horizon Client	↑ - □ ×
_ile	<u>C</u> onnecι	Eile Connection View Help	
+ N	ew Server	+ New Server	
		Add Server	Add Server Add Server Minimum Add Server Immum Add Server Immum Add Server
			Connect



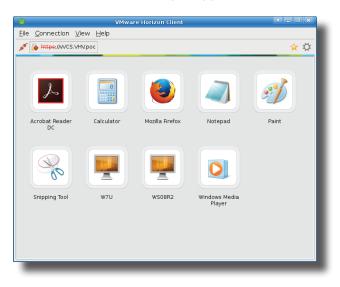
- 4. A Welcome window might appear, click **OK** to continue.
- 5. A window appears prompting for the credentials. Enter your user name, password, click the Domain drop-down menu to select the domain, and then click **OK**.

@	Server Login	×
vmware	e Horizon	
<u>S</u> erver: <u>U</u> sername:	https://wcs.vhwpoc	
<u>P</u> assword: <u>D</u> omain:	VHV	
	<u>C</u> ancel <u>O</u> K	

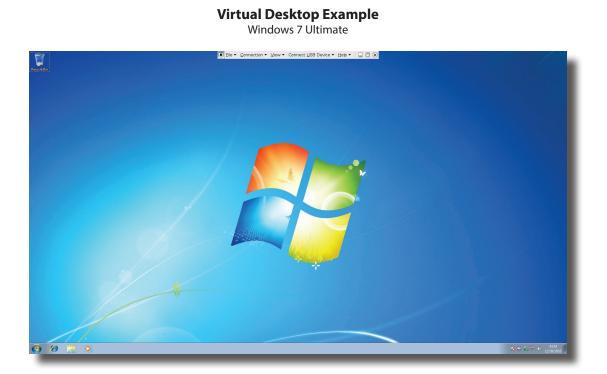


• A window might appear with a certificate message about the remote server. Consult the IT administrator for details and ensure the connection is secure *first*. To import a security certificate, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73. To bypass, click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

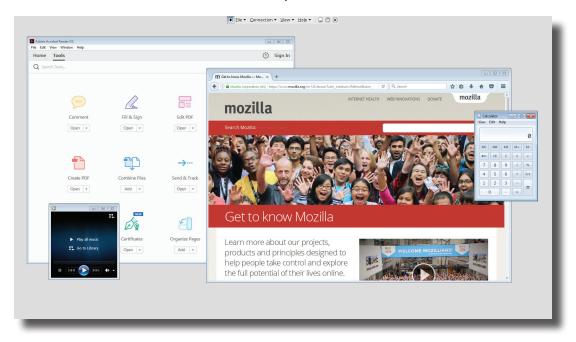


7. The virtual desktop or application will be displayed on the screen.



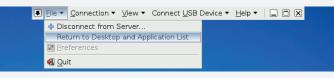
Virtual Application Examples (VMware Horizon 6 with View)

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

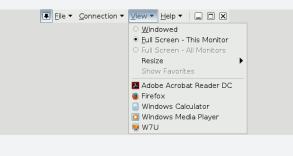




- Your desktop or application will be displayed in full screen. You can:
 - Click File > Return to Desktop and Application List on the top tool bar to recall the Desktop and Application list.



♦ Click View on the top tool bar to switch to a virtual desktop or application.

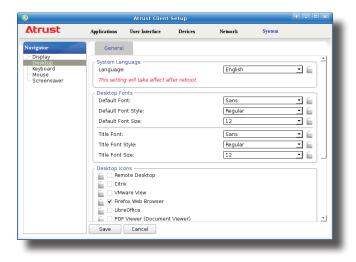


Topic 5: Using Built-in Applications

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



- 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.

<u>)</u>		Atrust Client S	ietup			+ _ E ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Display Display Display Keyboard Keyboard Screensaver Screensaver	Desktop For Default For Default For Title Font: Title Font S Title Font S Desktop Ico Exemption For Citrix Wither Wither	will take effect aft will take effect aft ts ts ts ts ts ts ts ts ts t		 Firefor LibreO 	re View x Web Bro Office fiewer (Dr Cancel	

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 I** icon in the bottom-right corner to launch Power Management. Here you can view the use and settings of power.

nformation			
Current power source :	AC power		
Charge status :	Not charging		
Remaining battery power :	98%		
Dimmed LCD: Never Turn off LCD: Never © Suspend ○ Shut down Never	Dimmed LCD: Turn off LCD: O Suspend O Sh	5 minutes later 10 minutes later nut down 1 hour later	
	You c	an click Adjust button to chang	je settings.

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.



 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.



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

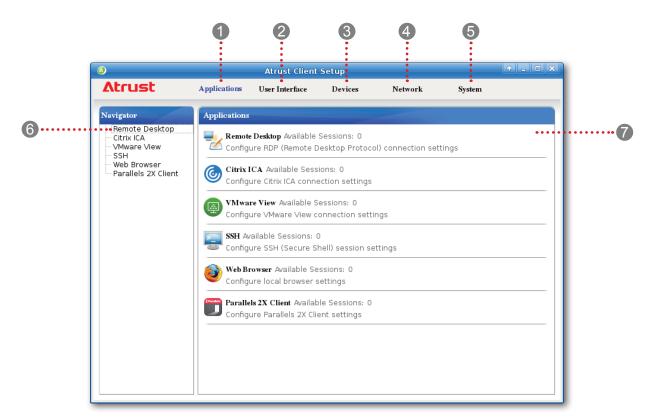
3.1 Atrust Client Setup

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

Interf	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

	٨		Atrust Client	Setup			X	
	Atrust	Applications	User Interface	Devices	Network	System		
0	Navigator Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager	Passwor Configu	e time zone and tir rd ure administration re Update	privileges and r	emote assistanc	e settings		2
	Advanced	Applian Configu	e firmware through .ce Mode ure Appliance mod :tup ure Auto Setup Mo	e				
		Configu	Connection ure Quick Connect Management ure the Power Mar					
		Configu	al ure the access of	command-line ir	terface			

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
	Time Zone	7.	Click to configure the time zone and time server for your mt182L.	3.2.3	47
			Click to configure the access privileges of Atrust Client Setup for mt182L users.	3.2.4	48
	Password	<u> </u>	Click to set the login password for the local desktop.	3.2.5	52
			Click to configure settings for remote assistance.	3.2.6	54
	Firmware Update	(1)	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	3	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	uto Setup Line Click to enable Auto Setup to allow the client to get its preset configurations on startup and enter the desired user environment automatically.			62
System	Quick Connection Click to configure the Quick Connection mode.		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
			Click to collect error log and launch the screen capturing program for error reporting.	3.2.14	70
	Error Report		Click to upload files to a specified FTP server for error reporting.	3.2.15	72
			Click to import or manage certificates for remote computers.	3.2.16	73
	Advanced	Ж	Click to configure advanced settings such as Auto Registration.	3.2.17	77
	System Information	0	Click to view detailed system and network information.	3.2.18	78



• 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**.

		Atrust Client	Setup			- 0
Δtrust	Applications	User Interface	Devices	Network	System	
lavigator	General					
Time Zone Password	Time Zone -					
Firmware Update Appliance Mode	Time Zone:			(GMT) C	oordinated Univer	sa 💌 💼
Auto Setup Quick Connection	NTP					
Power Management	NTP Server	Address		* pool.nt;	o.org	Ê
Terminal Error Report Certificate Manager Advanced System Information	Save	Cancel				

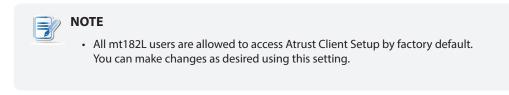
- 2. Under the Time Zone section, click the drop-down menu to select the desired time zone.
- 3. Under the NTP (Network Time Protocol) section, use the default or type in the desired time server.

- 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.



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**.

٥		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Local Deskt	ve Admin Authoriza op ble Password Auth g will take effect a ble Shadow npt For User Perm v User To Disconn	ientication for L fter reboot. ission			

- 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.

•	Set Password	↑ ×
Password Confirm Password	*	
* Your password car special characters * It must be 4 to 20	i contain letters, numbers, characters long.	and
ОК Са	incel	

- 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.

Atrust 🛛		Atrust Client	Setup			
	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Change Pass User	e Admin Authoriza sword e User Authorizati assword Required	on entication for Lo	ical Desktop		

• 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.

٨	Set Password	↑ ×
Password		*
Confirm Password		*
special characte * It must be 4 to 2	0 characters long.	bers, and
ОК	Cancel	

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.

٨		Atrust Clien	t Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terror Report Certificate Manager Advanced System Information	Change Pas User Privile * This settil User © I Acth © No F Change Pas Local Deskt	ve Admin Authoriz ssword ige Level: ng will take effect ve User Authoriza rassword Require ssword op op ole Password Aut g will take effect a	tion d			



• 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:



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

		Atrust Client	Setup			
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Local Deskt	op	nentication for L fter reboot.			

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

Set Passi	word 🔶 🔨 🗙
Password	*
Confirm Password	*
* Your password can contain lett special characters. * It must be 4 to 20 characters I	ers, numbers, and ong.

- 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**.

٩		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Auto Setup Quick Connection Power Management Terror Report Certificate Manager Advanced System Information	Local Deskt	ve Admin Authoriz op ble Password Auth g will take effect a ble Shadow npt For User Perm v User To Disconn	nentication for L Ifter reboot.			

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.

(1)	Set Password	↑ X
Password Confirm Password		*
* Your password car special characters * It must be 4 to 8 d	n contain letters, number 5. :haracters long.	s, and
ОК Са	ancel	

ΝΟΤΕ

- 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.

ΝΟΤΕ

• 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**.

٥		Atrust Client	Setup		+ - O X
Atrust	Applications	User Interface	Devices	Network	System
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information					Check Firmware

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

٨	Confirm Dialog 🔤	×
	List Loading Comple	ted!
	<u>Y</u> es	

4. Click **Yes** to continue.

٥		Atrust Client	Setup			
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Firmware \ Language: Reboot Imr	pdate pdate irsion: Ver. 5.40-IN i mediately: g will take effect a		ATRUST English NO	LINUX 5.40-INTL	T C

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.

ΝΟΤΕ

 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
		The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session.
	Annelianaa	Available actions include:
1	Appliance	 Re-launching a new session Restarting the thin client Turning off the thin client
		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)
2	Autostart	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:



- 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



- 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
 - \diamond "3.6.14 Configuring Advanced View Connection Settings" on page 216
 - \diamond "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**.

٩		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	General	igs ole Appliance Mod Cancel	e			

- 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.

Basic Settings		
Application Type:	Citrix ICA	_
Use Session:	XD	- 6
On Application Exit:	Shutdown	_ 6
* To launch Console: Shift+Ctrl+Delete		
* To minimize ICA Fullscreen Desktop: Pres	s Left Ctrl+F2 then Alt+F9	
* To minimize ICA Fullscreen Desktop: Pres	s Left Ctrl+F2 then Alt+F9]
* To minimize ICA Fullscreen Desktop: Pres	s Left Ctrl+F2 then Alt+F9	
* To minimize ICA Fullscreen Desktop: Press Basic Settings	s Left Ctrl+F2 then Alt+F9	
Basic Settings	<i>s Left Ctrl+F2 then Alt+F9</i> Remote Desktop	
Basic Settings		

* To launch Console: Shift+Ctrl+Delete

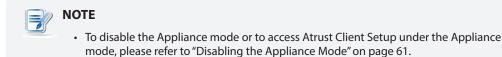
* To toggle RDP fullscreen: Ctrl+Alt+Enter

Basic Settings		
Application Type:	VMware View	- 6
Use Session:	VHV	- 6
On Application Exit:	Shutdown	- 6
* To launch Console: Shift+Ctrl+Delete		
* To release keyboard and mouse from the v	irtual desktop, press Ctrl+Alt	

盲 🗹 Enable Appliance Mode		
Application Type:	Web Browser	_ _ _
Use Session:	Gmail	6
On Application Exit:	Shutdown	- 6
* To launch Console: Shift+Ctrl+Delete		
* To restart system : Shift+Ctrl+End		

Basic Settings — ✔ Enable Appliance Mode		
Application Type:	Parallels 2X Client	-
Use Session:	P2X-RAS-G	-
On Application Exit:	Shutdown	-
* To launch Console: Shift+Ctrl+Delete		
* To restart system : Shift+Ctrl+End		

- 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.



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.

- 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.



• 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
		The client will start up directly with the desired RDP / ICA / View / Web / 2X session and perform the configured action after exiting the session.
1	Appliques	Available actions include:
1	Appliance	Re-launching a new session
		 Restarting the thin client
		Turning off the thin client
		-
		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)
2	Autostart	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.

ΝΟΤΕ

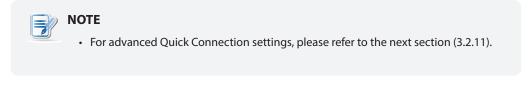
- To use the Quick Connection mode, ensure that both the Appliance and Autostart modes are disabled. If either of two modes are enabled, the Quick Connection mode will fail to work.
- For more information on the Appliance mode, please refer to section "3.2.8 Enabling or Disabling the Appliance Mode" 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

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

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

0	Atrust Client Setup					
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Auto Setup Quick Connection - Power Management - Terminal - Error Report - Certificate Manager - Advanced - System information	General Basic Settir Ena		ion after Power-	dn		

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.



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 Dendering	Check/Uncheck to enable/disable client rendering.				
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.				

盲 🗌 Redirect Connected USB Devices

* All connected USB devices will be redirected unless more specific settings are specified below.

* Enabling USB Redirection on the server side is also required for this feature.

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.			

Use of USB Storage Devices:	Mapping 🗾	Ê
Use of USB Printers:	Mapping 🗾	Ē

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 .

Plugged USB De	vices: 1	
(Vendor: 2047 P	roduct: 03df) Texas Instruments	
(Vendor: 0bda P	roduct: 0129) Realtek Semiconductor Corp. RTS5129 Ca	ard Reader Con
Redirection Rule	s: 2	
* Use redirection	n rules to manage specific USB devices.	
* Maximum num	ber of rules: 10	
Allow 🔽 Ve	ndor ID: Product ID:	Add

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



• 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**.

٥		Atrust Client	Setup			↑ - □ ×	
Atrust	Applications	User Interface	Devices	Network	System		
Navigator - Time Zone - Password - Firmware Update - Appliance Mode - Auto Setup Ouick Connection - Power Management - Terminal - Error Report - Certificate Manager - Advanced - System Information	General Extra Appin C Web * This sette VMware Vie Mass Stor Smart Car Human Int Printer: Plugged U	b Browser ing will take effect w Option age: d: erface Device: SB Devices:	after you re-er	INERNOTIK	nection mode.	•	0
	(Vendor: 0	46d Product: c52 986 Product: 054	e) Logitech, Inc		a louenpau		2
	* Use redii	rection rules to ma n number of rules: Vendor ID: Cancel	10	ISB devices. duct ID:	Ad	id E	3

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**.

Mass Storage:	Enabled 🗾	E
Smart Card:	Disabled 🗾	£.
Human Interface Device:	Disabled 🗾	£.
Printer:	Enabled 💌	Ê,

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

Plugged USB Devices: 2
(Vendor: 046d Product: c52e) Logitech, Inc.
Redirection Rules: 3 * Use redirection rules to manage specific USB devices. * Maximum number of rules: 10
Allow Vendor ID: Product ID: Add

- 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 <i>Plugged USB Devices</i> (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:

Extra Application Buttons	
盲 🗌 Web Browser	
* This setting will take effect after you re-enter the Quick Connection mode.	

Atrust Quick Connection Screen

Atr	rust Quick Connection	
	Remote Desktop	
	Citrix	
	VMware View	
	🕑 Web Browser	
😺 Web Browser		
Web blowser		
		Atrust
0 0 0		4 📼 🖣

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**.

0		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Dimmed LC Turn off LCI Enter Susp Suspend o Battery por Dimmed LC Turn off LCI Enter Susp	aving mode: D: D: eend or Shutdown: r Shutdown after (wer saving mode: D:	(Never = Disable)		Low Never Suspend Never Medium 5 minutes later 10 minutes later Suspend 1 hour later	

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.

When your mt182L enters *System Sleep mode* manually (Fn + F12 or U) > 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**.

Atrust Client Setup							
Atrust	Applications	User Interface	Devices	Network	System		
Navigator Time Zone Password Firmware Update Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	General	ngs	у				

- 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.

	DTE To open Terminal via the shortcut, click START > Settings > Terminal on the local Linux desktop.
	Atrust Client Setup System Information Ferminal
•	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.

• This U	JSB flash drive will be used for storing the event logs of your mt182L.
For de	e that you have enabled the access and automount of USB storage devices. etailed instructions, please refer to section "3.4.3 Configuring Settings for USB ge Devices" on page 94.
• Please	e note that files saved on the local desktop will be deleted after restart.

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

٨		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Auto Setup - Quick Connection - Power Management - Terroir Report - Certificate Manager - Advanced - System Information	Please ser	eenshot screenshot tool to Address: ame:	t file to your ad	ministrator.		

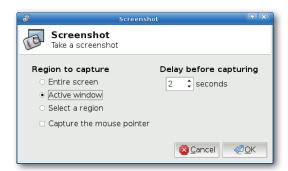
3. Click **Collect Log**. A window appears prompting you to choose where to save the log file set (named **events.tar.gz**). The attached USB flash drive is the default location if attached. Click **Save** to apply.

	Save Archive file to
Look in:	📄 /media/BOOT 🔹 🌸 🔶 👚 📰 🗐
📃 Co 💿 user	efi firmware
📄 воот	install.386
File <u>n</u> ame:	events.tar.gz
– Files of type:	

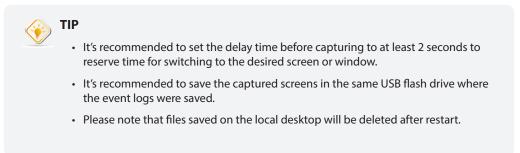
Capturing Error-Related Screens

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.



3.2.15 Uploading Files for Error Reporting

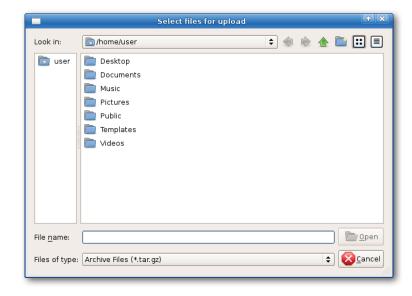
You can upload files to a specified FTP server for error reporting.

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

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

0		Atrust Client	Setup			↑ _ □ ×
Λtrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Auto Setup Quick Connection Power Management Terrinial Error Report Certificate Manager Advanced System Information	Please sen Collect Loo	Int logs to USB sto ad the Error Repor eenshot screenshot tool to eenshot s Address: ame:	t file to your ad	ministrator.		

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.





• 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)

• 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.

٨		Atrust Client S	etup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Appliance Mode - Auto Setup - Quick Connection - Power Management - Terminal - Error Report - Advanced - System Information	Applications Add Issued to	- Delete	Devices Expired on	Valid	System	

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

٩	Atrust Client Setup					
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Time Zone Password Firmware Update Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	servers). File Name: Note: Pleas From Server Enter the II and then c IP address From Atrust	Se select PEM or D address / URL / I lick Import (up to / URL / FQDN: [Device Manager -	ER format certi	certificates in tota ficate from your U ver where you war in total, including ne Atrust Device M	Browse	Import ice. rtificate(s),

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

٨		Atrust Client	Setup			-	×
Atrust	Applications	User Interface	Devices	Network	System		
Navigator	+ Add	- Delete					
Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information	Issued t			ssued by Microsoft Code Verifi	cation Root	Expired on 2021-04-15	
	•				<u> </u>		1

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.

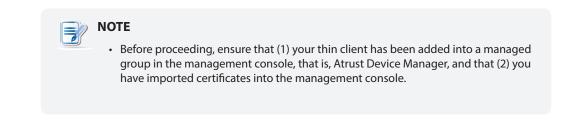
0		Atrust Clier	it Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Appliance Mode - Auto Setup - Quick Connection - Power Management - Tror Report <u>Certificate Manager</u> - Advanced - System Information	servers). File Name: Note: Pleas From Server Enter the II and then c IP address From Atrust	Se select PEM or P address / URL lick Import (up f / URL / FQDN: Device Manager	DER format cert / FQDN of the set to 16 certificates www.google.com	i certificates in to	Browse	Import /ice. ertificate(s),

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

٩		Atrust Client	Setup			•	. 🗆 🗙
Atrust	Applications	User Interface	Devices	Network	System		
Navigator	+ Add	- Delete					
 Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information 	Issued I	to ♥ Issued t Global CA Equifa		cate Authority	Expired on 2018-08-21	Valid Valid	Impo Serve
	4						<u>+</u>

Importing certificates from Atrust Device Manager through the network

To import certificates from Atrust Device Manager 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 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.

		Atrust Client	Setup			 □ 	
Atrust	Applications	User Interface	Devices	Network	System		
Navigator - Time Zone - Password - Firmware Update - Auto Setup - Quick Connection - Power Management - Terminal - Error Report Certificate Manager - Advanced - System Information	+ Add Issued t Go Dadd	- Delete	← e Authority - G2 uthority - G2	Issued by Go Daddy Root Microsoft Code		-	Expire 2031- 2031-
	•						×

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.

٥		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Auto Setup - Quick Connection - Power Management - Terminal - Error Report - Certificate Manager Advanced - System Information	General		ion			

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.

	Atrus	t Client Setup			◆ - □ ×
Atrust	Applications User Inte	erface Devices	Network	System	
Navigator - Time Zone - Password - Firmware Update - Auto Setup - Quick Connection - Power Management - Terminal - Error Report - Certificate Manager	System Ne System Product Name : Host Name : BIOS Information : MCU Version :	mt182L atrust-4616DA 1.24 v20			
– Certificate Manager – Advanced System Information	Firmware Version : CPU : RAM : Flash : Serial Number :	4trust Linux v5.40-IN Intel(R) Atom(TM) x5 4096 MB 30 GB 123456789			
	Back				

0		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	System	Network				
 Time Zone Password Firmware Update Appliance Mode Auto Setup Quick Connection Power Management Terminal Error Report Certificate Manager Advanced System Information 	Ethernet IP Address : MAC Address Subnet Mask Gateway : DNS : Speed : Wireless IP Address Subnet Mask Gateway : DNS : Back	255.255 192.168 192.168 192.168 100Mbp 0.0.0.0 : d4:6d:60	3:ba:ec:86 .255.0 .0.1 .0.2 .0.5			

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.

Output Applications User Interface • Display Desktop • Display Configure display settings Screensaver Desktop Configure desktop settings Configure desktop settings Configure desktop settings Configure desktop settings
Display Desktop Keyboard Mouse Screensaver Desktop Configure display settings Desktop Configure desktop settings
Desktop Keyboard Mouse Screensaver Desktop Configure display settings Desktop Configure desktop settings
Configure mouse settings

User Interface Tab Overview

Inter	face 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
	Display		Click to configure display settings.	3.3.3	80
Deskt	Desktop		Click to customize desktop and system language.	3.3.4 3.3.5 3.3.6	83 86 87
User Interface	Keyboard		Click to adjust keyboard settings.		
	Mouse	õ	Click to adjust mouse settings.	3.3.8	90
	Screensaver	Ţ	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**.

٨		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Display Desktop Keyboard Mouse ScreenSaver	General Display — Number of Display Lay Monitor Set Resolution	Display: yout: ttings	1 Use LCC		20x1080)	

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).

Display						
Item		Description				
	Click to select the	e number of used display(s).				
	Option I	Option Description				
Number of Display	1	One display is used.				
	2	Two displays are used.				
	Click to select the	e arrangement of displays.				
	Option	Description				
	Use External	Use the single external display attached.				
	Use LCD	Use the single internal display (LCD panel).				
	External - LCD horizontal	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.				
Display Layout	LCD - External horizontal	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.				
	External - LCD vertical	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.				
	LCD - External vertical	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.				
	down menu:	able only when 2 is selected in the Number of Display drop-				
Display Mode	Extend	One display is used as the extended display of the other.				
	Clone	Two displays have the same display content.				

Monitor Settings						
Item	Description					
		eck to enable/disable the automatic detection of the used monitor(s) ent is powered on.				
	Option Description					
Enable Auto-Detection at	Enabled	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.				
Power-up	Disabled	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).				
	Use this item	n to set an appropriate resolution for the used display.				
	Auto	This option is available only when Enable Auto-Detection at Power-up is selected.				
Monitor Resolution	Other options	Select the desired resolution from the Resolution drop-down menu for the used display.				
	drop Pleas	esolutions supported by the client will be listed in the Resolution -down menu when Auto-Detection at Power-up is disabled. Se note that some resolutions may not be applicable to monitor(s).				

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**.

٨	Atrust Client Setup	+ - • ×
Atrust	Applications User Interface Devices Network	System
Navigator Display Desktop Keyboard Mouse Screensaver	General System Language Language: This setting will take effect after reboot.	
	Default Fonts Sans Default Font Regular Default Font Style: Regular Default Font Size: 12	
	Title Font: Sans Title Font Style: Regular Title Font Size: 10	
	DPI Custom DPI Setting: Normal Some settings will take effect after reboot.	
	Desktop Icons Image: Clip Clip Clip Clip Clip Clip Clip Clip	

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,		
Default Font Style	text labels for desktop shortcuts, tabs on program windows etc.		
Default Font Size	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).		
Title Font			
Title Font Style	Click the drop-down menus to select the desired font, its style and size used for the titles of the opened windows.		
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 X on the START menu and local Linux desktop.
Firefox Web Browser	Check/Uncheck to show/hide desktop shortcuts Firefox Web Browser o 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.
PDF Viewer (Document Viewer)	Also see "Topic 5: Using Built-in Applications" on page 36. 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.

	1			
Icon Size	Click the drop	Click the drop-down menu to select the desired size of desktop icons/shortcuts.		
Icon Font Size		Click the drop-down menu to select the desired text label size of desktop icons/shortcuts.		
Desktop Background				
Item	Description			
	Check/Unchec	k to enable/disable the use of Atrust wallpaper.		
Enable Desktop Wallpaper	NOTE: If disa	bled, the solid color background (dark blue) will be used.		
Enable Custom Wallpaper	'	k to enable/disable the use of a custom wallpaper. More settings		
Download From	appear when			
Custom Wallpaper File	For details, pl	ease refer to "3.3.6 Using a Custom Wallpaper" on page 87.		
		-down menu to select the way to apply the wallpaper. Five options Centered, Tiled, Stretched, Scaled, and Zoomed. Description		
	Centered	Centers the original image on the screen.		
	Tiled	Tiles the screen with the original image.		
Wallpaper Style	Stretched	Centers and extends/shrinks the image to fit the screen.		
	Scaled	Centers and sizes the image proportionally to fit the screen until the top-bottom or left-right sides fit the screen.		
	Zoomed	Centers and sizes the image proportionally to fill the screen.		
	NOTE: Depen	Centers and sizes the image proportionally to fill the screen. ding on the size of the connected display, two options might have me effect.		
Wallpaper	NOTE: Depen the sa	ding on the size of the connected display, two options might have		
Wallpaper Taskbar	NOTE: Depen the sa	ding on the size of the connected display, two options might have me effect. -down menu to select the color of Atrust wallpaper. Four colors are		
	NOTE: Depen the sa	ding on the size of the connected display, two options might have me effect. -down menu to select the color of Atrust wallpaper. Four colors are		
Taskbar	NOTE: Depen the sa Click the drop available: Gre Description	ding on the size of the connected display, two options might have me effect. -down menu to select the color of Atrust wallpaper. Four colors are		

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.

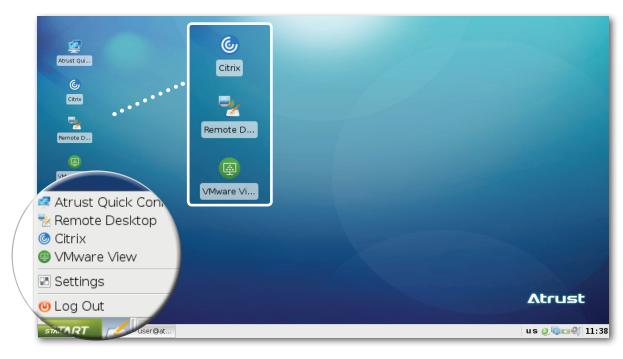
NOTE
They're hidden by default.

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**.

٥	¢.	trust Client	Setup			- C	
Atrust	Applications Us	ær Interface	Devices	Network	System		
Navigator Display Desktop Keyboard Mouse Screensaver	System Language: This setting with Desktop Fonts Default Font SI Default Font SI Title Font: Title Font Size:	ge // <i>take effect a</i> ryle: ze:		English Sans Regular 12 Sans Regular 10			
	DPI Custom DPI Se Some settings Desktop Icons - E Remote E Citrix Save C	will take effe	ct after reboot.	Normal			•

- 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

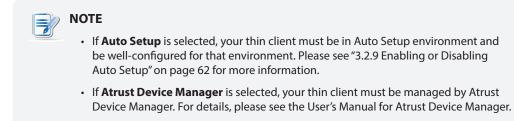
To use a custom wallpaper, please do the following:

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

٨	Atrust Clie	ent Setup			• - •	X
Λtrust	Applications User Interface	Devices	Network	System		
Navigator Display Desktop Keyboard Mouse Screensaver	General Icon Font Size: Desktop Background		10 Stretched Blue		-	1
	Taskbar Auto-hide the task Taskbar Size:	Dar	32		-	4

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.



4. Provide other information if required.

NO
•

ГΕ

- 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.

٥	Atrust C	lient Setup			↑ _ □ ×
Atrust	Applications User Interfa	ce Devices	Network	System	
Navigator Display Desktop Keyboard Mouse Screensaver	General Keyboard Use Custom Keyb Keyboard Layout: Keyboard Type: NumLock Enable NumLock Cursor	-	Japanes Japanes	ie (JIS) ie 106-key	
	☑ ☑ Show BlinkingBlink Delay	1300			Ê
	Type Settings Repeat Speed Repeat Delay	20			Ê
	Save Cancel				

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 La	yout	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 Num	Lock on Boot	Check/Uncheck to enable/disable the NumLock key after system startup.	
Curren	Show Blinking	Check/Uncheck to enable/disable the cursor blinking (local desktop only).	
Cursor Blink Delay		Move the slider to select the blink delay between each occurrence of cursor.	
Repeat Speed		Move the slider to select the character repeat rate when a key is held down.	
Settings 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.

Arabic	^	
Arabic (AZERTY)		
Arabic (AZERTY / digits)		
Arabic (digits)		
Arabic (QWERTY)		
Arabic (OWERD) (July)		
Canada (French Dvorak)		
Canada (French (legacy))		
Canada (Multilingual)		
Canada (Multilingual first part)		
Canada (Multilingual second part)		

- 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**.

٩		Atrust Client	: Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Display - Desktop - Keyboard Mouse - Screensaver	General Mouse Button Ord Enable tou Disable tou Feedback Acceleration Threshold Save	chpad: Ichpad when the	USB mouse inser	Right hai	nded	

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		
Ite	em	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.
Accelerati		Move the slider to select the rate at which the mouse increases speed while moving.
Feedback	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**.

٨		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Display Desktop Keyboard Mouse Screensaver	Display Display	ble Screensaver	e after Screensa	aver (minute):	Blank 10 5	
	Additional S When I clos				Turn off LCD	

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

Screensaver				
Item	Description			
Enable Screensaver	Check/Uncheck	Check/Uncheck to enable/disable screensaver.		
	Click to select th Blank, Logo, ar	ne display mode of screensaver. Three options are available: nd Image .		
	Option	Description		
Display Mode	Blank	Displays a black screen.		
	Logo	Displays the Atrust floating logo.		
	Image	Displays the specified images.		
Display After (minute)	Click to select th	ne wait time for screensaver.		

	Click to select where to get the images and use for screensaver. Three options are available: Default , Auto Setup , Atrust Device Manager .			
	Option	Description		
	Default	Uses the default image in your thin client.		
Specify the source	Auto Setup	Gets and uses images from Auto Setup.		
	Atrust Device Manager	Gets and uses images from Atrust Device Manager.		
	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.			
Change picture every	Click to set the interval to	change the displayed image.		
Enable Display Sleep Mode	Check to turn off (i.e. sto energy savings.	p sending signals to) the display to maximize the		
Enter Display Sleep Mode after Screensaver (minute)	Click to select when to tu Screensaver starts.	rn off (i.e. stop sending signals to) the display after		
On Resume, Password Protect	Check/Uncheck to resume	e with/without a password.		
Additional Settings				
Item	Description			
When I close the lid	Click to select what to do	when you close the lid.		



• 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.

	(1)		Atrust Client	Setup			↑ _ □ ×	
	Atrust	Applications	User Interface	Devices	Network	System		
	Navigator	Devices						
0	• •• USB Storage Audio Printer	Configu	ure USB storage se ure audio device se	ettings			····· •	2

Devices Tab Overview

Inter	face 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
	USB Storage	Ŷ	Click to configure settings for USB storage devices.	3.4.3 3.4.4	94 95
Devices	Audio	G	Click to configure settings for audio devices.	3.4.5 3.4.6 3.4.7	96 97 98
	Printer	٨	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:



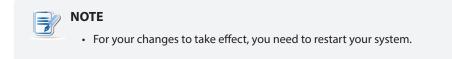
1. On Atrust Client Setup, click **Devices** > **USB Storage**.

(1)		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator USB Storage Audio Printer	🔓 🗹 Enat	e ole USB Storage ole Automount mg will take effect Cancel	after reboot.			

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.



3.4.4 Manually Mount and Eject Attached USB Storage Devices

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



- 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

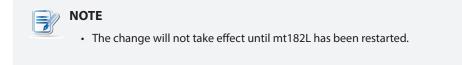
To disable/enable attached audio devices, please do the following:

NO	TE
•	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

- (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**.

٨	Atrust Client Setup					↑ - □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator USB Storage Audio Printer		ble System Audio I ing will take effect				

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



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 \P icon in the bottom-right corner.
 - On the *local desktop*, right-click 🤍 icon in the bottom-right corner, and then select **Sound Preferences**.

0)	Sound	↑ _ X
Settings		
Output volume: 🥥 📕 Output Input Applicati	ions	
Choose a device fo	r sound output:	
🧿 Speakers - Built-in		
🞯 Speakers - USB Pr	14 Sound Device	
Settings for the se	lected device:	
Balance:	Left Ri	l ight
Profile:	Analog Stereo Output	▼ Test Speakers

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**.

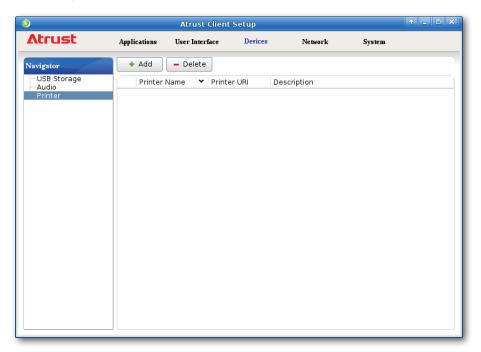
٩		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - USB Storage Audio - Printer		ble System Audio ing will take effect				

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

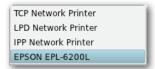
3.4.8 Adding a Local Printer

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.

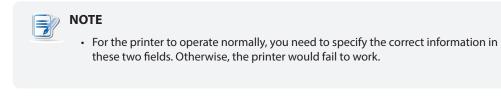


7. Fields in the Add Printer section will automatically change to fit the type of the selected printer.

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

٩		Atrust Client	t Setup				C	
Atrust	Applications	User Interface	Devices	Netwo	rk	System		
Navigator - USB Storage - Audio Printer	 ✓ Mapp 	ne -6200L :: :- e Printer oing in RDP Sessi oing in ICA Sessio oing in VMware So	ons	* ?	EPSON EPL	-6200L 2160612111		
	Save	Cancel						

- 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.



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



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

Settings for Printers Item Description			
Item			
	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:		
	 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.		
Share Printer	 Click Stop to cancel the automatic printer search, and then click The printer that I want isn't listed. 		
	 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		
	 Click Next to continue. 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.		
	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:		
	 Attach the printer to a computer running a Windows OS, complete the required installation, and ensure the printer works well. 		
	 Click Start > Devices and Printers, and then, in the opened window, 		
	right click the printer to open a popup menu.		
Windows Driver Name	 On the popup menu, click to select Printer properties. In the opened window, click Advanced. The driver name is shown. 		
	In the opened window, elect Advanced . The driver halffe is shown.		
	First Epson EPL-6200L Forter General Sharing Pots Advanced Color Management. Security Optional Settings Available 00.00 Priority: 1 Driver: Epson EPL-6200L		
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.

Add Printer	
Printer Name	*
Printer Port:	TCP Network Printer
TCP Print Server	*
TCP Port	9100
Description:	É
Add Printer	
Add Printer Printer Name	*
Printer Port:	LPD Network Printer
LPD Print Server	*
LPD Queue Name	E
Description:	E
Add Printer	
Printer Name	*
Printer Port:	IPP Network Printer
IPP URI	*

- 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.

_ (3)	Atrust Client Setup	• _ • ×
Atrust	Applications User Interface Devices Network	System
Navigator	Network	
- Ethernet - VPN - Hosts - Host Name - Wireless - Proxy	Ethernet Configure wired network settings VPN Configure VPN (Virtual Private Network) connection set Hosts Create the mapping of IP addresses to host names and Host Name Adjust the host name for your client Wireless Configure wireless network settings Proxy Configure proxy settings for Web-based access to server	nd aliases

Network Tab Overview

Interface Elements				
Name	Description			
Navigation area	Click to select a setting item under Network tab or to select a setting entry under a selected setting item.			
Configuration area	Configures setting values when a setting item or entry is selected.			
í	Name Navigation area			

3.5.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
	Ethernet	-	Click to configure wired network settings.	3.5.3 3.5.4	105 108
	VPN	S	Click to configure VPN (Virtual Private Network) connection settings and create a VPN connection.	3.5.5 3.5.6	109 113
Network	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
Network	Host Name	1	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.

Interface		
IP Address	DHCP	- 6
DNS DNS Type:	Dynamic DNS (via DHCP)	

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:



• 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.

٥	Atrus	st Client Setup		. □ ×
Atrust	Applications User Int	terface Devices	Network	System
Navigator Ethernet VPN Hosts Host Name Wireless Proxy	General Interface P Address IP Type: IP Address: Subnet Mask: Gateway: DNS Search Domain:		* * *	
	Nameserver 1: Nameserver 2:			

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

IP address IP type:	Static IP
IP address:	* 192.168.12.88
Subnet mask:	* 255.255.255.0
Gateway:	* 192.168.12.254

) ΝΟΤΕ

- 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.



• 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:



• 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:

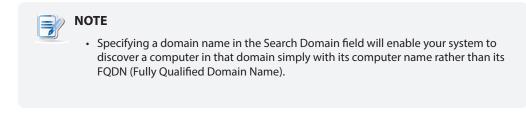
- 1. On Atrust Client Setup, click **Network** > **Ethernet**.
- 2. Under the DNS section, click the drop-down menu to select Manual setting.
- 3. The Search domain, Nameserver 1, and Nameserver 2 fields appear in the DNS section.

Difference 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)**.

٥		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet - VPN - Hosts - Host Name - Wireless - Proxy	Wake On L	main: er 1: er 2:	ation	DHCP Manual s		

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.



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**.

		Atrust Client	Setup			+ - • ×
Λtrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet - VPN - Hosts - Host Name - Wireless - Proxy	UNS	ble	ation	DHCP Dynamic Enabled	DNS (via DHCP	

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

(1)		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet - VPN - Hosts - Host Name - Wireless - Proxy	Authentica Identity: CA Certific: Private Key	ANANANANANANAN: tionAN: tionAIL Authentic ation: date Server Certific ate:	ation	Enabled	NS (via DHCP)	

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



• 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.



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.

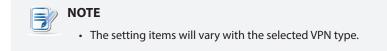
3		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Ethernet VPN - Hosts - Host Name - Wireless - Proxy	Connections	Settings Delete on Name VPN T		Comment		

• 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**.

0		Atrust Client	Setup			
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet VPN Hosts Host Name Wireless Proxy	Authenticatio	Name: ess: js Compression Sett ioint-to-Point encry	-	* PPTP * *		



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.

0		Atrust Client	Setup			+ _ O ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	Connections	Settings				
VPN Hosts	+ Add	- Delete				
Wireless Proxy	Connect	tion Name VPN		Comment Connected		

- 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 Source button then appears on the top of the Virtual Private Network list.

٨		Atrust Client	Setup			+ ×
Λtrust	Applications	User Interface	Devices	Network	System	
Navigator - Ethernet VPN - Hosts - Host Name - Wireless - Proxy	Connections Add Connec Gamma Add Connections Add Connections Add Connections	- Delete	Type Status	nnect Connected		

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.

0		Atrust C	lient Setu	р		-	
Atrust	Applications	User Interfa	ice De	vices	Network	System	
Navigator - Ethernet VPN - Hosts - Host Name - Wireless - Proxy	Connections Add Connect Add Add ATSVPN	 Delete tion Name 		Status connected	Commer Connecte	ıt d before, auto connec	t

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 *P* 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 <a>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.

٨		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Ethernet VPN - Hosts - Host Name - Wireless - Proxy			tup	ATSVPN		

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.

٨		Atrust Client S	etup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet -VPN Hosts Host Name -Wireless Proxy	+ Add Hostnam	- Delete ne ▼ IP Address	Alias / C	Group Priority		

- 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.

Hosts Table Settings)
Hostname:	* WS2012R2RDSH
IP Address:	* 192.168.7.12
Alias / Group:	WS12
Priority:	Ê



- 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.

3		Atrust Client S	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet VPN - Hosts - WS2012R2RDSH Host Name Wireless Proxy	+ Add Hostnar	 Delete me ✓ IP Address R2RDSH 192.168.7 		iroup P O	iriority	

- 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

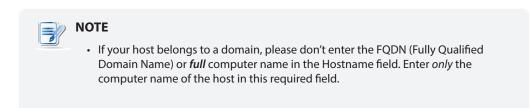
To create a Failover Cluster list, please do the following:

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

		Atrust Client S	etup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet - VPN Hosts Host Name - Wireless Proxy	* Add Hostnam	- Delete P Address	Alias / Gro	up Priority		

- 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.

CHosts Table Settings	
Hostname:	* ADM1
IP Address:	* 192.168.7.21
Alias / Group:	ADM 🗧
Priority:	1
[



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

٥		Atrust Client S	Setup		↑ . □ ×
Atrust	Applications	User Interface	Devices	Network	System
Navigator	+ Add	– Delete			
Ethernet VPN	Hostnam	e 👻 IP Address	Alias / Gr	oup Priority	
Hosts	ADM1	192.168.7		1	
- ADM1	ADM2	192.168.7		2	
ADM2 ADM3 Host Name Wireless Proxy	ADM3	192.168.7	.23 ADM	3	

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

Hostname	✓ IP Address	Alias / Group	Priority	
ADM1	192.168.7.21	ADM	1	
ADM2	192.168.7.22	ADM	2	
ADM3	192.168.7.23	ADM	3	

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.

0		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Ethernet VPN Hosts Host Name Wireless Proxy	General Name Settir Host Name * This settir Save		after reboot.	* atrust-46	516DA	

- 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:



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

3		Atrust Client	Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Atrust Navigator Ethernet VPN Hosts Host Name Wireless Proxy	Connection		Devices	Yes	System	

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

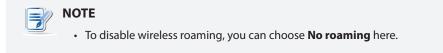
3.5.11 Configuring the Trigger Threshold for Roaming

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.

٩		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Atrust Navigator Ethernet -VPN Hosts Host Name Wireless Proxy	Connection Interface – Enable wir			Network	System	

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



3. Click Save to apply.

3.5.12 Establishing and Stopping a Wireless Connection



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.

Atrust							
Acrusc	Applications	User Interface	Devices		Network	System	
lavigator	Connection	wireless					
Ethernet VPN Hosts	+ Add	- Delete	🔍 Scan				
Host Name	SSID	Priorit	y Signal	^	Security	Status	Comment 📤
Wireless	HP-PI	int-F9-L 20	100		Insecure		
Proxy	IT-AP	2 20	100		WPA		
	SMCV	/GBR14 20	100		WPA		
	roam	ing24 20	100		WPA		
	roam		100		WPA		
		AP01 20	97		WPA 802.1x		
		ortable 20	94		WPA		
		VK_F36B 20	94		WPA		
	MIX2	20	91		WPA		
		a_2.4G 20	81		WPA		
		AP02 20	81		WPA		
	Кікі-к		80		WPA		
	gues		80		WPA		
		VK_EF01 20	74		WPA		
	Batte	rylife_5G 20 03 20	72 70		WPA WPA		
		13 20 LOOON 20	70		WPA		_
		r~HerH 20	68		WPA		
	MIX5	20 20	64		WPA		
	IT-AP		62		WPA		
		N-69B0 20	60		WPA		
		N-9920 20	55		WPA		
	СНТ1		54		WPA		
	min h		54		WPA		-
		20					I → []



• 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 Science button then appears on the top of the Wireless Network list.

		Atrust Client	Setup			
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	Connections	Wireless				
Ethernet VPN Hosts	+ Add	- Delete	🔍 Scan 🏒	🔊 Connect		
Host Name	SSID	Priority	/ Signal	 Security 	Status	Comment 📤
Wireless	HP-Pri	nt-F9-L 20	100	Insecure		
Proxy	✓ IT-AP0	2 20	100	WPA		
	SMCW	GBR14 20	100	WPA		
	roamir	ng24 20	100	WPA		
	roamir		100	WPA		
	Demo-		97	WPA 802.1x		
	HTC PC	ortable 20	94	WPA		
	TP-LIN	< F36B 20	94	WPA		
	MIX2	20	91	WPA		
	sophia		81	WPA		
	Demo-		81	WPA		
	KiKi-KR		80	WPA		
	guest		80	WPA		
		<_EF01 20	74	WPA		
		ylife_5G 20	72	WPA		
	IT-AP0		70	WPA		
	DSR-1		70	WPA		_
		~HerH 20	68	WPA		
	MIX5	20	64	WPA		
	IT-AP0		62	WPA		
		V-69B0 20	60	WPA		
		V-9920 20	55	WPA		
	— _ снтіо		54	WPA		_
	min h	ome 20	54	WPA		
						<u>`</u>

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

Ø Wireless Network Au	thenticationRequired 📃 💽
Authentication required by wireles keys are required to access the w	s network. Passwords or encryption ireless network.
Wireless Security:	WPA & WPA2 Personal 🔹
Key:	*
Show character	
	Connect Cancel



- 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.

	SSID	Priority	Signal	Security	Status 🔺	Comment
	IT-AP02	20	100	WPA	connected	Connected before
	sophia_2.4G	20	92	WPA		
	roaming5	20	87	WPA		
·····	roaming24	20	100	WPA		
···· 🗌	guest001	20	87	WPA		
·····	dlink_DWR-113	20	38	WPA		
···· 🗌	dir-810-5g	20	45	WPA		
·····	dir-810-2g	20	94	WPA		
	amphenol_S	20	72	WPA		

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 *P* 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.

Onfire	Confirm Dialog							
You are going to connect this n Are you sure?	etwork.							
Wireless Network Name (SSID):	*							
Security:	Disable Encryption							
	Connect Cancel							

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

OTE
• 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.



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:

	Atrust Client	Setup			↑ _ □ ×
Applications	User Interface	Devices	Network	System	
General Wireless Se Wireless Na Mode: Connect au Priority: Authenticat Security:	IPV4 Settings		IT-APO: Manag Enable 20 WPA &	2 ged ed WPA2 Personal	
Save	Cancel				
	General Wireless Set Wireless Ne Mode: Connect au Priority: Authenticat Security:	General IPV4 Settings Wireless Settings Wireless Network Name (SSID Mode: Connect automatically: Priority: Authentication Security: Network Key:	General IPV4 Settings Wireless Settings Wireless Network Name (SSID): Mode: Connect automatically: Priority: Authentication Security: Network Key:	General IPV4 Settings Wireless Settings IT-APO: Wireless Network Name (SSID): IT-APO: Mode: Manage Connect automatically: Enable Priority: 20 Authentication Security: Network Key: Ifference	General IPV4 Settings Wireless Settings IT-AP02 Mode: Managed Connect automatically: Enabled Priority: 20 Authentication Security: Network Key: ####################################

• 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.



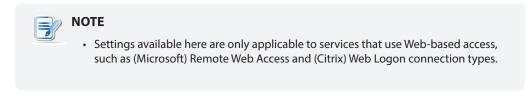
- To connect to wireless networks in order of priority, you can set **Priority**. By default, there is no priority, and the lowest value, **20**, is given for all networks.
- On the IPV4 Settings tab, click the drop-down menu or type values in fields to configure IP settings.



- 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:



- 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.

• The setting items will vary with the selected mode.

0		Atrust Clien	t Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Ethernet - VPN - Hosts - Host Name - Wireless - Proxy	General Connection Mode: * These set (Microsoft) Save		No Proxy plicable to servi ess and (Citrix)	ces that use Web- Web Logon conne	based access, ction types.	such as

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

Connection Settings						
Item	Description					
	Click to select the desi	red proxy configuration mode.				
	Mode	Description				
	No Proxy	Don't use any proxy server.				
Mode	Auto-detect proxy settings	Detects the proxy settings for your network automatically.				
	Manual proxy configuration	Configures the proxy settings manually.				
	Auto proxy configuration	Loads proxy settings automatically through the connection to a proxy configuration file.				
Mode: Manual proxy config	uration					
HTTP Proxy	Provides the IP addres	s of your HTTP proxy server.				
Port	Provides the port numl	per which your HTTP proxy server uses.				
No Proxy for	Provides No Proxy list. Don't use any proxy server while connecting to the specified URLs.					
Mode: Auto proxy configura	ation					
URL	Provides the URL of a proxy configuration file where proxy settings can be loaded through the network.					

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

	0		Atrust Client	Setup			×	
	Atrust	Applications	User Interface	Devices	Network	System		
•	Navigator	Applications						
1	• • Remote Desktop - Citrix ICA - VMware View - SSH - Web Browser - Parallels 2X Client	Config	e Desktop Available ure RDP (Remote D ICA Available Sessi ure Citrix ICA connu- re View Available Se ure VMware View c vailable Sessions: (ure SSH (Secure S rowser Available Se ure local browser s els 2X Client Availab ure Parallels 2X Cli	Desktop Protoco iions: 0 ection settings iessions: 0 onnection settii 0 hell) session se essions: 0 settings ole Sessions: 0	ngs	tings		

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
	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 (🕢 Architecture) connection		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
Applications	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	2	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	۷	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.

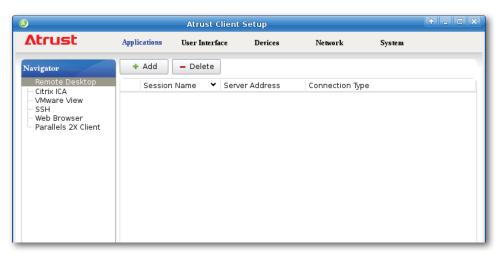
Three connection types are available:

Connection Type	Connection Type Description				
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.





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

()		Atrust Clie	nt Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	General Server Setti Session Na Computer: Connectior Network Le Authentica Server Auth Login Settin Username:	Options mgs mgype: vel tion: hentication: gg	Derices	* * Remo Enabl	te Desktop	arn me
	Common Se	Vhen Startup:	jin	No Do Not	thing	

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.



- To create an entry of RDP connection settings for MultiPoint[™] Remote Desktop sessions, please do the following:
 - In the Server Settings section, click 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.



• 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.

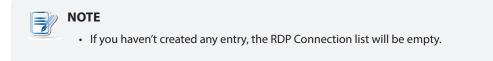
Connection Type: Remote Web Access

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



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

٨	Atrust Client Setup					+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	+ Add Session	– Delete	ierver Address	Connection Typ		



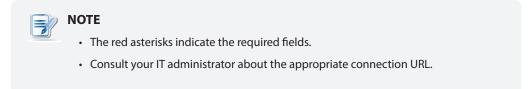
3. Click **Add** on the top of the RDP Connection list to create a new entry of RDP connection.

		Atrust Clie	nt Setup		↑ _ □ ×
Δtrust	Applications	User Interface	Devices	Network	System
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	General Server Setti Session Na Computer: Connection Network Le Authentica Server Auth Username: Password:	me: n Type: vel tion: nentication: gs	RD Gateway	Enable	e Desktop V ed V ct and don't warn me V
	Domain:	Smart Card Log	in		

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

٨		Atrust Clie	nt Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options	RD Gateway			
Remote Desktop Citrix ICA VMware View	Server Setti	ngs ———				
Web Browser Parallels 2X Client	Session Na	me:		*		Ê
	Connection	URL:		*		£
	Connection	Туре:		Remote	Web Access	- E
	Common Se	ttings ———				
	Autostart W	/hen Startup:		No		
	On Applicat	ion Exit:		Do Noth	ing	
	Save	Cancel				

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



- 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.

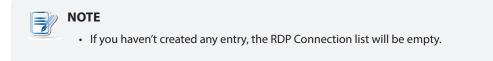
Connection Type: Web Feed

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



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

3		Atrust Cli	ient Setup			↑ _ □ ×
Atrust	Applications	User Interface	e Devices	Network	System	
Acrust Navigator Remote Desktop Chrix ICA VMware View SSH Web Browser Parallels 2X Client	Applications Add Session	– Delete	e Devices	Network		



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

٨		Atrust Clie	nt Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options	RD Gateway			
Remote Desktop Citrix ICA	Server Sett	ings ———]
- VMware View SSH	Session Na	ame:		*		6
Web Browser Parallels 2X Client	Computer:			*		6
	Connection	n Type:		Remo	ote Desktop	- E
	Network Le Authentica			Enab	led	- 6
	Server Aut	hentication:		Conn	iect and don't w	arn me 💌 盲
	Login Settir	ngs —				
	Username:					6
	Password:					6
	Domain:					£
	📔 🗆 Use	Smart Card Loo	jin			
	Common Se	ettings —				
	Autostart \	When Startup:		No		- 6
	On Applica	tion Exit:		Do No	othing	£
	Save	Cancel				

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

٩		Atrust Clie	nt Setup			+ - • ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options	RD Gateway			
Remote Desktop Citrix ICA VMware View	Server Setti	ngs				
SSH Web Browser Parallels 2X Client	Session Na	me:		*		£
	Web Feed U	JRL:		*		£
	Connection	Туре:		Web Fe	ed	- 6
	Login Settin	as				
	Username:	90		*		6
	Password:			*		6
	Domain:			*		£
	RemoteApp	and Desktop C	onnections			
	Update Nov	v				
	Summary:					
	Last Updat	e:				
	Save	Cancel				

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

) ΝΟΤΕ

- 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.

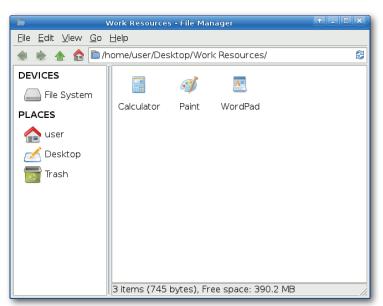
RemoteApp and Update Now	Desktop Connections	Ì
Summary:	3 applications, 0 desktops	
Last Update:	Mon Jun 30 2014 10:13:16	



- 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.





• 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:

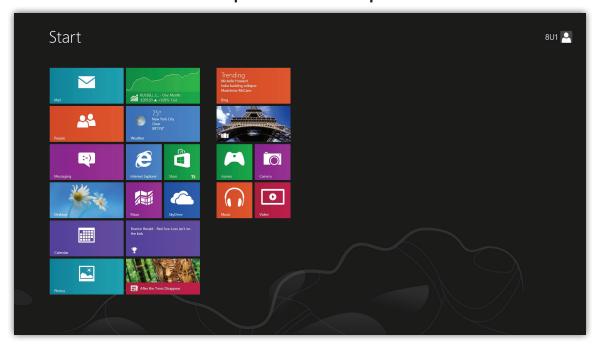
- 1. Double click the created shortcut on the desktop.
- 2. Follow the on-screen instructions and provide required credentials if needed.
- 3. The remote desktop will be displayed on the screen.

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.

ſ	Et not North Resources	Web Access
		Help
	Domaintuser name3 Security Wanning: Rylogong in to this web page, you confirm that this compater compiles with your organization's security policy Sign in	
	To protect against invalidation of the second system (D to protect against invalidation second second second second after a period of inactivity if your second second second refresh your browser and sign in again.	A.
	Windowsteiner 2012 122 M	Kersoft



 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.



 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.

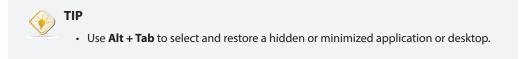
Work Resources Remotagep and Desktop Connection		12 BD Web Access
Current folder: /		5 Sign out
•••	Current	folder: /
E Windows Server 2012 R2	Calculator	Paint
	-	

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.

🛬 Windov	vs Security			
Enter your credentials				
These credentials will be used to connect to VRDWEB12R2.RDWEB.POC:3389.				
Username:	*			
Password:				
Domain:				
	OK Cancel			

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

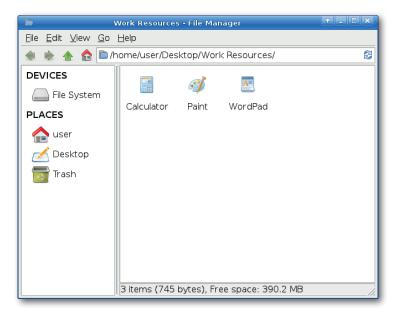


Connection Type: Web Feed

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

Image: Constrained and the second a	
START 🔏 🛙 [Terminal]	

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

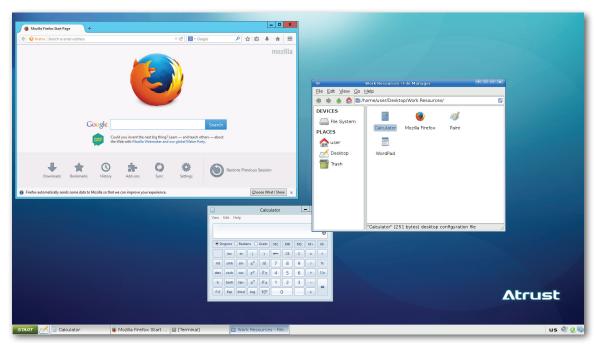


3. Double-click to select the desired application.

4. A window appears prompting for credentials.



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

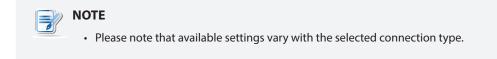


Remote Application Examples

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.



Settings for the Connection Type of Remote Desktop

- 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

Server Settings					
Item	Description				
Session Name	Type in the name for Remote Desktop sessions.				
Computer	Type in the computer name or IP address of the server where to deliver a Remote Desktop session.				
	This table only provides Desktop is selected. Three connection types	descriptions for available settings when Remote are available:			
	Option Description				
Connection Type	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.			
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.				

	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 .				
Server Authentication	Option	Description			
	Connect and don't warn me	Connects anyway without any warning.			
	Warn me	Warns and allows users to choose whether to connect or not.			
	Do not connect	Disallows the connection.			
Login Settings	NOTE: To import certificates for remote computers, please refer to section "3.2.16 Importing Certificates for Remote Computers" on page 73.				
Item	Description				
Username	Type in the user/account name used for authentication.				
Password	Type in the password o	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.				
Use Smart Card Login	Check to enable logon	with a smart card.			

Common Settings			
Item	Description		
	mt182L	is started up (Auto There are three sin	nilar but different modes for your mt182L and only one ct if all are enabled. Three modes and the order of
	No.	Mode	Description
			The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.
		A	Available actions include:
	1	Appliance	Re-launching a new session
			Restarting the thin client
			• Turning off the thin client
Autostart When Startup			The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.
			Available actions include:
	2	Autostart	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 Autosta	t mode, ensure that the Appliance mode is disabled.
On Application Exit	availab		Remote Desktop session is ended. Five options are start Application, Force-Restart Application,
	Optio	n	Description
	Do No	othing	Returns to the mt182L local Linux desktop.
	Resta	rt Application	Opens a Remote Desktop session again.
	Force-	Restart Application	Opens a Remote Desktop session again and skips any messages in-between.
	Reboo	ot	Restarts your mt182L.

Options Sub-tab

Programs			
Item	Description		
Start the following program on connection	 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. 		
Start in the following folder	 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. 		
Program path and file name	Type in the name of the connection is enable Remote APP Windows Media Player Adobe Reader X Adobe Reader X NOTE: the file extense	Format Example C:\Programs Files (x86)\Windows Media Player\wmplayer.exe C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32.exe C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32	
Window Settings			
Item	Description		
Color Depth	Description 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.		

	Desktop session.	own menu to select the desired display resolution on a Remote . Four options are available: Fullscreen, Large Window , w, and Small Window .		
	Option	Description		
	Fullscreen	Opens a Remote Desktop session in full screen with the same display resolution as the local desktop.		
Resolution	Large Window	Opens a Remote Desktop session in a large display resolution.		
	Medium Window	Opens a Remote Desktop session in a medium display resolution.		
	Small Window	Opens a Remote Desktop session in a small display resolution.		
		ure the display resolution of the local desktop, please refer to 3.3.3 Configuring Display Settings" on page 80.		
Use Toolbar	Remote Desktop	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.		
	Δι	trust 🖡 🛛 🕞 🗞		
Fullscreen Toggle		Click the drop-down menu to allow/disallow fullscreen toggle for a remote session by Ctrl + Alt + Enter .		
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.		
	Click the drop-do	own menu to disable/enable RemoteFX.		
		NOTE: Windows [®] RemoteFX [™] is a technology that offers a rich user experience over a network for remote desktop users.		
Use RemoteFX	mt182L t detailed	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.		
GFX Preferred Mode	Click the drop-down menu to select preferred graphics compression meth RemoteFX, Progressive RemoteFX, or H.264/AVC 444.			
	NOTE: This setti	ng item is shown only when Use RemoteFX is enabled.		
Use Bulk Compression		Click to enable/disable the bulk compression for the data traffic between the server and client.		

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		
	Click the drop-down menu to disable/enable multimedia redirection.		
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.		
	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.		
USB Storage Mapping	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.		
	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.		
Printer Mapping	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.		
	Click the drop-down menu to enable/disable serial port mapping.		
Serial Port Mapping	When Enable is selected, users can access a serial device, such as a barcode scanner, in a Remote Desktop session.		

	1		
	Click the drop-down menu t	o enable/disable parallel port mapping.	
Parallel Port Mapping	When Enable is selected, users can access a parallel device, such as a printer or scanner, in a Remote Desktop session.		
	Click the drop-down menu t	o enable/disable smart card mapping.	
Smart Card Mapping	When Enable is selected, us reader in a Remote Desktop	sers can access smart cards through a smart card session.	
Load Balance Info	Use this field to specify the collection if needed.	value for the desired Remote Desktop Services	
	Click the drop-down menu t	o enable/disable connection status check.	
Server Status Check	status check. Enabli	yed for remote sessions may not support connection ng this feature would cause remote sessions s 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		
		o configure the audio playback setting in a Remote ons are available: Play on this computer, Play on o not play.	
	Option	Description	
Remote Audio Playback	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.	

	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 .		
	Option	Description	
Remote Audio Recording	Recording from this computer	Allows audio recording in a Remote Desktop session using locally attached audio devices.	
	Do not record	Disables audio recording in a Remote Desktop session using locally attached audio devices.	
RemoteFX USB Redirection	Settings		
Item		Description	
Use RemoteFX USB Redirection	 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 ba Remote Desktop service not to session based one. For more informatic 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: 		

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

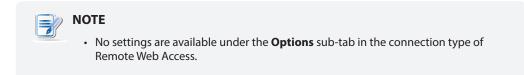


General Sub-tab

Server Settings			
Item	Description		
Session Name	Type in the name for Remote Web Access sessions.		
Connection URL	Type in the URL of the server where to deliver Remote Web Access sessions.		
	This table only provides descriptions for available settings when Remote Web Access is selected. Three connection types are available: Option Description		
Connection Type	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.	

Common Settings					
Item	Description				
	mt1821	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:			
	No.	Mode	Description		
			The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.		
	1	Appliance	Available actions include:		
			 Re-launching a new session 		
			Restarting the thin client		
			• Turning off the thin client		
Autostart When Startup			The client will start up directly with the desired Microsoft RDP session and perform the configured action after exiting the session.		
			Available actions include:		
	2	Autostart	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:	NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.			
	are ava	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 .			
On Application Exit	Optic	on	Description		
	Do No	othing	Returns to the mt182L local Linux desktop.		
	Resta	rt Application	Opens a Remote Web Access session again.		
	Force	-Restart Application	Opens a Remote Web Access session again and skips any messages in-between.		
	Reboo	ot	Restarts your mt182L.		
	Shuto	lown	Turns off your mt182L.		

Options Sub-tab



RD Gateway Sub-tab



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 We	eb Feed sessions.	
Web Feed URL	Type in the URL of the s	erver where to deliver Web Feed sessions.	
	This table only provides descriptions for available settings when Web Feed is selected. Three connection types are available:		
	Option	Description	
Connection Type	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		
	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 .		
Color Depth	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.		
	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.		
Use RemoteFX	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		
	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.		
USB Storage Mapping	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.		
	Click the drop-down menu to enable/disable printer mapping.		
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.		

	Click the drop-down menu to	o enable/disable serial port mapping.	
Serial Port Mapping	When Enable is selected, users can access a serial device, such as a barcode scanner, in a Remote Desktop session.		
	Click the drop-down menu to enable/disable parallel port mapping.		
Parallel Port Mapping	When Enable is selected, us scanner, in a Remote Deskto	sers can access a parallel device, such as a printer or op session.	
	Click the drop-down menu to enable/disable smart card mapping.		
Smart Card Mapping	When Enable is selected, us reader in a Remote Desktop	sers can access smart cards through a smart card session.	
Load Balance Info	Use this field to specify the collection if needed.	value for the desired Remote Desktop Services	
	Click the drop-down menu to	o enable/disable connection status check.	
Server 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	
	Click the drop-down menu to Desktop session. Three option remote computer, and Do	o configure the audio playback setting in a Remote ons are available: Play on this computer, Play on not play .	
	Option	Description	
Remote Audio Playback	Play on this computer	Allows audio playback in a Remote Desktop session using locally attached audio devices.	
		Allows audio playback in a Remote Desktop session using audio devices attached to the	
	Play on remote computer	remote computer.	

	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 .			
	Option	Description		
Remote Audio Recording	Recording from this computer	Allows audio recording in a Remote Desktop session using locally attached audio devices.		
	Do not record	Disables audio recording in a Remote Desktop session using locally attached audio devices.		
RemoteFX USB Redirection	Settings			
Item		Description		
Use RemoteFX USB Redirection	 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 in server-hosted virtual machines (with guest operating systems). NOTE: RemoteFX USB Redirection is only applicable to the virtual machine Remote Desktop service not to session based one. For more inform please visit Microsoft Support website at support.microsoft.com. On the client side, please do the following to enable locally attached USB of in a virtual machine based desktop: Ensure that the desired USB device has been connected to your mt Ensure that RemoteFX is enabled on your mt182L (see "Use Remote on page 148). Click to check Use RemoteFX USB Redirection. A new checkbox appears with the required device driver. Check to e the driver. Click Save to apply. NOTE: You also need to configure the host server and its guest OSs to ena RemoteFX USB Redirection in a Remote Desktop session. For instruot on server-side configuration, please visit Microsoft Support website support.microsoft.com. 			

RD Gateway Sub-tab



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.



• 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



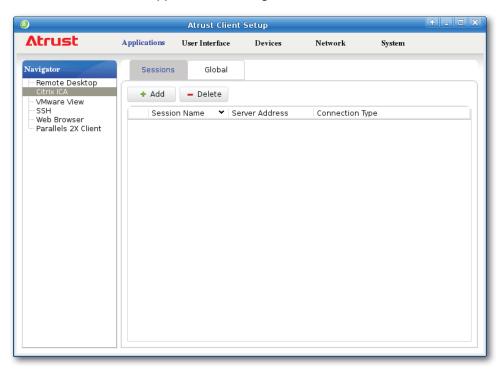
• You can refer to the following table for Citrix products and recommended connection types:

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.





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.

3		Atrust Client	t Setup			+ _ O X
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	General Server Setti Session Na Connection Server Add	Options ngs me: n Type: ress: trix sessions are		* Web Logi *		
	Autostart V On Applicat	Vhen Startup: ion Exit: Cancel		No Do Nothi	ng	

ΝΟΤΕ

• 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 <i>sub-path</i> 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.



• 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.

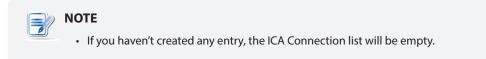
Connection Type: StoreFront

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

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

0		Atrust Client	Setup			+ - O X
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Sessions + Add Sessio	– Delete	rver Address	Connection T	/pe	

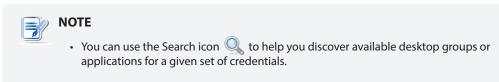


3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

٨		Atrust Client	Setup			↑ _ O X
Atrust	Applications	User Interface	Devices	Netwo	ork System	
Navigator	General	Options				
Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Server Setti Session Na Connection Server Addi Store Name Usernam Password Domain:	me: Type: ress: a: e:		* [[* [[[[StoreFront	
	Access T	iype: Group / Applicati	on:	L Q. [Specified	
	Common Se	ttings				
	Autostart W	/hen Startup:		[No	- 6
	On Applicat	ion Exit:		[Do Nothing	
	Save	Cancel]

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.



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



• 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.

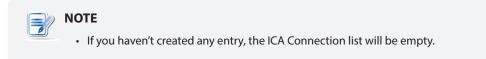
Connection Type: VDI-in-a-Box

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

> NO		for Citrix products and recommended
	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.

0		Atrust Client	Setup			+ - O X
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Sessions + Add Sessio	– Delete	rver Address	Connection T	/pe	

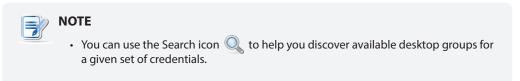


3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

٥		Atrust Client	Setup			↑ _ □
Λtrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options				
Remote Desktop Citrix ICA	Server Sett	ings ———				
VMware View SSH	Session Na	ame:		*		Ê
Web Browser Parallels 2X Client	Connection	n Type:		VDI-in-a	а-Вох	- 6
Parallels 2X Client	Server Add	lress:		*		Ê
	Usernar	ne:				6
	Passwor	rd:				É
	Domain					6
	Desktop	Group:	C	*		Ê
	Common Se	ettings —				
	Autostart	When Startup:		No		- 6
	On Applica	tion Exit:		Do Not	hing	
	Save	Cancel				

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.



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



• 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.

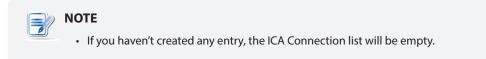
Connection Type: XenDesktop

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

) NO		for Citrix products and recommended
	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.

0		Atrust Client	Setup			+ - O X
Δtrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Sessions + Add Sessio	– Delete	rver Address	Connection T	/pe	

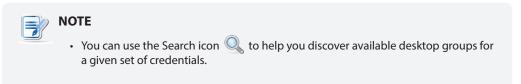


3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.

3		Atrust Client	Setup			Φ - Ο Σ
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Remote Desktop Citrix ICA - VMware View - SSH - Web Browser - Parallels 2X Client	General Server Sett Session Na Connection Server Ado Usernar Passwor	ame: n Type: Iress: ne:	* XenDesktop *			
	Domain: Desktop) Group:	C	*		
		When Startup:	No Do Nothing			
	Save	Cancel				

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.



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



• 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.

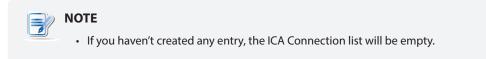
Connection Type: XenApp

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

NO	FE 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.

Applications User Interface Devices Network System Navigator Sessions Global	٨	Atrust Client Setup					↑ _ □ ×
	Atrust	Applications	User Interface	Devices	Network	System	
Citracica VMware View SSH Web Browser Parallels 2X Client Session Name Server Address Connection Type	Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser	Sessions + Add	Global – Delete				



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

D		Atrust Client	Setup			
Atrust	Applications	User Interface	Devices	Network	System	
Tavigator	General	Options				
Remote Desktop Citrix ICA	Server Sett	ings				
VMware View SSH	Session Na	ame:		*		Ê
Web Browser	Connection	n Type:		XenApp		- 6
Parallels 2X Client	Server Add	lress:		*		Ê
	Usernar	ne:				Ê
	Passwor	d:				6
	Domain					Ê
	Applicat	ion Name:	(*		£
	Common Se	ettings				
	Autostart	When Startup:		No		-
	On Applica	tion Exit:		Do Noth	ning	-
	Manual Pa	rameters:				Ê
	Save	Cancel				

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.

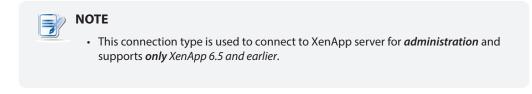
 NOTE You may need to provide the <i>XML port number</i> as well for your server (for example, XA65P.CTX.poc:8080), depending on your server-side content of the server server (for example, XA65P.CTX.poc:8080), depending on your server-side content of the server server	
 NOTE You can use the Search icon Q to help you discover available applingiven set of credentials. 	cations for a

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



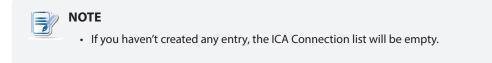
Connection Type: Server Connection

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



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

0		Atrust Client	Setup			+ _ O X
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Remote Desktop Citrix ICA - VMware View - SSH - Web Browser - Parallels 2X Client	Sessions + Add Sessio	Global — Delete n Name ▼ Se	erver Address	Connection '	Type	



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

٩		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	General Server Sett Session N Connectio Server Add Usernat Passwo Domain	ame: n Type: dress: me: rd:		* Serv *	er Connection	
	Server 1	Name:		Q *		£
	Common S	ettings ———				
	Autostart	When Startup:		No		-
	On Applica	ition Exit:		Do N	lothing	E
	Save	Cancel				

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 <i>XML port number</i> 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.



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**.

Applications User Interface Devices Network System Navigator Sessions Global Global	0		Atrust Client	Setup			+ - • ×
Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client Citrix Receiver Version: Use Esc to quit Web Logon: Ves Keyboard Layout Depends on: Local Input Language: Session Reliability. The change to the used Receiver version will affect all sessions. * All current Citrix sessions will be disconnected after switching the Receiver version.	Atrust	Applications	User Interface	Devices	Network	System	
	Navigator - Remote Desktop Citrix ICA - VMware View - SSH - Web Browser	Sessions Common Sec Citrix Recei Use Esc to Keyboard L Keyboard T Input Lang Session Re * The chan * All curren	Global tttings ver Version: quit Web Logon: ayout Depends on ype: uage: liability: uge to the used Rea tt Citrix sessions without the session of th	ceiver version w	13.x Yes Local Default Default Disabled	- 	



- 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:



• 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.

٨		Atrust Client	Setup			↑ - □ >	3
Atrust	Applications	User Interface	Devices	Network	System		
Atrust Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Sessions Common Se Citrix Receit Use Esc to Keyboard L Keyboard T Input Langu Session Re * The chan	Global ttings ver Version: quit Web Logon: ayout Depends or ype: uage: liability: ge to the used Re	n:	13.x Yes Local Default Disablec will affect all sessio			
	 The change to the used Receiver version will affect all sessions. All current Citrix sessions will be disconnected after switching the Receiver Save Cancel 						

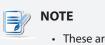
3. Click **Save** to apply.

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.

۵		Atrust Client	Setup				
Atrust	Applications	User Interface	Devices	Network	System		
Atrust Navigator - Remote Desktop Cttrx ICA - VMware View - SSH - Web Browser - Parallels 2X Client	Sessions Common Se Citrix Receiv Use Esc to Keyboard Li Keyboard Ty Input Langu Session Re * The chan	Global ttings ver Version: quit Web Logon: ayout Depends on ype: Jage: Jage: liability: ge to the used Ret	ceiver version w	Network	- 	• • •	



• 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.

Logen Message Preferances	
Welcome Logariti access your applications. User area: Domit: Log the Log the	
<u>citre</u> :	

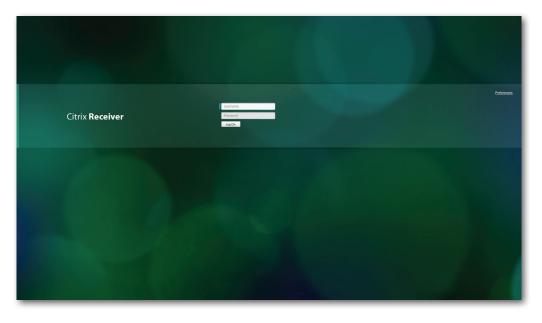
Citrix Logon Screen Example: XenApp 6.0 Fundamentals



Citrix Logon Screen Example: XenApp 6.5 Platinum

Citrix Logon Screen Example: XenDesktop 5.6 Platinum



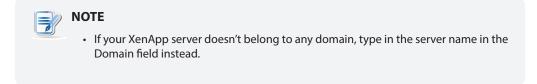


Citrix Logon Screen Example: VDI-in-a-Box

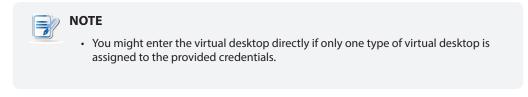
Citrix Logon Screen Example: XenApp and XenDesktop 7.5 Platinum



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



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



Selection Screen Example: XenApp 6.5 Platinum

Search P Logged on as: CTXA1	Settings
Main	Select view: -
Notepad POF Reader X PPT Venere 2007	
Hint: Click Disconnect to pause any running resources started from this computer.	
 CÎTR <u>I</u> X'	

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.

Search	D Logged on as: CTXA1		Settings Log Off - CITRU	K ′
Main A No		1 / 0 1 100% 100%	-	Sign Comment
Constant Look r Peccer Place Deckoo Lookoo Lookoo Feeseo Place Tere a Upoe	👌 Open	×	Acrobat.com Services	rox c r r r r r

Virtual Application Examples

PowerPoint Viewer, Adobe Reader, and Notepad

Virtual Application Examples

Adobe Reader, Mozilla Firefox, and PowerPoint Viewer

Cit	ix Receiver					
			Masila Fierfax Start Page x + Fierdax Start Page x +	∀ C Scople		
	Adde Rader Re Edit View Woodow Help E Decuments @ C @ @ @ @ @ @ @ @ @ @ Adde Rader XI Open & Recent File Open & Recent File M Compute.	lobe Online Services	Congle Subset of the text of text of the text of te	Search S What else can be Web I our global Maker Puny.	mozilla	
	S Aorbail.com	Send and Track Files Online	Peter submitted to Motifie to the two can improve your experience.	ings Nar Recent Places	Documents 🔹 🕲 🗗 🛛	Type
	Consert 1761 to Word Address Vision of Address to Conserve. 2014 States		> Store Film > Store Film		gen [d type: [Asseffact Preestators	, Qom Cancel
			0 2013-2014 Citrix Systems, Inc. All rights reserved. Third Panty Notices			

Virtual Desktop Example

Windows 7 Ultimate

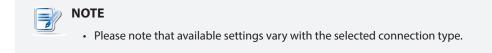


Virtual Desktop Example Windows Server 2008 R2

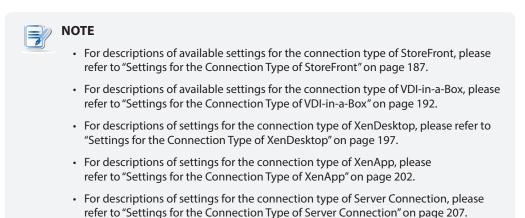


3.6.11 Configuring Advanced ICA Connection Settings

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.



Settings for the Connection Type of Web Logon



Server Settings				
Item	Description			
Session Name	Type in the name	Type in the name of browser sessions for Citrix service access.		
	This table only pr is selected.	ovides descriptions f	or available settings when Web Logon	
	Six connection ty	pes are available:		
	Option	Description		
	Web Logon		virtual desktops and applications ce of a Web browser (Mozilla Firefox).	
	StoreFront	Provides access to virtual desktops and applications through a StoreFront.		
	VDI-in-a-Box	Provides access to	virtual desktops through VDI-in-a-Box.	
	XenDesktop	Provides access to of XenDesktop.	virtual desktops for an earlier version	
Connection Type	XenApp	Provides access to version of XenApp.	virtual applications for an earlier	
	Server Connection	Provides access to servers only).	servers for administration (XenApp	
	Refer to the table	e below for Citrix proc	ducts and recommended connection types: Recommended Connection Type	
	XenApp 6.5 or e	earlier	XenApp / Web Logon	
	XenDesktop 5.6 or earlier		XenDesktop / Web Logon	
	Virtual Apps and (XenApp/XenDe	d Desktops sktop 7.5 or later)	StoreFront / Web Logon	
	VDI-in-a-Box		VDI-in-a-Box / Web Logon	
	are accessible.		of the server through which Citrix services	
	Refer to the table	below for details:		
	Citrix Product	Component to Connect	Connection Address	
	XenApp 6.5 or earlier	Web Interface	IP / URL / FQDN	
Server Address	XenDesktop 5.6 or earlier	Web Interface	IP / URL / FQDN	
	\/:	4	IP / URL / FQDN plus sub-path	
	Virtual Apps and Desktops (XenApp and XenDesktop 7.5 or later)	StoreFront	For example — FQDN: X75.CTX.poc Sub-path: /Citrix/StoreWeb (default) Connection Address: X75.CTX.poc/Citrix/StoreWeb	

	Select	what to do next w	hen all Citrix sessions are closed.
	Optic	on	Description
When all Citrix sessions are	Retur	rn to Web Logon	Stay on the Web Logon screen.
closed	Quit	Web Logon	Exit the Web Logon screen.
	NOTE	If only one virtua option here woul	I application or desktop is opened and then closed, your d apply.
Common Settings	I		
Item	Descr	iption	
			a browser session for Citrix service access automatically L is started up (Autostart mode).
	NOTE		similar but different modes for your mt182L and only one ffect if all are enabled. Three modes and the order of I as follows:
	No.	Mode	Description
			The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.
	1	Appliance	Available actions include:
			 Re-launching a new session
			Restarting the thin client
Autostart When Startup			Turning off the thin client
			The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.
			Available actions include:
	2	Autostart	Returning to the local desktop
			Re-launching a new session
			Restarting the thin client
			• Turning off the thin client
	3	Quick Connection	n The client will enter Atrust Quick Connection screen after system startup.
	NOTE	: To use the Autosi	tart mode, ensure that the Appliance mode is disabled.

		en a browser session for Citrix service access is ended. able: Do Nothing, Restart Application, Reboot , and
	Option	Description
On Application Exit	Do Nothing	Returns to the Local Linux desktop.
	Restart Application	Opens a browser session again for service access.
	Reboot	Restarts your thin client.
	Shutdown	Turns off your thin client.

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				
Printers				
Redirect Connected USB Devices	Please refer to "Advanced Quick Connection Settings for Citrix ICA Sessions" on page 64 for detailed instructions on these similar settings.			
Plugged USB Devices				
Redirection Rules				

Settings for the Connection Type of StoreFront

Difference 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.

Server Settings					
Item	Description				
Session Name	Type in the name for Citrix ICA sessions.				
	This table only provides descriptions for available settings when StoreFront is selected.				
	Six connection ty	pes are available:			
	Option	Description			
	Web Logon		virtual desktops and applications ce of a Web browser (Mozilla Firefox).		
	StoreFront	Provides access to through a StoreFro	virtual desktops and applications nt.		
	VDI-in-a-Box	Provides access to	virtual desktops through VDI-in-a-Box.		
	XenDesktop	Provides access to of XenDesktop.	virtual desktops for an earlier version		
Connection Type	XenApp	Provides access to virtual applications for an earlier version of XenApp.			
	ServerProvides access to servers for administration (XenA servers only).		servers for administration (XenApp		
	Refer to the table	e below for Citrix proc	ducts 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		

Server Address	Type in the IP address / URL / FQDN of the server through which virtual desktops or applications are accessible (where a StoreFront is hosted).					
Store Name	Type in	Type in the store name of your Citrix environment if required.				
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.					
	Click the drop-down menu to select the access type. Two options are available: Specified and All .					
	Optio	n Descri	ption			
Access Type	Speci	fied .	cific desktop/application, or ess shortcuts in a window			
	All	• Acc	ess shortcuts on the desktop			
Desktop Group / Application	Type in in front	the name of the c t of the field to disc	lesktop group / application or use the Search icon 🔍 cover available desktop groups / applications.			
Common Settings						
Item	Descri	ption				
	mt1821	L is started up (Au There are three si mode will take eff	milar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of			
	mt1821	L is started up (Aut There are three si	 costart mode). milar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of as follows: Description 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 			
Autostart When Startup	MOTE:	L is started up (Au There are three si mode will take eff priority are listed Mode	 milar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of as follows: Description 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 			

	Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing, Restart Application, Reboot , and Shutdown .				
	Option	Description			
	Do Nothing	Returns to the Local Linux desktop.			
On Application Exit	Restart Application	Opens an ICA session again.			
	Reboot	Restarts your thin client.			
	Shutdown	Turns off your thin client.			
Prompt for Credentials on Application Restart	This setting item is available only when Restart Application is selected for Or Application Exit . Click to select whether to prompt for credentials or not when an ICA session restarts.				

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			
	Click the drop-down menu to enable/disable the mapping of the local USB drive(s) in a Citrix ICA session.			
Mapping Local USB Storage	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.			
	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.			
Mapping Local Serial Ports	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.			

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.		
Description		
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.		
This item is available only	when Client Rendering is selected.	
When Yes is selected, a lo	cally attached webcam can be used in an ICA session.	
Click to enable/disable H.2 data are sent from the serv	64 compression support on the client, allowing session ver side using H.264 format encoding.	
Check/Uncheck to enable/o was interrupted.	lisable automatic reconnecting after an ICA session	
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.		
Click the drop-down menu	to select the number of retries, ranging from 1 to 10.	
Click the drop-down menu 5 to 60 seconds.	to select the delay time between retries, ranging from	
Check/Uncheck to enable/o	lisable sound in an ICA session.	
	to choose the desired sound quality in an ICA session. : 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.	
	Citrix ICA session. If Yes is sele in launched Citrix ICA session NOTE: To enable locally att Adding a Local Print Click the drop-down menu server. Two options are avai NOTE: The Client Render This item is available only w When Yes is selected, a loc Click to enable/disable H.24 data are sent from the serve Check/Uncheck to enable/of was interrupted. NOTE: Automatic reconnect XenDesktop ICA serve visit Citrix websites Click the drop-down menu Click the drop-down menu Click the drop-down menu 5 to 60 seconds. Check/Uncheck to enable/of Medium Quality Medium Quality	

Enable Audio Input	Check/Uncheck to enable/disable audio input in an ICA session.		
	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 .		
	Option	Description	
Windows Key Combination	On the local computer	Applies to the local desktop only.	
	On the remote server	Applies to the virtual desktop only.	
	In full screen mode only	Applies to the virtual desktop only when the desktop is running in the full-screen mode.	
Connection Dialog Setting	JS		
Item	Description		
Show Remember Field	Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.		
USB Redirection Settings			
Item	Description	Description	
USB Storage			
Printers			
Redirect Connected USB Devices	Please refer to "Advanced Quick Connection Settings for Citrix ICA Sessions" on page 64 for detailed instructions on these similar settings.		
Plugged USB Devices			
Redirection Rules			

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

D 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.

Server Settings			
Item	Description		
Session Name	Type in the name for Citrix ICA sessions.		
	This table only provides descriptions for available settings when VDI-in-a-Box is selected.		
	Six connection types are available:		
	Option	Description	
	Web Logon		virtual desktops and applications ce of a Web browser (Mozilla Firefox).
	StoreFront	Provides access to through a StoreFro	virtual desktops and applications nt.
	VDI-in-a-Box	Provides access to virtual desktops through VDI-in-a-Box.	
	XenDesktop	Provides access to virtual desktops for an earlier version of XenDesktop.	
Connection Type	XenApp	Provides access to virtual applications for an earlier version of XenApp.	
	Server Connection	Provides access to servers for administration (XenApp servers only).	
	Refer to the table below 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

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 ir	the password of th	e user account used for authentication.
Domain	Type ir	the domain of the	server.
Desktop Group / Application	Type ir field to	the name of the de discover available of	esktop group or use the Search icon \mathbb{Q}_{k} in front of the desktop groups.
Common Settings			
Item	Descri	iption	
		whether to open a (L is started up (Auto	Citrix ICA session automatically or not when your ostart mode).
	NOTE:		nilar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of 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
Autostart When Startup		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:
	2		 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 Autosta	rt mode, ensure that the Appliance mode is disabled.

	Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing , Restart Application , Reboot , and Shutdown .		
	Option	Description	
On Analization Fuit	Do Nothing	Returns to the Local Linux desktop.	
On Application Exit	Restart Application	Opens an ICA session again.	
	Reboot	Restarts your thin client.	
	Shutdown	Turns off your thin client.	
Prompt for Credentials on Application Restart	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.		

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 serial-based barcode scanner, and attach it to your mt182L with a seri to-USB adapter, you need to enable this setting in order to use the loc barcode scanner in a virtual desktop.	

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.			
Description			
server. Two options are ava	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.		
This item is available only v	when Client Rendering is selected.		
When Yes is selected, a loo	cally attached webcam can be used in an ICA session.		
	64 compression support on the client, allowing session ver side using H.264 format encoding.		
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.			
Click the drop-down menu	to select the number of retries, ranging from 1 to 10.		
Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.			
Check/Uncheck to enable/disable sound in an ICA session.			
	to choose the desired sound quality in an ICA session. : 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.		
	Citrix ICA session. If Yes is sele in launched Citrix ICA session NOTE: To enable locally att Adding a Local Print Click the drop-down menu server. Two options are avai NOTE: The Client Render This item is available only w When Yes is selected, a loc Click to enable/disable H.20 data are sent from the serve Check/Uncheck to enable/d was interrupted. NOTE: Automatic reconnect XenDesktop ICA serve visit Citrix websites Click the drop-down menu 5 to 60 seconds. Check/Uncheck to enable/d Medium Quality Medium Quality		

Enable Audio Input	Check/Uncheck to enable/disable audio input in an ICA session.		
	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 .		
	Option	Description	
Windows Key Combination	On the local computer	Applies to the local desktop only.	
	On the remote server	Applies to the virtual desktop only.	
	In full screen mode only	Applies to the virtual desktop only when the desktop is running in the full-screen mode.	
Connection Dialog Setting	5		
Item	Description		
Show Remember Field	Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.		
USB Redirection Settings			
Item	Description		
USB Storage			
Printers			
Redirect Connected USB Devices	Please refer to "Advanced Quick Connection Settings for Citrix ICA Sessions" on page 64 for detailed instructions on these similar settings.		
Plugged USB Devices			
Redirection Rules			

Settings for the Connection Type of XenDesktop

D 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.

Server Settings			
Item	Description		
Session Name	Type in the name	Type in the name for Citrix ICA sessions.	
	This table only provides descriptions for available settings when XenDesktop is selected.		
	Six connection types are available:		
	Option	Description	
	Web Logon		virtual desktops and applications ce of a Web browser (Mozilla Firefox).
	StoreFront	Provides access to through a StoreFro	virtual desktops and applications nt.
	VDI-in-a-Box	Provides access to virtual desktops through VDI-in-a-Box.	
	XenDesktop	Provides access to virtual desktops for an earlier version of XenDesktop.	
Connection Type	XenApp	Provides access to virtual applications for an earlier version of XenApp.	
	Server Connection	Provides access to servers for administration (XenApp servers only).	
	Refer to the table below 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

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 ir	Type in the user/account name used for authentication.		
Password	Type ir	Type in the password of the user account used for authentication.		
Domain	Type ir	the domain of the	server.	
Desktop Group		Type in the name of the desktop group or use the Search icon $\mathbb{Q}_{}$ in front of the field to discover available desktop groups.		
Common Settings	1			
Item	Descri	iption		
	mt182	L is started up (Auto There are three sir	nilar but different modes for your mt182L and only one	
		mode will take effe priority are listed a	ect if all are enabled. Three modes and the order of as follows:	
	No.	Mode	Description	
		Appliance	The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.	
	1		Available actions include:	
			 Re-launching a new session 	
			 Restarting the thin client 	
			• Turning off the thin client	
Autostart When Startup			The client will start up directly with the desired Citrix ICA session and perform the configured action after exiting the session.	
			Available actions include:	
	2	Autostart	 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 Autosta	rt mode, ensure that the Appliance mode is disabled.	

	Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing , Restart Application , Reboot , and Shutdown .		
	Option	Description	
	Do Nothing	Returns to the Local Linux desktop.	
On Application Exit	Restart Application	Opens an ICA session again.	
	Reboot	Restarts your thin client.	
	Shutdown	Turns off your thin client.	
Prompt for Credentials on Application Restart	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.		

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 serial-based barcode scanner, and attach it to your mt182L with a seri to-USB adapter, you need to enable this setting in order to use the loc barcode scanner in a virtual desktop.	

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.		
Description		
server. Two options are ava	to select resources rendering on the endpoint or the ilable: Server Rendering and Client Rendering. ing option may not be available on your system.	
This item is available only	when Client Rendering is selected.	
When Yes is selected, a lo	cally attached webcam can be used in an ICA session.	
Click to enable/disable H.2 data are sent from the serv	64 compression support on the client, allowing session ver side using H.264 format encoding.	
Check/Uncheck to enable/o was interrupted.	lisable automatic reconnecting after an ICA session	
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.		
Click the drop-down menu to select the number of retries, ranging from 1 to 10.		
Click the drop-down menu to select the delay time between retries, ranging from 5 to 60 seconds.		
Check/Uncheck to enable/disable sound in an ICA session.		
	to choose the desired sound quality in an ICA session. : 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.	
	Citrix ICA session. If Yes is sele in launched Citrix ICA session NOTE: To enable locally att Adding a Local Print Click the drop-down menu server. Two options are avai NOTE: The Client Render This item is available only w When Yes is selected, a loc Click to enable/disable H.24 data are sent from the serve Check/Uncheck to enable/of was interrupted. NOTE: Automatic reconned XenDesktop ICA servisit Citrix websites Click the drop-down menu 5 to 60 seconds. Click the drop-down menu 5 to 60 seconds. Click the drop-down menu High Quality Medium Quality	

Enable Audio Input	Check/Uncheck to enable/disable audio input in an ICA session.		
	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 .		
Windows Key Combination	Option	Description	
	On the local computer	Applies to the local desktop only.	
	On the remote server	Applies to the virtual desktop only.	
	In full screen mode only	Applies to the virtual desktop only when the desktop is running in the full-screen mode.	
Connection Dialog Setting	JS		
Item	Description		
Show Remember Field	Click the drop-down menu to show or hide the checkbox Remember my credentials on the dialog window.		
USB Redirection Settings			
Item	Description		
USB Storage			
Printers			
Redirect Connected USB Devices	Please refer to "Advanced Quick Connection Settings for Citrix ICA Sessions" on page 64 for detailed instructions on these similar settings.		
Plugged USB Devices			
Redirection Rules			

Settings for the Connection Type of XenApp

D 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.

Server Settings			
Item	Description		
Session Name	Type in the name for Citrix ICA sessions.		
	This table only provides descriptions for available settings when XenApp is selected.		
	Six connection types are available:		
	Option	Description	
	Web Logon		virtual desktops and applications ce of a Web browser (Mozilla Firefox).
	StoreFront	Provides access to virtual desktops and applications through a StoreFront.	
	VDI-in-a-Box	Provides access to virtual desktops through VDI-in-a-Box.	
Connection Type	XenDesktop	Provides access to virtual desktops for an earlier version of XenDesktop.	
	XenApp	Provides access to virtual applications for an earlier version of XenApp.	
	Server Connection	Provides access to servers for administration (XenApp servers only).	
	Refer to the table below for Citrix products and recommended connection types:		
	Citrix Product		Recommended Connection Type
	XenApp 6.5 or e	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

Server Address	Type ir	Type in the IP address / URL / FQDN of a XenApp server.			
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	Type in the domain of the server.			
Application Name		Type in the application name or use the Search icon \mathbb{Q}_{k} in front of the field to discover available applications.			
Common Settings					
Item	Descr	iption			
	mt182	 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		
Autostart When Startup	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.		

	Select what to do when a Citrix ICA session is ended. Four options are available: Do Nothing , Restart Application , Reboot , and Shutdown .		
On Application Exit	Option	Description	
	Do Nothing	Returns to the Local Linux desktop.	
	Restart Application	Opens an ICA session again.	
	Reboot	Restarts your thin client.	
	Shutdown	Turns off your thin client.	
Prompt for Credentials on Application Restart	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.		
Manual Parameters	Type in parameters for extended parameter passing.		

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.

		choose the desired sound quality in an ICA session. 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.
Audio Quality	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.
Enable Audio Input	Check/Uncheck to enable/disa	able audio input in an ICA session.
		select where to apply Windows Key Combinations. On the local computer, On the remote server, ly.
	Option	Description
Windows Key Combination	On the local computer	Applies to the local desktop only.
		Applies to the local desktop only.
	On the remote server	Applies to the virtual desktop only.
	On the remote server In full screen mode only	
		Applies to the virtual desktop only. Applies to the virtual desktop only when the
USB Redirection Settings		Applies to the virtual desktop only. Applies to the virtual desktop only when the
USB Redirection Settings Item		Applies to the virtual desktop only. Applies to the virtual desktop only when the
	In full screen mode only	Applies to the virtual desktop only. Applies to the virtual desktop only when the
Item	In full screen mode only	Applies to the virtual desktop only. Applies to the virtual desktop only when the
Item USB Storage	In full screen mode only Description	Applies to the virtual desktop only. Applies to the virtual desktop only when the desktop is running in the full-screen mode.
Item USB Storage Printers Redirect Connected	In full screen mode only Description Please refer to "Advanced Qu	Applies to the virtual desktop only. Applies to the virtual desktop only when the desktop is running in the full-screen mode.

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

Server Settings						
Item	Description					
Session Name	Type in the name	e for Citrix ICA sessio	ons.			
Connection Type		This table only provides descriptions for available settings when Server Connection is selected.				
	Six connection t	Six connection types are available:				
	Option	Description				
	Web Logon	Provides access to virtual desktops and applications through the interface of a Web browser (Mozilla Firefox).				
	StoreFront	Provides access to virtual desktops and applications through a StoreFront.				
	VDI-in-a-Box	Provides access to virtual desktops through VDI-in-a-Box.				
	XenDesktop	Provides access to of XenDesktop.	virtual desktops for an earlier version			
	XenApp	Provides access to virtual applications for an earlier version of XenApp.				
	Server Connection	Provides access to servers for administration (XenApp servers only).				
	Refer to the tabl	•	ducts and recommended connection types: Recommended Connection Type			
		-				
	XenApp 6.5 or	earlier	XenApp / Web Logon			
	XenDesktop 5.	6 or earlier	XenDesktop / Web Logon			
	Virtual Apps an (XenApp/XenDe	nd Desktops esktop 7.5 or later)	StoreFront / Web Logon			
	VDI-in-a-Box		VDI-in-a-Box / Web Logon			

Server Address			RL / FQDN of the XenApp server.	
Username	Туре і	n the user/account r	name used for authentication.	
Password	Type ii	n the password of th	ne user account used for authentication.	
Domain	Type ii	n the domain of the	server.	
Server Name	Type ii	n the name of the se	erver.	
Common Settings				
Item	Description			
	mt182	L is started up (Aut There are three sir	milar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of	
	No. Mode Description			
Autostart When Startup	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 Autosta	art mode, ensure that the Appliance mode is disabled.	

		en a Citrix ICA session is ended. Four options are available: t Application, Reboot, and Shutdown.		
	Option	Description		
On Application Exit	Do Nothing	Returns to the Local Linux desktop.		
	Restart Application Opens an ICA session again.			
	Reboot	Restarts your thin client.		
	Shutdown	Turns off your thin client.		
Prompt for Credentials on Application Restart		vailable only when Restart Application is selected for On ck to select whether to prompt for credentials or not when ts.		

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.

	Three options are available: F			
	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.		
Audio Quality	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.		
Enable Audio Input	Check/Uncheck to enable/disa	able audio input in an ICA session.		
Enable Audio Input	Click the drop-down menu to	select where to apply Windows Key Combinations. On the local computer, On the remote server,		
Enable Audio Input	Click the drop-down menu to Three options are available: C	select where to apply Windows Key Combinations. On the local computer, On the remote server,		
	Click the drop-down menu to Three options are available: C and In full screen mode on	select where to apply Windows Key Combinations. On the local computer, On the remote server, ly.		
Enable Audio Input Windows Key Combination	Click the drop-down menu to Three options are available: C and In full screen mode on Option	select where to apply Windows Key Combinations. On the local computer, On the remote server, ly. Description		
	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer	select where to apply Windows Key Combinations. On the local computer, On the remote server, ly. Description Applies to the local desktop only.		
	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server	select where to apply Windows Key Combinations. On the local computer, On the remote server, ily. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the		
Windows Key Combination	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server	select where to apply Windows Key Combinations. On the local computer, On the remote server, ily. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the		
Windows Key Combination	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server In full screen mode only	select where to apply Windows Key Combinations. On the local computer, On the remote server, ily. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the		
Windows Key Combination USB Redirection Settings Item USB Storage	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server In full screen mode only	select where to apply Windows Key Combinations. On the local computer, On the remote server, ily. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the		
Windows Key Combination USB Redirection Settings Item	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server In full screen mode only Description	select where to apply Windows Key Combinations. On the local computer, On the remote server, ly. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the desktop is running in the full-screen mode.		
Windows Key Combination USB Redirection Settings Item USB Storage Printers Redirect Connected	Click the drop-down menu to Three options are available: C and In full screen mode on Option On the local computer On the remote server In full screen mode only Description	select where to apply Windows Key Combinations. On the local computer, On the remote server, ly. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the desktop is running in the full-screen mode.		

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.

те
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

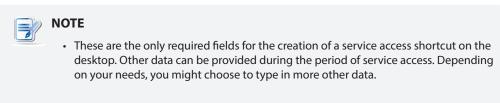
Applications User Interface Derices Network System Navigator + Add - Delete	٨		Atrust Client	t Setup			 ×
Remote Desktop Citrix ICA VMware View SSH Web Browser	Atrust	Applications	User Interface	Devices	Network	System	
	Navigator – Remote Desktop – Citrix ICA – VMware View – SSH – Web Browser	+ Add	– Delete		Network	System	



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

٥		Atrust Clie	nt Setup			•	- • ×
Atrust	Applications	User Interface	Devices	Net	work S	ystem	
Navigator	General	Options	SECUREMATRIX				
Errik ICA VMware View SH Web Browser Parallels 2X Client	Server Setti Session Na Connectior Port: Use Secure Certificate When Conr SSL Proxy: * Example: Login Settin User Name Password: Domain:	ngs me: Server: connection(S: checking mode election Ends: proxy.example gs	SL): : .com:8888	* *	Ves Warn before ccc Return to VMwa		
	Save	Cancel					

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.



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:

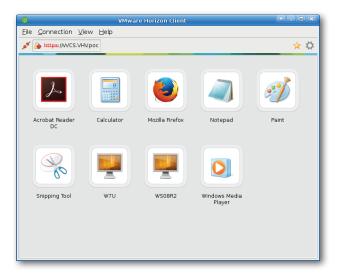
1. Double click the created (customized) access shortcut on the desktop.

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 <i>first</i> .
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 .
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 dropdown menu to select the domain, and then click **OK**.

@	Server Login	A ×
vmware	e Horizon	
<u>S</u> erver: Username:	https://WCS.VHV.poc	
<u>P</u> assword:		
<u>D</u> omain:	VHV	-
	<u>C</u> ancel	<u>o</u> k

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 Applie recall the Desktop and Application list. 	ication List on the top tool bar to
Elie Connection View Connect USB Device Disconnect from Server Return to Desktop and Application List Preferences Quit	▼ Help ▼ _ O X
♦ Click View on the top tool bar to switch to	a virtual desktop or application.
Elle Connection View Help (Windowed Euli Screen - All Resize Show Favorites Adobe Acrobat f Firefox Windows Calcul Windows Media	Reader DC

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 VMwa	are View or Horizon View sessions.			
	Type in the computer nam	e or IP address of the View Connection Server.			
Connection Server	NOTE: For more information on View Connection Server, please visit VMware website at www.vmware.com.				
Port	Type in the port number us To use the default value, s	sed to communicate with the View Connection Server. imply 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 .				
	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			
When Connection Ends	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 Q to help you discover available desktops or applications for a given set of credentials.				

Ture	Click the drop-down menu to select the correct type. NOTE: Select Desktop for a desktop name given in the previous setting				
Туре	Application for an application name.				
	Click the drop- virtual desktop	-down menu to select whether to verify the entitlement to the or application provided in the previous setting item:			
	Option	Description			
Verify before Access	Yes	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.			
	No	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.			
Remember Credentials for the next login	Click the drop-	-down menu to select whether to remember the logon credentials.			
		-down menu to select the desired display protocol. Three options Manual, Microsoft RDP, and PCoIP.			
	Option	Description			
Preferred Display Protocol	Manual	Manually select the desired display protocol.			
	Microsoft RD	P Use Microsoft RDP as the display protocol.			
	PCoIP	Use VMware PCoIP as the display protocol.			
Common Settings	T				
Item	Description				
		${f No}$ to allow or disallow the Non-Interactive mode. The default is to nteractive mode.			
	Option	Description			
Non-Interactive Mode	Yes	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.			
	No	The Interactive mode is used. Users are allowed to re-select different settings even if the settings have been specified in View connection settings.			

.....

	not wh	 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: 			
	No.	No. Mode Description			
			The client will start up directly with the desired VMware View session and perform the configured action after exiting the session.		
	1	Appliance	Available actions include:		
		Аррпансе	Re-launching a new session		
			Restarting the thin client		
			• Turning off the thin client		
Autostart When Startup			The client will start up directly with the desired VMware View or Horizon View session and perform the configured action after exiting the session.		
	2	Autostart	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 Autos	tart mode, ensure that the Appliance mode is disabled.		
	Four o		a VMware View or Horizon View session is ended. e: Do Nothing, Restart Application, Reboot ,		
On Application Exit	Optio	on	Description		
	Do N	othing	Returns to the local desktop.		
	Resta	art Application	Opens a VMware View or Horizon View session again.		
	Rebo	ot	Restarts your thin client.		
	Shute	down	Turns off your thin client.		

Options Sub-tab

Window Settings							
Item	Description						
		wn menu to select the desired display size of a View session. e available: Full Screen, Large Window , and Small Window .					
	Option	Description					
Resolution	Full Screen	Opens the selected View session in full screen.					
	Large Window	Opens the selected View session in a large window.					
	Small Window	Opens the selected View session in a small window.					
Window Mode		wn menu to select the window mode. Two options are available: \pmb{w} and Seamless Window .					
Use Toolbar	Click the drop-do	wn menu to select if the Toolbar is accessible in a session.					
USB Redirection Settings							
Item	Description						
Mass Storage							
Smart Card							
Human Interface Device		dvanced Quick Connection Settings for VMware View Sessions"					
Printer		on page 66 for detailed instructions on these similar settings.					
Plugged USB Devices							
Redirection Rules							
Connection Settings							
Item	Description						
	Click to enable/d	isable printer mapping for VMware View connections.					
Printer Mapping		NOTE: You need to add a local or network printer for your mt182L first, and the enable this feature here to use that mapped printer in a virtual desktop session.					
	thin clien	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.					
	to a virtu	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).					

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).

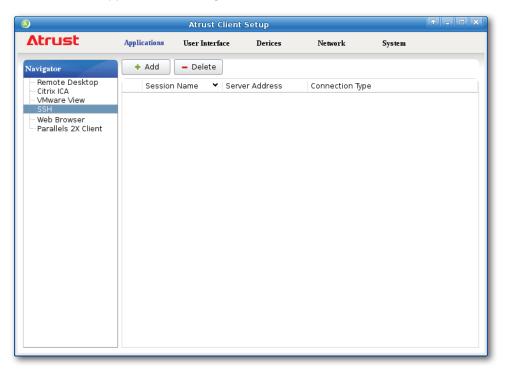


• For details, please refer to "A.3 Using SECUREMATRIX Authentication for VMware Connections" on page 252.

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.





• 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.

Applications User Interface Devices Network System Navigator General Server Settings •	0		Atrust Client	Setup			↑ - □ ×
Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client Port:	Atrust	Applications	User Interface	Devices	Network	System	
Save Cancel	- Remote Desktop - Citrix ICA - VMware View SSH - Web Browser	Server Sett Session Na Connection Port: Username	ame: n Server: n Type: :		* SSH 		

- 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.

٨		Atrust Cl	ient Setup			↑ - □ ×
Atrust	Applications	User Interfac	e Devices	Network	System	
Navigator Remote Desktop Citrix ICA VMware View SSH SDF Web Browser Parallels 2X Client	+ Add Session		Server Address bbs.iscabbs.com sdf.org	Connection Type Telnet SSH		

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

		Terminal	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o	<u>H</u> elp		
Welcome to the SDF Publi You are the 11st guest t		UNIX System - Est. 1987 gged in on 02-Jul-14 03:23	:14.
Are you using Windows 2M	or XP?	(Y/N) NO	
Please press your BACKSF	ACE key:		
Would you like to view t		book? (y/n) YES	
[30-Jun-14 20:12:16 % full time	new	d1]
[01-Jul-14 00:37:45 % Whatever	new	Daniel D]
[01-Jul-14 01:45:32 % india ftw	new	shared4you	india]
[01-Jul-14 14:21:48 %	new	nemysis	Switzerland]
		Girish	Bangalore] •

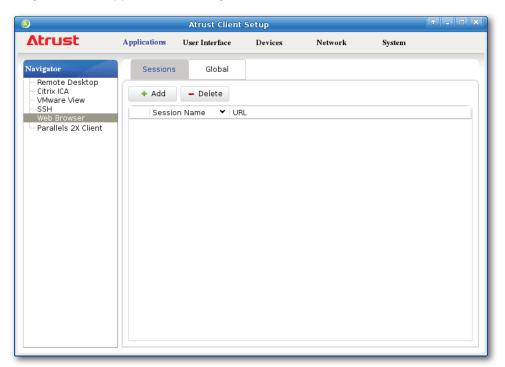
Example: Telnet Session

Terminal	+ - • ×
<u>E</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
DOC (Dave's Own version of Citadel) Version 1.7	
Welcome to the ISCA BBS.	
Login as 'Guest' to just look around, or 'New' to create a new account. Name: Guest	
Iowa Student Computer Association BBS.	
Welcome to ISCA BBS!	
As a Guest there are a few simple things to remember:	
 To see the commands available to you, type <? > To leave ISCABBS, type <l></l> To read about ISCABBS in depth, type <h> to enter the help system from which you may access the topics listed</h> 	
 More commands will be available once you start your own account on ISCABBS If you decide to create your own account here, you might want to keep the following in mind. 	•

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.





• 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.

0		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator - Remote Desktop - Citrix ICA - VMware View - SSH Web Browser - Parallels 2X Client	General Basic Settin Session Na Initial Page	ame:		* [
	Common Se Autostart V	When Startup:		No		T E

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.

a		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator Remote Desktop Citrik ICA VMware View SSH Web Browser Grail Parallels 2X Client	Sessions + Add	Global — Delete n Name 💙 UR			System	

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

Gmail - Mozilla Firefox					4		
G Gmail × •							
🛞 🗟 https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail 🕶 🕑 🛛 Q. Search	5	1		+	A	9	≡
Google							
One account. All of Google.							
Sign in to continue to Gmail							
Enter your email Nex Find my account Create account							
One Google Account for everything Google							
G M 🗷 🖬 🛆 💠 🕨 🌚							
About Goagle Privacy Terms Help	Ð	Eng	lish (Ur	nited S	itates)		

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

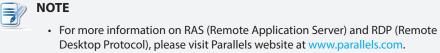
Common Settings					
Item	Descr	Description			
Session Name	Type ir	n the name for brow	ser sessions.		
Initial Page	Type ir	n the URL of the We	b page.		
Common Settings					
Item	Descr	iption			
	mt182	L is started up (Auto	nilar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of		
Autostart When Startup	1	Appliance	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		
	2	Autostart	The client will start up directly with the desired browser session.		
	3	Quick Connection	The default. The client will enter Atrust Quick Connection screen after system startup.		
	NOTE:	To use the Autosta	rt mode, ensure that the Appliance mode is disabled.		

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.



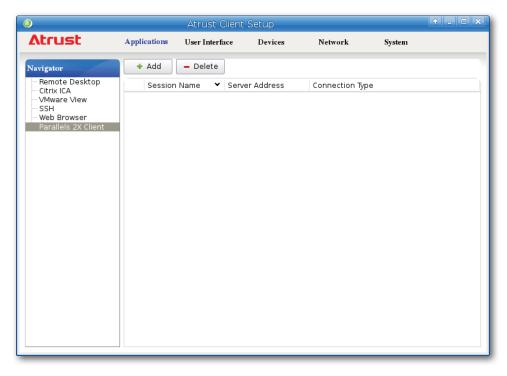
Two connection types are available:

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.





• 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.

٨		Atrust Client	Setup			↑ _ □ ×
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options				
Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Server Setti Session Na Primary Set Secondary Connection Port: Login Settin Username: Password: Domain: Common Set Autostart M	ime: ver: Server: Mode: mgs ttings vhen Startup:		* Parallel Gatewa * 80 No		
	Save	Cancel]

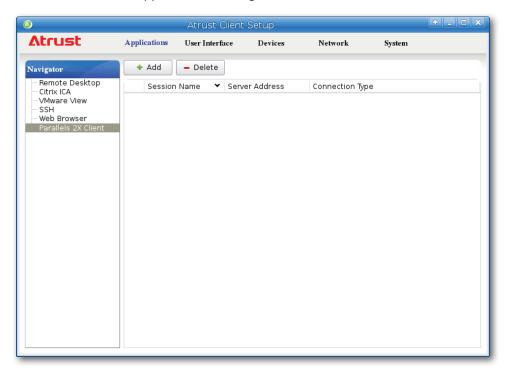
- 4. On **General** sub-tab, ensure that **Parallels Remote Application Server** is selected for the connection type, type in the session name and the primary server address under the Server Settings section.
- 5. Click Save to confirm.
- 6. The new entry is added to the RAS / RDP Connection list and the access shortcuts are automatically created on the local desktop and START menu.

0	Atrus	st Client Setup		+ _ O X
Atrust	Applications User Int	terface Devices	Network	System
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client P2X-RAS-G	Add Dele Session Name P2X-RAS-G	te Server Address 192.168.0.10	Connection Type Parallels Remote	e Application Server

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.





• 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.

٩		Atrust Client	Setup			↑ _ □ X
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options				
Remote Desktop Citrix ICA VMware View SSH Web Browser Parallels 2X Client	Server Sett Session Na Primary Se Connection Network Le Port: Login Settin Username: Password: Domain:	ime: rver: n Type: ivel Authentication igs	1:	*	ard RDP	
	Common Se	ttings Vhen Startup:		No		E
	On Applica			Do Not	hing	
	Save	Cancel				

- 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.

٥	Atrust C	Client Setup		
Atrust AF	pplications User Interfa	nce Devices	Network	System
Navigator Remote Desktop Citrix ICA VMware View SSH Web Browser - Parallels 2X Client P2X-RDP-G	 Add – Delete Session Name ▼ P2X-RDP-G 	Server Address 192.168.0.11	Connection Type Standard RDP	

3.6.21 Accessing Remote Desktops or Applications

Connection Type: Parallels Remote Application Server

To access remote desktops or applications, please do the following:

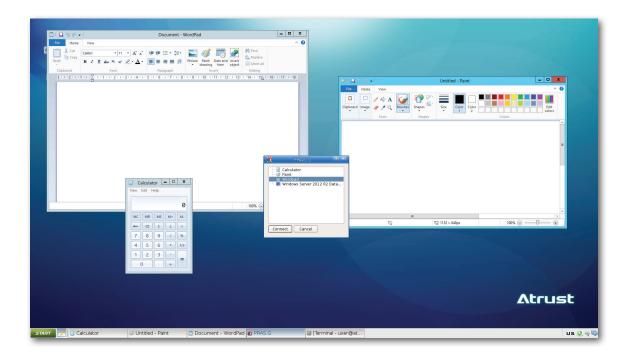
- 1. Double click the created shortcut on the desktop.
- 2. On the opened window, provide your credentials as required, and then click OK.

	Authentication
User	*
Password	*
Domain	
	OK Cancel

3. A window appears with available applications and desktops.

🗊 P2X-RAS-G 🔹 🗙
Calculator Paint Wordpad Windows Server 2012 R2 Data
Connect Cancel

- 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.



Reych Bin	
	Windows Server 2012 R2
	Activate Windows Go to System in Control Planet to activate Windows. Windows Server 2012 R2 Datacenter
- 2	8 10 10 10 10 10 10 10 10 10 10 10 10 10

NOTEThe desktop will be displayed in full screen.

Connection Type: Standard RDP

To access remote desktops, please do the following:

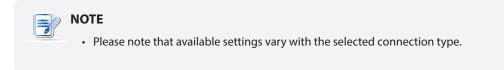
- 1. Double click the created shortcut on the desktop.
- 2. On the opened window, provide your credentials as required, and then click OK.

	Authentication	↑ ×
User	*	
Password	*	
Domain		
		OK Cancel

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.



Settings for the Connection Type of Parallels Remote Application Server



• 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

Server Settings		
Item	Description	
Session Name	Type in the name for RAS (Remote Application Server) sessions.	
Primary Server	Type in the computer name or IP address of the server through which to deliver an RAS session.	
Secondary Server	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.	
	This table only provides descriptions for available settings when Parallels Remote Application Server is selected. Two connection types are available:	
	Option	Description
Connection Type	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.

	Click the drop-down n are available:	Click the drop-down menu to select the desired connection mode. Four options are available:		
	Option	Description		
Connection Mode		Connected with the RAS (Remote Application Server) Secure Client Gateway and data tunneled through the first available connection.		
	Gateway Mode	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.		
	Direct Mode	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.		
	Direct SSL Mode	NOTE: This is best when the client and the server are on the same network and high security safeguards are required.		
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	Description		
Username	Type in the user/acco	Type in the user/account name used for authentication.		
Password	Type in the password	Type in the password of the user account used for authentication.		
	Type in the domain of	Type in the domain of the server.		
Domain	database and	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.		

Common Settings			
Item	Description		
	started	up (Autostart mod There are three sin	nilar but different modes for your mt182L and only one ect if all are enabled. Three modes and the order of
	No.	Mode	Description
			The client will start up directly with the desired RAS session and perform the configured action after exiting the session.
	1	Appliance	Available actions include:
			 Re-launching a new session
			 Restarting the thin client
			• Turning off the thin client
Autostart When Startup	2	Autostart	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
	3	Quick Connection	The default. The client will enter Atrust Quick Connection screen after system startup.
	NOTE:	To use the Autosta	rt mode, ensure that the Appliance mode is disabled.
			Parallel 2X session is ended. Four options are available: blication, Reboot, and Shutdown.
	Optio	on	Description
On Application Exit	Do No	othing	Not to do anything.
	Resta	rt Application	Launches an RAS session again.
	Reboo	ot	Restarts your mt182L.
	Shuto	lown	Turns off your mt182L.

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	Check to show window contents while dragging a window.	
dragging		
dragging Menu and window animation	Check to show menu and window animation.	

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 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. 		
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 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.		
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 RAS 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 RAS session.		
Clipboard Mapping	Click the drop-down menu to enable/disable Clipboard mapping.		
Local Resources Settings	<u> </u>		
Item	Description		
	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 .		
	Option	Description	
Remote Audio Playback	Play on this computer	Allows audio playback in an RAS session using locally attached audio devices.	
	Do not play	Disables audio playback in an RAS session using locally attached audio devices.	
	Play on remote computer	Allows audio playback in an RAS session using audio devices attached to the remote computer.	

	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 .		
Remote Audio Recording	Option	Description	
	Recording from this computer	Allows audio recording in an RAS session using locally attached audio devices.	
	Do not record Disables audio recording in an RAS session using locally attached audio devices.		
		o select where to apply Windows key combinations. On the local computer, On the remote server, nly. Description	
Windows key combination	Three options are available: and In full screen mode o	On the local computer, On the remote server, nly.	
Windows key combination	Three options are available: and In full screen mode of Option	On the local computer, On the remote server, nly. Description	
Windows key combination	Three options are available: and In full screen mode of Option On the local computer	On the local computer, On the remote server, nly. Description Applies to the local desktop only.	
	Three options are available: and In full screen mode on Option On the local computer On the remote server	On the local computer, On the remote server, nly. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the	
Windows key combination Proxy Settings	Three options are available: and In full screen mode on Option On the local computer On the remote server	On the local computer, On the remote server, nly. Description Applies to the local desktop only. Applies to the virtual desktop only. Applies to the virtual desktop only when the	

Item	Description
Use Proxy Server	Check this item if a proxy server is used and then specify the details.
Ргоху Туре	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.
Proxy Host	Specify the IP address of the proxy server.
Proxy Port	Specify the port used for proxy service.
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.

Settings for the Connection Type of Standard RDP



General Sub-tab

Server Settings						
Item	Description					
Session Name	Type in the name for RI	DP sessions.				
Primary Server	Type in the computer n an RDP session.	ame or IP address of the server through which to deliver				
	This table only provides is selected.	s descriptions for available settings when Standard RDP				
	Two connection types a	re available:				
	Option	Description				
Connection Type	Parallels Remote Application Server	Select to access remote desktops and applications via Parallels Remote Application Server.				
	Standard RDPSelect 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.					
	Type in the domain of t	he server.				
Domain	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.					

Common Settings						
Item	Description					
	started	l up (Autostart mode There are three sin	, nilar but different modes for your mt182L and only one ct if all are enabled. Three modes and the order of			
	No.	Mode	Description			
			The client will start up directly with the desired Remote Desktop session and perform the configured action after exiting the session.			
	1	Appliance	Available actions include:			
			 Re-launching a new session 			
			 Restarting the thin client 			
Autoctort Miken Charter			• Turning off the thin client			
Autostart When Startup			The client will start up directly with the desired RDP session and perform the configured action after exiting the session. Available actions include:			
	2	Autostart				
		Autostart	Not to do anything Do lounghing a new cossion			
			 Re-launching a new session Restarting the thin client			
			Turning off the thin client			
	3	Quick Connection	The default. The client will enter Atrust Quick Connection screen after system startup.			
	NOTE: To use the Autostart mode, ensure that the Appliance mode is disabled.					
		Select what to do when an RDP session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown .				
	Optio	on	Description			
On Application Exit	Do No	othing	Not to do anything.			
	Resta	rt Application	Launches an RDP session again.			
	Rebo	ot	Restarts your mt182L.			
	Shuto	down	Turns off your mt182L.			

Options Sub-tab

Window Settings						
Item	Description					
Color Depth	 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. 					
		wn menu to select the desired display resolution on an RDP ions are available: Fullscreen, Large Window, Medium mall Window.				
	Option	Description				
	Fullscreen	Opens an RDP session in full screen with the same display resolution as the local desktop.				
Resolution	Large Window	Opens an RDP session in a large display resolution.				
	Medium Window	Opens an RDP session in a medium display resolution.				
	Small Window	Opens an RDP session in a small display resolution.				
		ure the display resolution of the local desktop, please refer to 3.3.3 Configuring Display Settings" on page 80.				
		wn menu to set graphics acceleration. Four options are Basic, RemoteFX , and RemoteFX Adaptive .				
Graphics Acceleration	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.				
Connection Settings					
Item	Description				
USB Storage Mapping Printer 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. 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. Click the dram down many to enable (disable carial part mapping)				
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.				

Local Resources Settings						
Item	Description					
	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 .					
	Option	Description				
Remote Audio Playback	Play on this computer	Allows audio playback in an RDP session using locally attached audio devices.				
	Do not play	Disables audio playback in an RDP session using locally attached audio devices.				
	Play on remote computer	Allows audio playback in an RDP session using audio devices attached to the remote computer.				
		o configure the audio playback setting in a Remote s are available: Recording from this computer				
	Option	Description				
Remote Audio Recording	Recording from this computer	Allows audio recording in a Remote Desktop session using locally attached audio devices.				
	Do not record	Disables audio recording in a Remote Desktop session using locally attached audio devices.				
	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 .					
	Option	Description				
Windows key combination	On the local computer	Applies to the local desktop only.				
	On the remote server	Applies to the virtual desktop only.				
	In full screen mode only	Applies to the virtual desktop only when the desktop is running in the full-screen mode.				
Duran Catting a						
Proxy Settings Item	Description					
Use Proxy Server	Charly this item if a provy conver is used and then energify the details					
USE FIUXY SELVEL	Check this item if a proxy server is used and then specify the details.					
Proxy Type	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.					
Proxy Host	Specify the IP address of the	e proxy server.				
	Specify the port used for proxy service.					

E.

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 Using SECUREMATRIX authentication Changing Your Password Pattern	252 254 257
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:



- 1. Restart your mt182L.
- 1. During the POST (Power-on Self-Test) period, press **Esc** on the keyboard to enter Atrust Thin Client Menu.

Atrust Thin Client Menu
Normal Mode
Safe Mode
Reset Mode
Firmware update
Reboot
Shutdown



....

- 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	lode 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.

- 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:



 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:



- 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.

٥		Atrust Clie	nt Setup				•	
Atrust	Applications	User Interface	Devices	Net	work	System		
Navigator Permote Desktop Ctrix ICA Ctrix ICA VMware View VHV6 SSH	General Server Settin Session Na Connection Port: Use Secure Certificate of Login Settin User Name: Password: Domain: Desktop / A Preferred D	Options me: Server: Connection(SS checking mode gs pplication Nam isplay Protocol ttings ttwe Mode: /hen Startup:	SECUREMATRIX SL): :	Net	VHV6 VCS.VHV.	poc fore connectir		
	Save	Cancel						

4. On the SECUREMATRIX tab, click to check **Use SECUREMATRIX**.

	Atrust Client Setup					
Atrust	Applications	User Interface	Devices	Network	System	
Navigator	General	Options	SECUREMATRIX			
⊢ Remote Desktop ⊢ Citrix ICA ⊟ 'UNware View VHV6 └ SSH	Connection	Settings — Settings SECUREMATRIX				
	Save	Cancel				

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).

Connection Settings		
GSB Server Address:	* 192.168.0.77	£
Username:		Ê

- 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.

0	Login 🔶 🗙
Login ID	Change Password
	ОК

3. Type your Login ID, and then click **OK** to confirm.



4. The SECUREMATRIX window appears prompting for the password.

0 SI	CUREMATRIX
SECUREMATRIX 7 9 0 8 5 5 4 7 6 0 6 6 9 5 6 3 4 1 5 9 4 5 1 5 0 2 5 Authentication Password	8 2 5 7 1 9 1 5 4 7 3 1 0 7 9 3 7 3 5 7 9 7 4 8 0 9 5 7 5 6 9 8 1
ОК	Cancel

5. Type numbers under your *password pattern* using the keyboard or click numbers directly on the window, and then click **OK** to confirm.



For example, if your *password pattern* is shown as below, type or click numbers,
 0, 0, 4, 5, 1, 3, 6, 2, in sequence.

7920	8 5 5 8	2 5 7 1	1 1 9 1
4 7 6 0	6 6 9 5	4 7 3 1	0793
5634	1 5 9 7	3 5 7 9	7448
4515	0250	9 5 7 5	6981

6. A message appears when SECUREMATRIX authentication is completed. Click **OK** to continue.

0	Message 🔶 🖈 🗙
	Notification from SECUREMATRIX Last Login Timestamp : 2015-11-16 05:56:33
	ОК

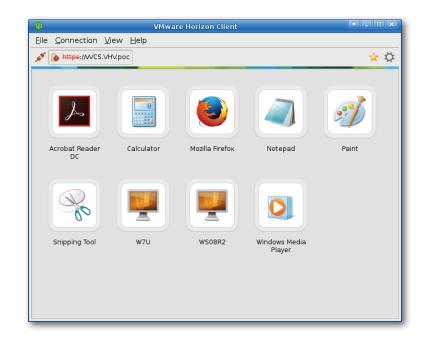
7. A message appears prompting to provide credentials for access to VMware virtual desktops and applications. Click **OK** to continue.



8. Type your credentials on the opened window, and then click **OK** to continue.

0	Authentication	A ×
User	*	
Password	*	
Domain	*	•
		ОК

9. The Desktop and Application list appears. Double-click to select the desired desktop or application.



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**.

0	Login 🔶 🛧 🗙
Login ID	Change Password

2. Type or click numbers under your *old password pattern*, and then click **OK** to continue.

0	SECUREM	IATRIX	A X
SECUREMATRIX			
7920	8 5 5 8	2 5 7 1	1 1 9 1
4 7 6 0	6 6 9 5	4 7 3 1	0793
5634	1 5 9 7	3 5 7 9	7448
4 5 1 5	0250	9 5 7 5	6981
Authentication			
Password			
	ОК	Cancel	

3. Type or click numbers under your *new password pattern*, and then click **OK** to continue.

	0	SECUREM	ATRIX	
Your new password pattern, – for example	SECUREMATRIX 6 2 8 1 2 4 0 2 1 6 5 0 7 6 7 3 Authentication New Password	8 0 7 9 2 5 5 3 3 1 0 9 7 2 2 3	9859 7107 8782 1836	4 9 9 9 0 3 8 3 8 4 1 7 6 8 2 1
		ок	Cancel	

4. Type or click numbers under your *new password pattern* again, and then click **OK** to continue.

0 SECUREN	MATRIX	↑ ×
SECUREMATRIX 7 3 9 2 0 3 0 4 5 1 5 6 7 8 5 3 8 6 2 6 4 1 8 9 4 1 7 8 7 Authentication Confirm Password	2 1 9 3 6 4 5 2 5 5 3 6 9 5 2 4 3 9 6 7 7 6 4 8 0 1 7 0	6 0 5 8
ОК	Cancel	

5. A window appears showing your *new password pattern* in numerical order and prompting for confirmation. Click **OK** to confirm.

0	SECUREM	ATRIX	The second secon
SECUREMATRIX			
	ок	Cancel	

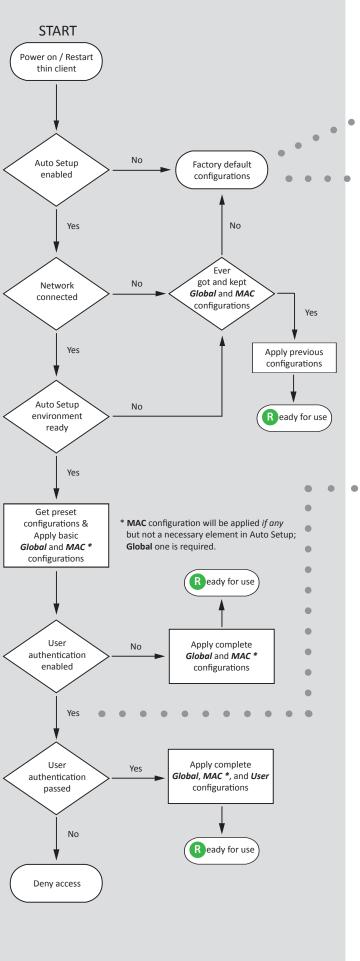
A.4 Auto Setup Flowchart

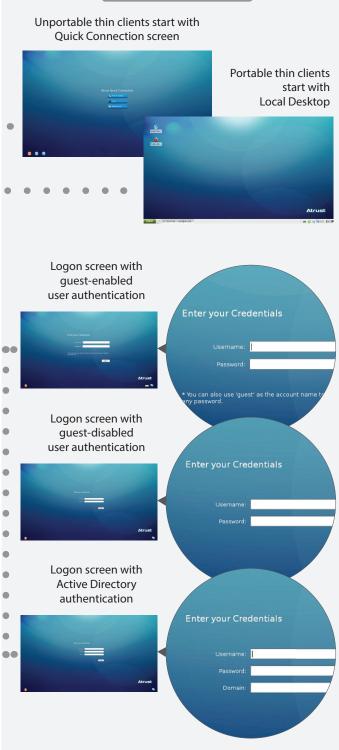
Please see *next page* for sequence of actions in Auto Setup mode.

For details, please refer to User's Guide for Auto Setup.



SCREENS





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	Туре: 14″, FHD 1920 х 1080		
Keyboard / Touchpad	Keyboard: full layout including the numeric keypad Touchpad: 2-button Glide pad		
Sound	Built-in speakers		
I/O interfaces	Left side:Right side:Display and base:1 x DC IN2 x USB-A (USB 3.1 Gen 1)2 x Built-in microphone1 x HDMI1 x USB-C (USB 3.1 Gen 1)1 x Webcam1 x USB-C (USB 3.1 Gen 1)2 x Built-in speaker1 x Audio combo jack1 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° CNon-operating Temperature:-20° C ~ 60° COperating Humidity (Rh):10% ~ 90% (non-condensing)Non-operating Humidity (Rh):5% ~ 95%		

UM-mt182L-ENJP-20031910

