Atrust

Topics Covered:

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

Mobile Thin Client Solution
Atrust mt178W

for Windows 10 IoT Enterprise

USER'S MANUAL

Internal Draft 0.01

Copyright © 2017 Atrust Computer Corp.

Copyright and Trademark Statements

Copyright © 2017 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, and VDI-in-a-Box 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 mt178W mobile thin clients.

Manual Structure and Subjects

Chapter	Subject
1	Provides an overview of Atrust mt178W mobile thin clients.
2	Provides detailed instructions on how to set up Atrust mt178W mobile thin clients.
3	Provides the basics of how to use Atrust mt178W mobile thin clients.
4	Provides instructions on how to configure client settings and customize Atrust mt178W mobile thin clients with the Atrust Client Setup console.
Appendices	Provides supplementary instructions on the maintenance and upgrade of Atrust mt178W mobile thin clients.
Specifications	Provides detailed information on key components of Atrust mt178W mobile thin clients.

Notes, Tips, and Warnings

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

NOTE

- A note provides important information for a specific situation.

TIP

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

WARNING

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

Style Conventions

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

Item	Style	Example
keys on the keyboard	bold	**Ctrl** + **Alt** + **Pause**, **Ctrl** + **Alt**, **Alt** + **Tab**
application windows or entry lists	first letter capitalized	ICA Connection list, RDP 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	**Start the following program on connection**, **Remote Desktop Services**, **Better Appearance (32-bit)**, **Web Logon**
selecting a series of options	bold	**Applications** > **Citrix ICA**, **Applications** > **Remote Desktop**, **Applications** > **VMware View**, **System** > **UWF**

Safety and Regulatory Information

Regulatory Statement

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

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

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

IMPORTANT NOTE:

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

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

Regulatory Information

WEEE (Waste Electrical and Electronic Equipment) Directive

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

Safety Information

WARNING

- Use only power supplies listed in the user instructions.

WARNING

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

WARNING

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

Table of Contents

Copyright and Trademark Statements i

Disclaimer i
Trademark Statements i

About This User's Manual ii

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

Safety and Regulatory Information iv

Regulatory Statement iv
Regulatory Information v
Safety Information v

1 Overview 1

1.1 Introduction 3

1.2 Features 3

1.3 Package Contents 3

1.4 Exterior Components 4

1.5 Before Getting Started 9

1.6 Service Access with your mt178W 10

2 Setting Up Your mt178W 11

2.1 About the AC Adapter 13

2.2 Charging Your Lithium-ion Polymer Battery 13

2.3 Setting Up Your mt178W 14

3 Getting Started 15

3.1 Standard Shortcuts 17

3.2 Accessing Citrix Services 18

3.3 Accessing Microsoft Remote Desktop Services 24

3.4 Accessing VMware View and Horizon View Services 26

4 Configuring Client Settings 29

4.1 Atrust Client Setup 31

4.1.1 Interface Overview 31
4.1.2 Client Settings at a Glance 32

4.2 Configuring System Settings 33

4.2.1 System Tab Overview 33
4.2.2 Available Settings at a Glance 34
4.2.3 Securing the Access to Atrust Client Setup 35
4.2.4 Configuring Shadow Settings for Remote Assistance 36
4.2.5 Updating Firmware from the Management Computer 38
4.2.6 Taking Snapshots for Mass Deployment or System Recovery 40

4.2.7 Deploying Systems with a Created Snapshot 41
4.2.8 Restoring Systems with a Created Snapshot 44
4.2.9 Enabling or Disabling the Appliance Mode 47
4.2.10 Configuring UWF (Unified Write Filter) 51
4.2.11 Enabling or Disabling Auto Registration 53

4.3 Configuring External Device Settings 54

4.3.1 Devices Tab Overview 54
4.3.2 Available Settings at a Glance 54
4.3.3 Configuring Settings for USB Storage Devices 55
4.3.4 Disabling or Enabling Attached Audio Devices 56

4.4 Configuring User Interface Settings 57

4.4.1 User Interface Tab Overview 57
4.4.2 Available Settings at a Glance 57
4.4.3 Configuring the Display of Standard Desktop Shortcuts for Quick Access 58
4.4.4 Configuring the Num Lock Mode 59

4.5 Configuring Service Access Settings 60

4.5.1 Applications Tab Overview 60
4.5.2 Available Settings at a Glance 61
4.5.3 Configuring Basic RDP Connection Settings 62
4.5.4 Accessing Remote Desktop Services 69
4.5.5 Configuring Advanced RDP Connection Settings 74
4.5.6 Configuring Basic ICA Connection Settings 87
4.5.7 Accessing Citrix Services 95
4.5.8 Configuring Advanced ICA Connection Settings 99
4.5.9 Configuring Basic VMware View Connection Settings 110
4.5.10 Accessing VMware View or Horizon View Services 112
4.5.11 Configuring Advanced View Connection Settings 114
4.5.12 Configuring Web Browser Settings 116

Appendices 119

A.1 Resetting Your mt178W 121

A.2 Updating Firmware for Your mt178W 122

Specifications 125

1

Overview

This chapter provides an overview of Atrust mt178W.

1.1 Introduction

Desktop virtualization and simple endpoint devices 3

1.2 Features

Key features of Atrust mt178W 3

1.3 Package Contents

Check your package contents 3

1.4 Exterior Components

Exterior components of Atrust mt178W 4

1.5 Before Getting Started

About UWF (Unified Write Filter) 9
About the default user accounts 9
About the behavior of the system startup 9

1.6 Service Access with your mt178W

Standard and customized desktop shortcuts 10

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

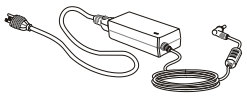
1.2 Features

The key features of Atrust mt178W mobile thin clients are:

- Built-in Wireless 802.11 ac/a/b/g/n and Ethernet network interface
- Support for a wide range of desktop virtualization solutions from industry-leading companies:
  - Microsoft® Remote Desktop
  - Citrix® XenApp™, XenDesktop®, and 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
- Built-in Atrust Client Setup as the local client management console

1.3 Package Contents

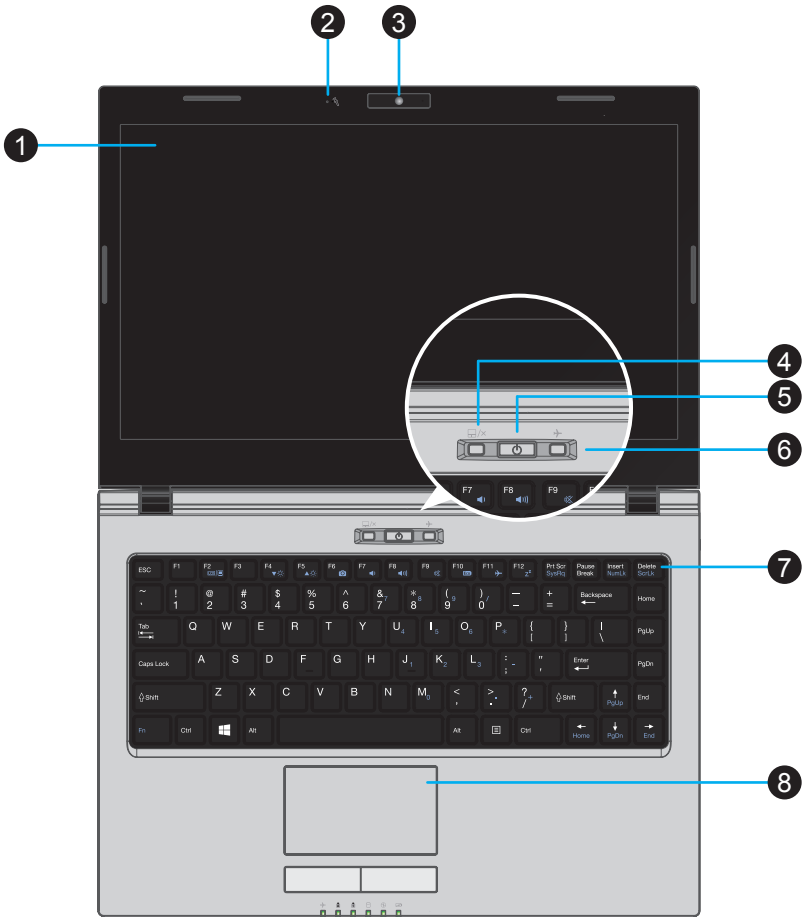
Please check your package contents. Ensure that all of the items are present in your package. If any items are missing or damaged, please contact your dealer immediately.

Atrust mt178W	AC adapter	Battery
		
Quick Start Guide		

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

1.4 Exterior Components

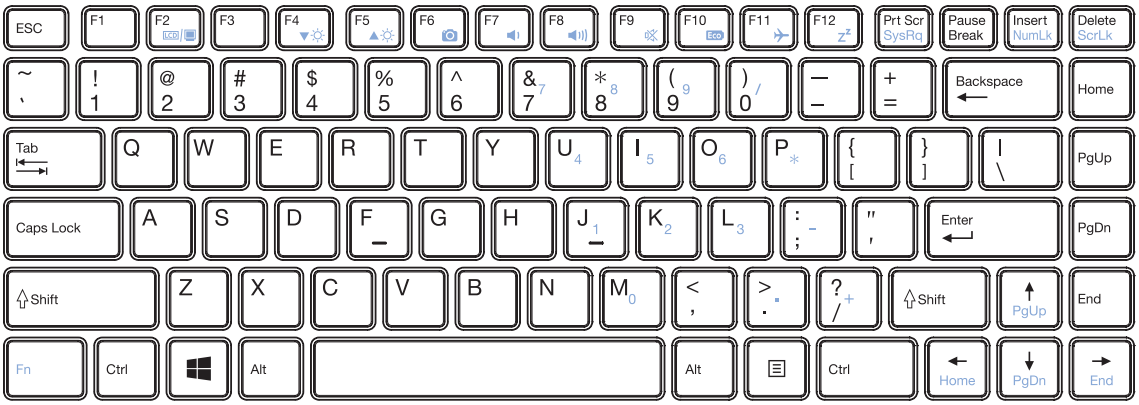
Display and Base Components



No.	Sign	Component	Description
1		LCD display	Built-in display for visual output.
2		Microphone	Built-in microphone for audio input.
3		Webcam (optional)	Built-in video camera for real-time video.
4		Touchpad switch	Press to enable / disable the touchpad.
5		Power button	Press to power on / shut down the mobile thin client.
6		Airplane mode switch	Press to enable / disable the Airplane mode. **Airplane mode:** disabled wireless module
7		Keyboard	Built-in keyboard for control and input.
8		Touchpad	Built-in pointing device for control and input.

Fn Key Combinations

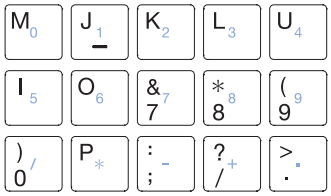
With the combination of **Fn** plus another specific key (with one printed blue symbol on it), you can quickly adjust hardware settings to suit your needs.

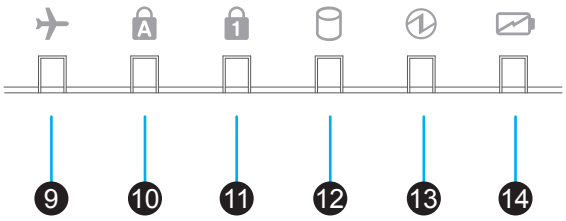


NOTE

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

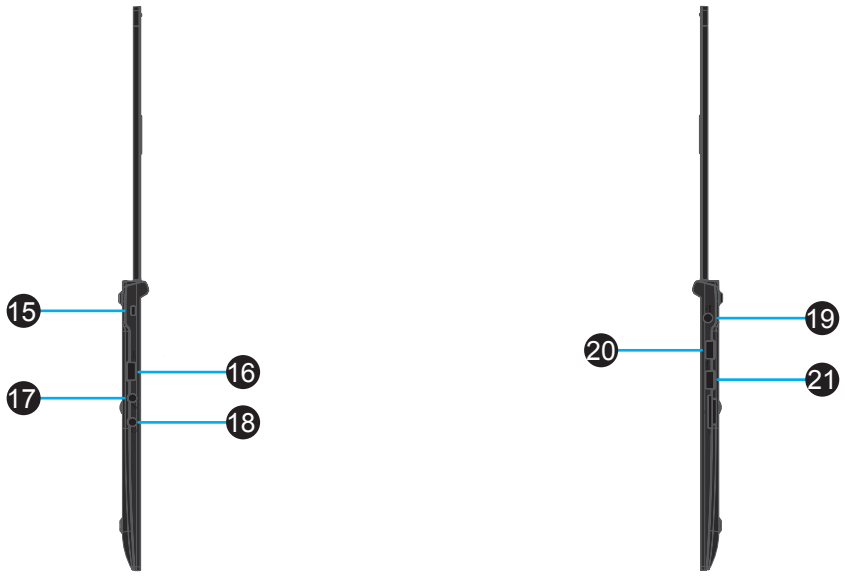
Combination	Description	Combination	Description
Fn + F2	Use to switch the use of displays.	Fn + F12	Use to enter the System Sleep mode. Press the Power button or any key to exit.
Fn + F4	Use to decrease the brightness of the LCD display.	Fn + Prt Scr SysRq	Use to function as a SysRq key.
Fn + F5	Use to increase the brightness of the LCD display.	Fn + Insert NumLk	Use to enable / disable Num Lock mode. **Num Lock Mode:** switches specific keys to enter digits and symbols. Refer to the next ***table*** for details.
Fn + F6	Use to enable / disable the Webcam.	Fn + Delete ScrLk	Use to enable / disable Scroll Lock mode. **Scroll Lock Mode:** allows to scroll through the screen with arrow keys.
Fn + F7	Use to decrease the volume of the built-in speaker.	Fn + PgUp	Use to page up.
Fn + F8	Use to increase the volume of the built-in speaker.	Fn + PgDn	Use to page down.
Fn + F9	Use to mute / unmute the sound.	Fn + Home	Use to function as a Home key.
Fn + F10	Use to enable / disable the ECO mode. **ECO Mode:** Screen Off mode	Fn + End	Use to function as an End key.
Fn + F11	Use to enable / disable the Airplane mode. **Airplane Mode:** disabled wireless module		

Digits and Symbols in Num Lock Mode	Description
	Use to type in the desired digit or symbol (blue one on the key). **NOTE:** You must enable the Num Lock mode first. **NOTE:** To customize Num Lock mode, please see "4.4.4 Configuring the Num Lock Mode" on page 59.



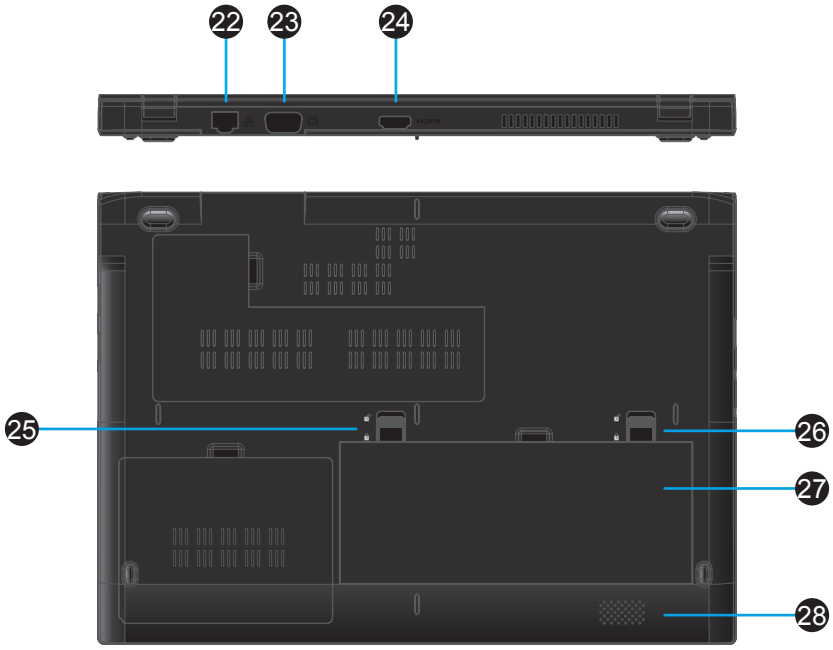
No.	Sign	Component	Description
9		Airplane mode LED	Glows blue when Airplane mode is enabled. **Airplane mode:** disabled wireless module
10		Caps Lock LED	Glows blue when Caps Lock is enabled.
11		Num Lock LED	Glows blue when Num Lock is enabled.
12		Storage LED	Glows blue when flash memory is being accessed.
13		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.
14		Battery LED	Glows orange when the battery is being charged. Glows blue when the battery is fully charged.

Left and Right Side Components



No.	Sign	Component	Description
15		Kensington security slot	Connects a Kensington cable to secure the mobile thin client.
16		USB port (USB 2.0)	Connects to a USB device.
17		Microphone port	Connects to a microphone.
18		Headphone port	Connects to a set of headphones or a speaker system.
19	19V	DC IN	Connects to an AC adapter.
20	SS	USB port (USB 3.0)	Connects to a USB device.
21		USB port (USB 2.0)	Connects to a USB device.

Rear Side and Bottom Components



No.	Sign	Component	Description
22		LAN port	Connects to a network.
23		VGA port	Connects to an external display.
24	HDMI	HDMI port (TBD)	Connects to a high quality digital audiovisual device.
25		Left battery latch	Unlocks the battery by sliding and holding upwards. **NOTE:** To remove the battery, use the right battery latch to unlock the battery, and then slide upwards and hold this latch to remove the battery.
26		Right battery latch	Locks / Unlocks the battery by sliding downwards / upwards. **NOTE:** To remove the battery, use this latch to unlock the battery, and then slide upwards and hold the left battery latch to remove the battery.
27		Lithium-ion polymer battery	Supplies the mobile thin client with the power when an external power source is not available.
28		Speaker	Built-in speaker for audio output.

1.5 Before Getting Started

About UWF (Unified Write Filter)

Before getting started on client configuration through the Atrust Client Setup console or through the Windows 10 IoT Enterprise operating system, please note that in a session any changes to the system will not be kept by default after the system restart. This is due to a special feature called UWF (Unified Write Filter) in your Windows Embedded-based system.

By default, your mt178W is UWF-enabled. Unified Write Filter (UWF) is a sector-based write filter intercepting all write attempts to a protected volume and redirecting those write attempts to a virtual overlay. With UWF, all system changes will only affect the session where the changes are made. After restart, all changes will be discarded.

You can change the default via the Atrust Client Setup console. It's strongly recommended that you read the related section in this user's manual first before making any changes to your system.

WARNING

- Please read the following section **FIRST** before making any changes to your system: "4.2.10 Configuring UWF (Unified Write Filter)" on page 51.

NOTE

- As a thin client device, your mt178W is mainly for access to remote or virtual desktops on servers. With the limited and protected (UWF-enabled) hard disk space, it's ***not*** recommended to save data on your mt178W. Instead, you can use storage spaces over remote / virtual desktops, removable storage devices, or networks.
- In case that you need to copy a file to the protected volume, ensure that its size is smaller than the free memory (overlay) space. Otherwise, your system may have unexpected results or become unresponsive.

About Default User Accounts

There are two default user accounts for your Windows 10 IoT Enterprise-based system: one is the standard, the other administrative. The default credentials are shown as follows:

Type	Account Name	Password
Administrator	Administrator	Atrustadmin
Standard user	User	Atrustuser

NOTE

- The passwords are case sensitive.

About the Behavior of System Startup

Every time when the system is started up, it will automatically log in to the Windows 10 IoT Enterprise operating system using the default standard user account as indicated in the preceding table about default user accounts.

1.6 Service Access with your mt178W

With Atrust mt178W, you can simply access desktop virtualization solutions from Microsoft, Citrix, and VMware, by mouse-clicking. Two types of access shortcuts are available: ***standard*** and ***customized***. The former is available on the desktop of Windows 10 IoT Enterprise by default; the latter can be created and customized through the Atrust Client Setup console.

Standard Desktop Shortcuts

You can find the instructions on how to use standard desktop shortcuts to access on-demand applications or desktops in chapter 3 "Getting Started" on page 15 or in the Quick Start Guide for mt178W.

Customized Desktop Shortcuts

You can find the instructions on how to create and customize access shortcuts in chapter 4 "Configuring Client Settings" on page 29.

2

Setting Up Your mt178W

This chapter provides detailed instructions on how to set up your mt178W mobile thin client.

2.1 About the AC Adapter

Information on the use of the AC adapter 13

2.2 Charging Your Lithium-ion Polymer Battery

How to charge your Lithium-ion polymer battery (Recommended for first time use) 13

2.3 Setting Up Your mt178W

How to set up your mt178W 14

2.1 About the AC Adapter

To use the supplied AC adapter, please do the following:

1. Unpack your mt178W package, and then take out the AC adapter and its detached power cord.
2. Attach the power cord to the AC adapter to assemble your AC adapter.

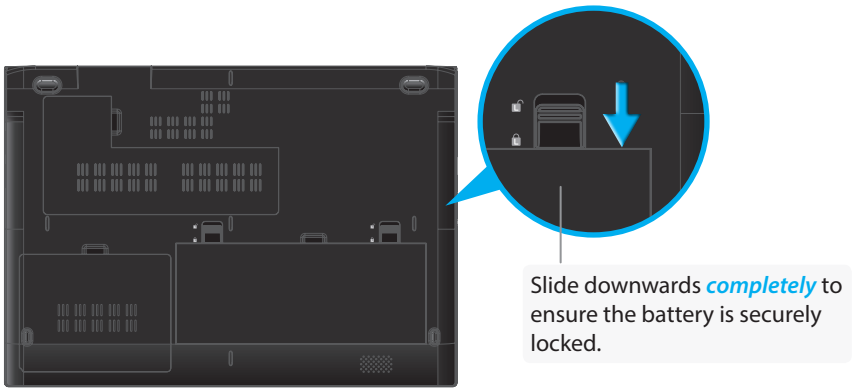
2.2 Charging Your Lithium-ion Polymer Battery

NOTE

- For the first time use, it's recommended to charge your Lithium-ion polymer battery first.

To charge your Lithium-ion polymer battery, please do the following:

1. Place the battery into the battery compartment until it clicks into place, and then S***lide downwards the right battery latch to lock the battery securely***.



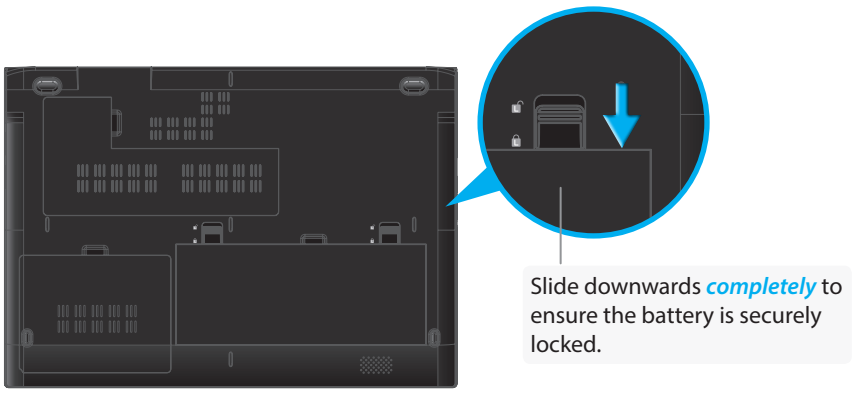
2. Attach the DC plug of the AC adapter to your mt178W, and then connect the AC plug of the adapter to a power outlet.
3. The Battery LED glows orange while the battery is being charged.
4. On completion, the Battery LED glows blue.

2.3 Setting Up Your mt178W

To set up your mt178W, please do the following:

1. Use the AC adapter or the Lithium-ion polymer battery as the power source:

   - To use the AC adapter, attach its DC plug to your mt178W, and connect its AC plug to a power outlet.
   - To use the Lithium-ion polymer battery, place it into the battery compartment until it clicks into place, and then ***slide downwards the right battery latch to lock the battery securely***.



2. Connect the LAN port to your local network with an Ethernet cable or set up a wireless connection later.

3

Getting Started

This chapter provides the basics of how to use your mt178W.

3.1 Standard Shortcuts

Default shortcuts on the local (Windows 10 IoT Enterprise) desktop 17

3.2 Accessing Citrix Services

How to access Citrix services 18

3.3 Accessing Microsoft Remote Desktop Services

How to access Microsoft Remote Desktop services 24

3.4 Accessing VMware View and Horizon View Services

How to access VMware View and Horizon View services 26

3.1 Standard Shortcuts

You can access virtual desktop or application services simply through standard shortcuts available on the desktop.

No.	Shortcuts	Description	See
1	Citrix Receiver	Double click to access Citrix services. **NOTE:** If the secure network connection is not implemented in your Citrix environment, you might not be able to access Citrix services through Citrix Receiver of this new version. Alternatively, Citrix allows service access simply through a Web browser. Try to use the built-in Internet Explorer if you have problems with Citrix Receiver (refer to instructions in this chapter).	3.2
2	Remote Desktop Connection	Double click to access Microsoft Remote Desktop services.	3.3
3	VMware Horizon View Client	Double click to access VMware View and VMware Horizon View services.	3.4

3.2 Accessing Citrix Services

Accessing Citrix Service with Internet Explorer

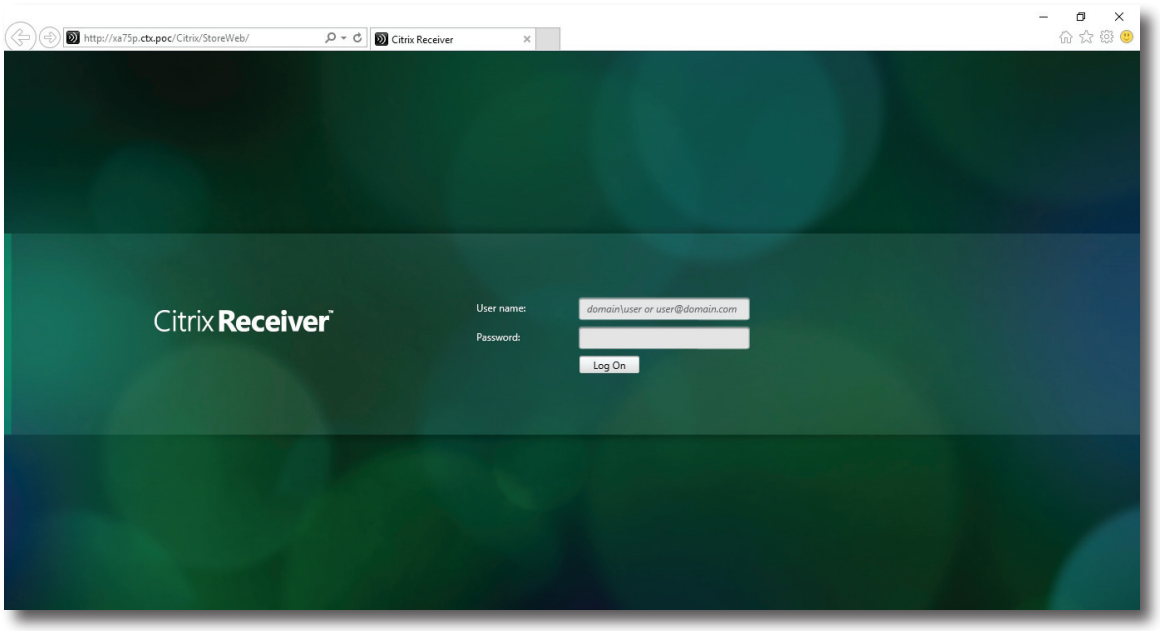
To quickly access Citrix services with the Internet Explorer, please do the following:

1. Open the Internet Explorer by clicking its icon on **Start**.
2. Enter the IP address / URL / FQDN of the server through which Citrix services are accessible.

> **NOTE**
>
> - For XenDesktop 7.0 or the later, consult your IT administrator for the appropriate IP address / URL / FQDN.

3. Follow the on-line instructions to provide the required data and access Citrix services.

Logon Screen Example
XenDesktop / XenApp 7.5 Platinum

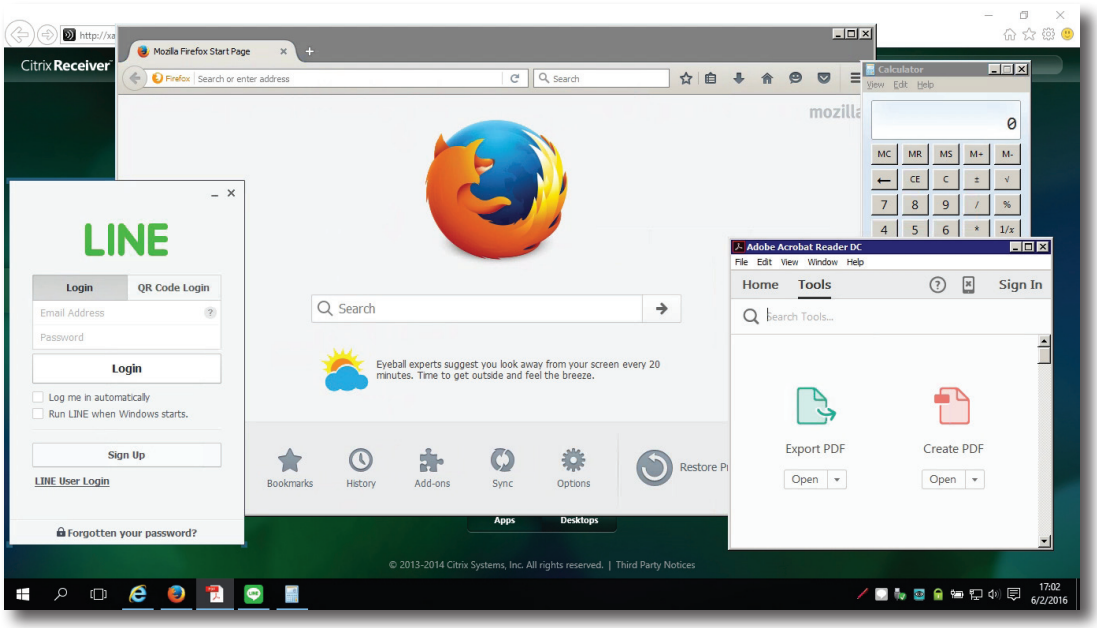


Virtual Desktop Example

Windows 7 Ultimate
(launched in mt178W)

Virtual Application Examples

LINE, Firefox, Calculator, and Adobe Reader
(launched in mt178W)



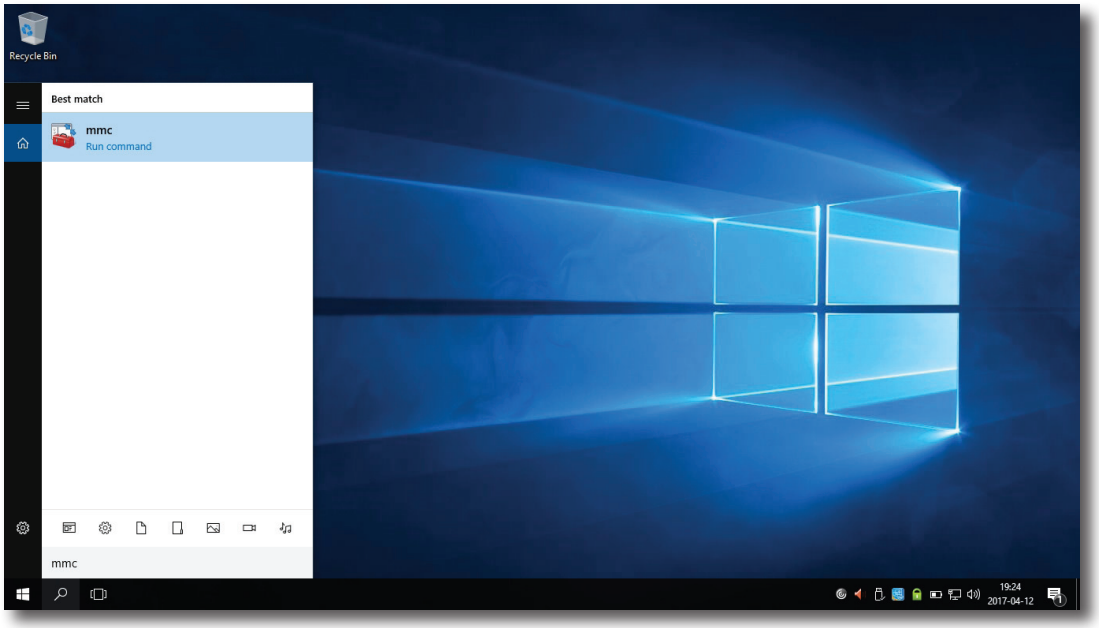
Accessing Citrix Service through the Citrix Receiver Shortcut

To access Citrix services through the Citrix Receiver shortcut, please do the following:

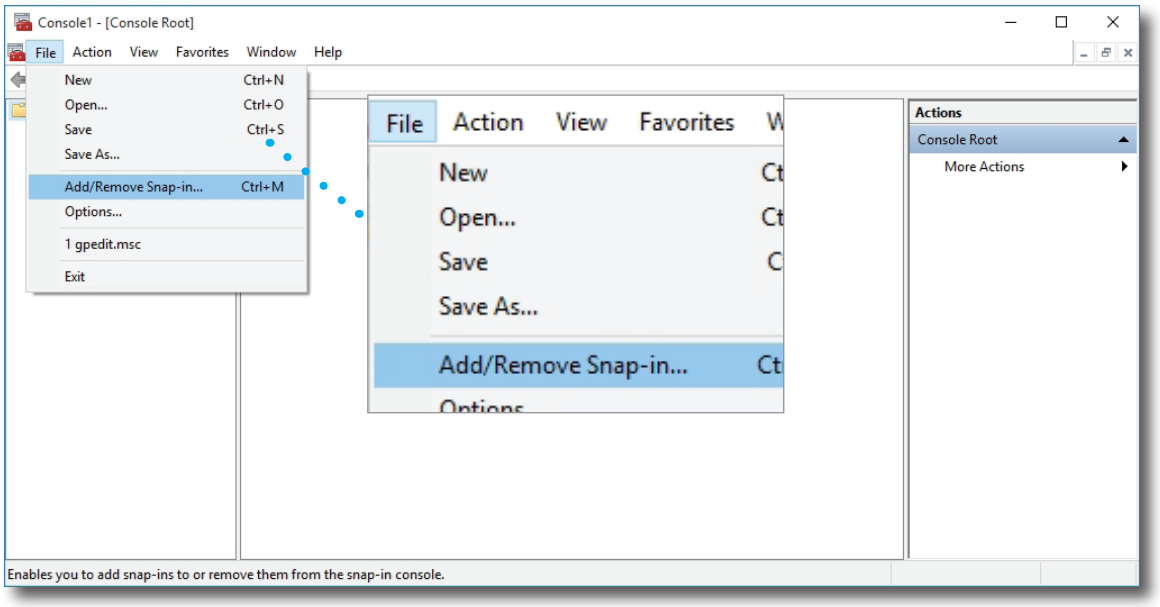
1. Import the required safety certificate for available Citrix services with an administrator account. ***Consult your IT administrator for necessary assistance***.

   a. On the desktop, click in the bottom-left corner.

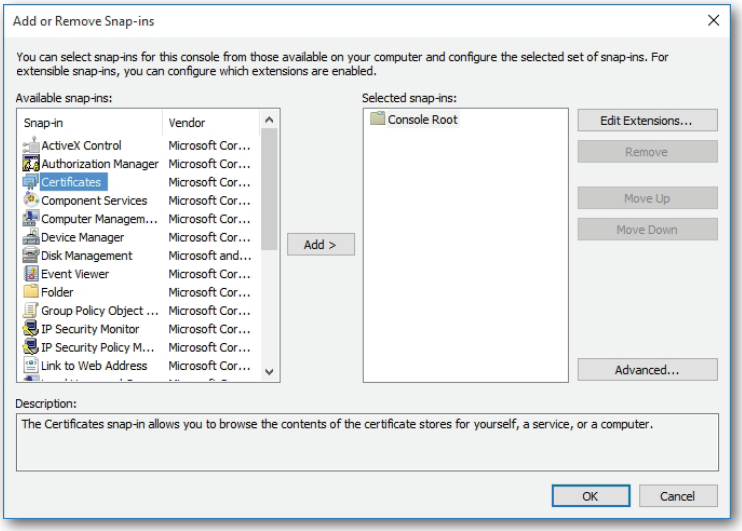
   b. Enter **mmc** on the opened window, and then press **Enter**.



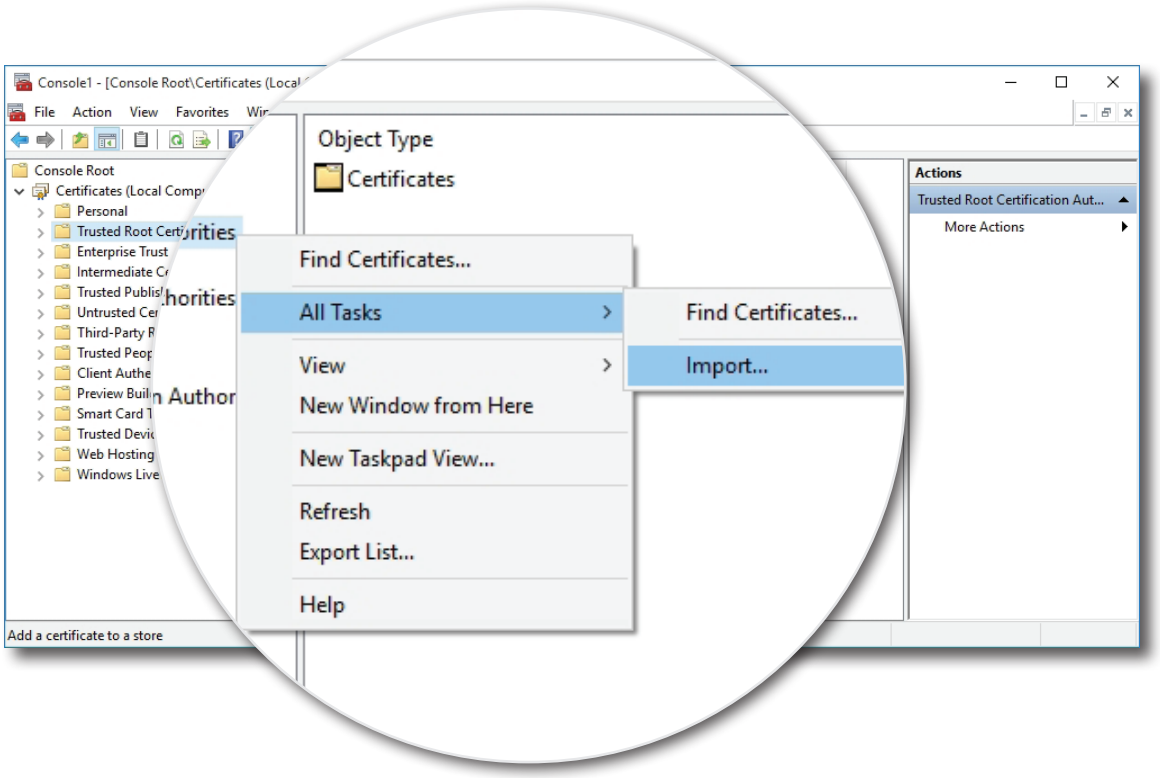
   c. On the Console window, click the File menu to select **Add/Remove Snap-in**.



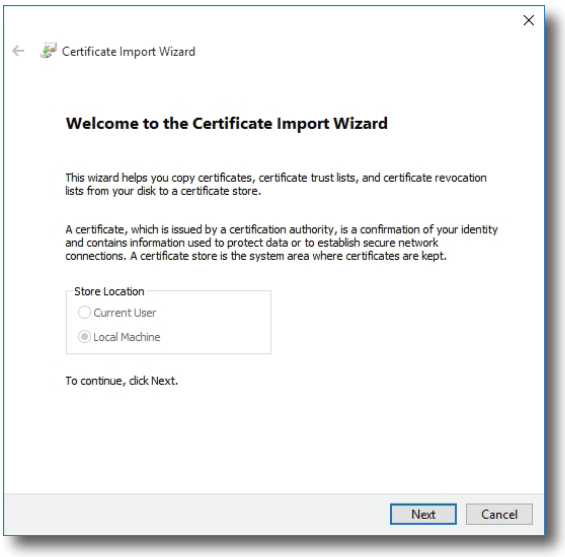
d. On the opened window, click **Certificates** > **Add** > **Computer account** > **Local computer** > **OK** to add the Certificates snap-in.



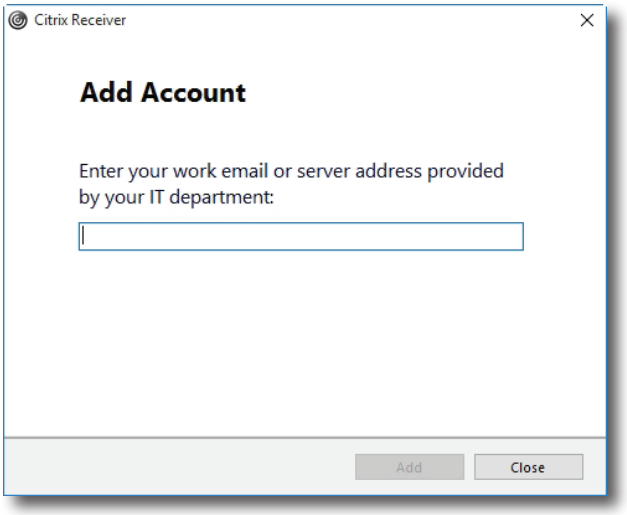
e. On the Console window, click to expand the group tree of Certificates, right-click on **Trusted Root Certification Authorities**, and then select **All Tasks** > **Import** on the popup menu.



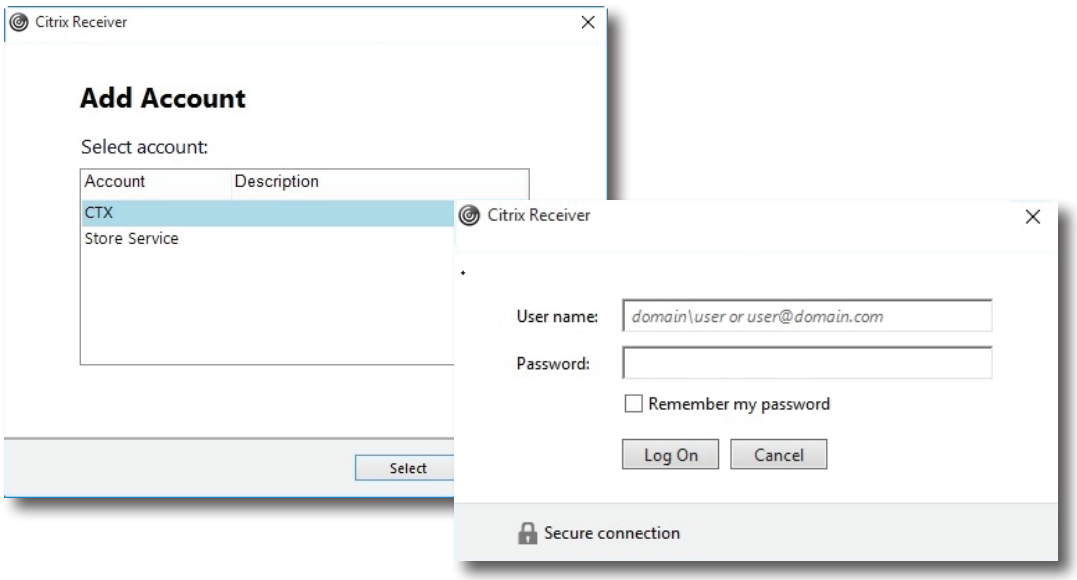
f. Follow the Certificate Import Wizard to import your certificate, and then close the Console window when it's done.



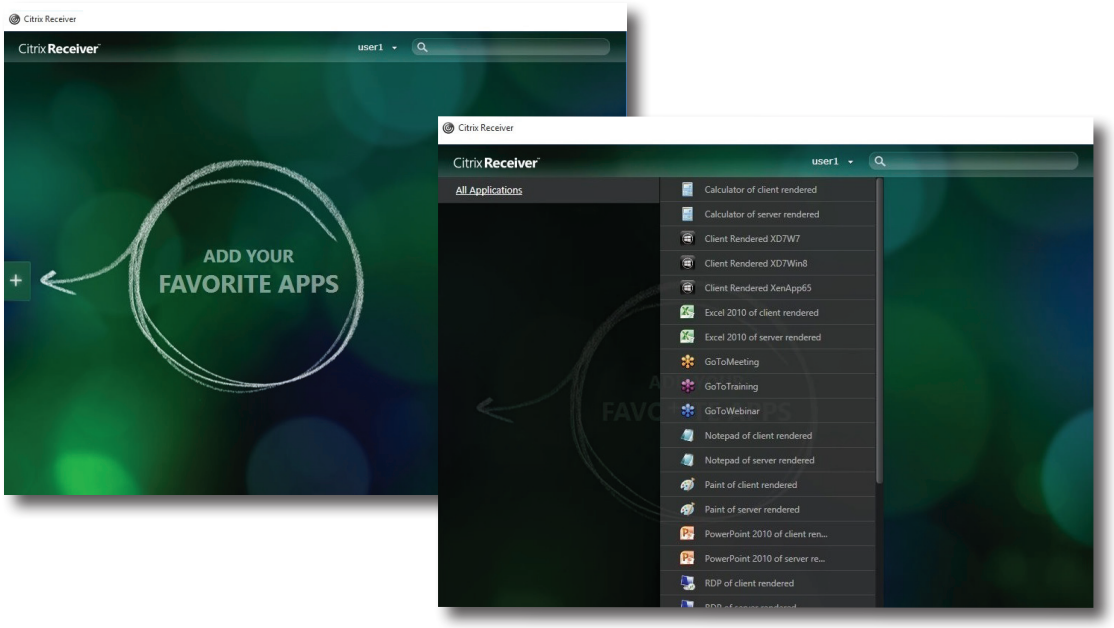
2. Double click **Citrix Receiver** on the desktop.
3. A window appears prompting for the work email or server address. Consult your IT administrator for proper information to provide here, enter the required data, and then click **Add** to continue.



4. Select the desired store account if more than one store is available, type credentials in the opened window, and then click **Log On**.



5. A window appears allowing you to add favorite apps (virtual desktops and applications) for the provided credentials. Click to select the desired application(s). The selected application(s) will appear on that window.

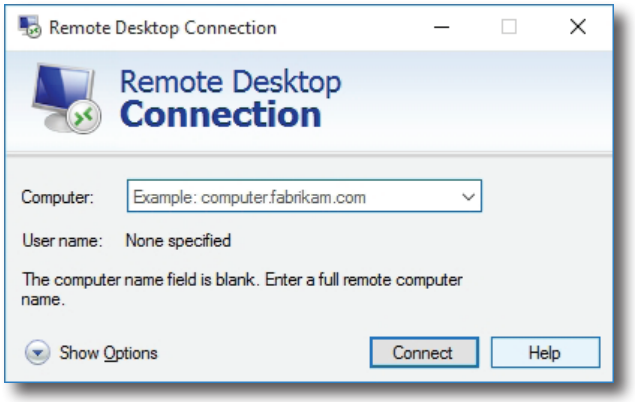


6. Now you can click to launch the desired application. The virtual desktop or application will be displayed on the screen.

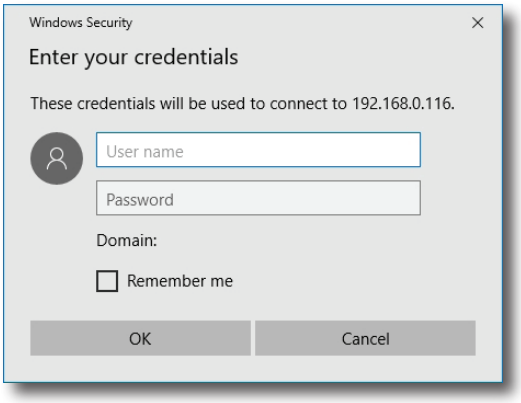
3.3 Accessing Microsoft Remote Desktop Services

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

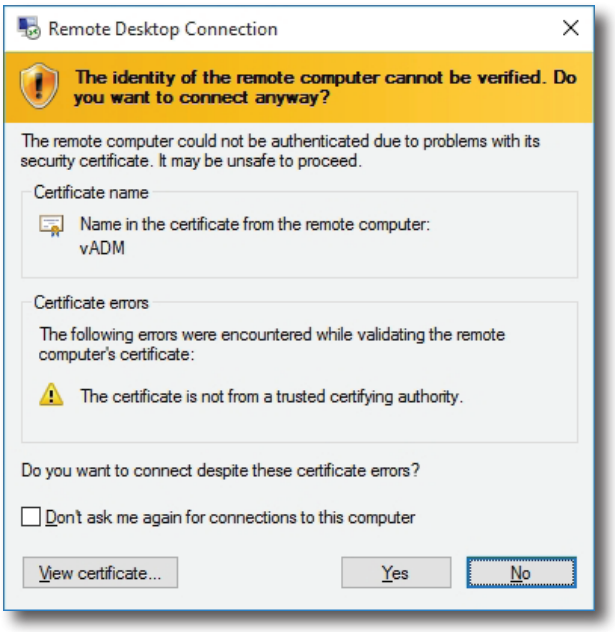
1. Double click **Remote Desktop Connection** on the desktop.
2. Enter the name or IP address of the remote computer on the opened window, and then click **Connect**.



3. Enter your credentials, and then click **OK**.



4. A window may appear with a certificate message about the remote computer. Consult your IT administrator for details and ensure the connection is secure ***first***. To bypass, click **Yes** to continue.

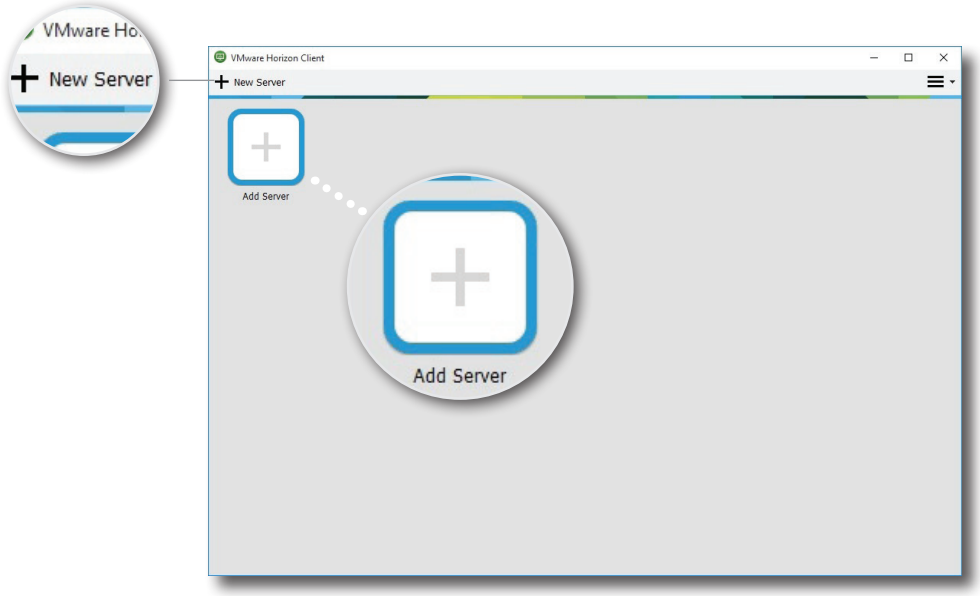


5. The remote desktop will be displayed on the screen (in full-screen by default).

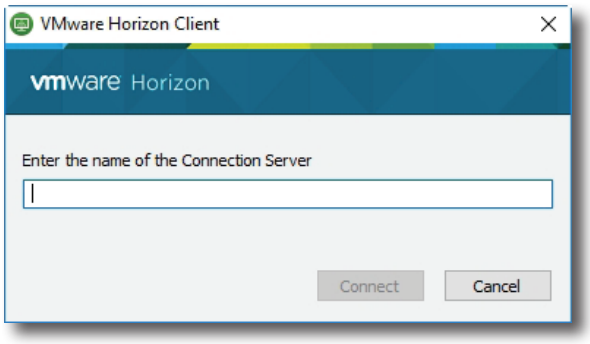
3.4 Accessing VMware View and Horizon View Services

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

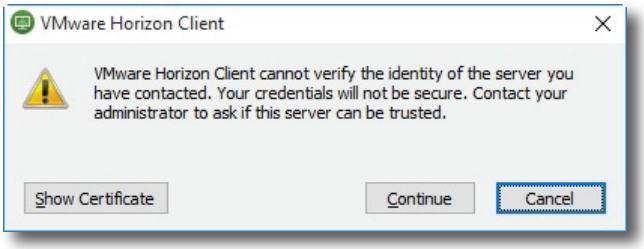
1. Double click **VMware Horizon View Client** on the desktop.
2. A window appears allowing you to add the name or IP address of the View Connection Server.
3. Double-click **Add Server** icon or click **New Server** in the top-left corner.



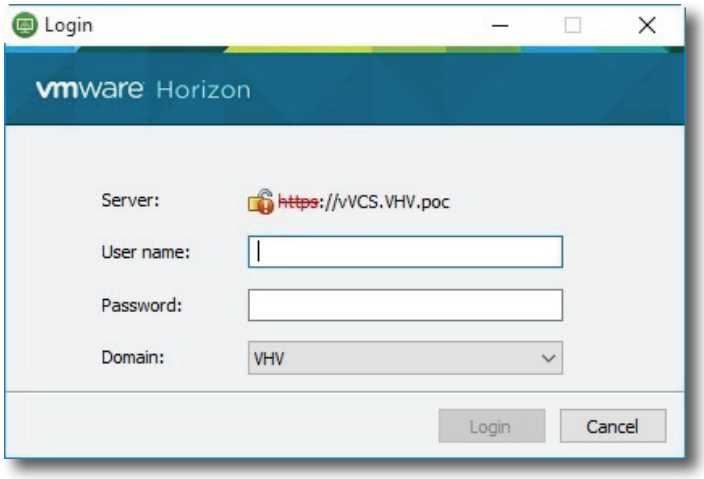
4. A window appears prompting for the name or IP address of the View Connection Server. Enter the required information, and then click **Connect**.



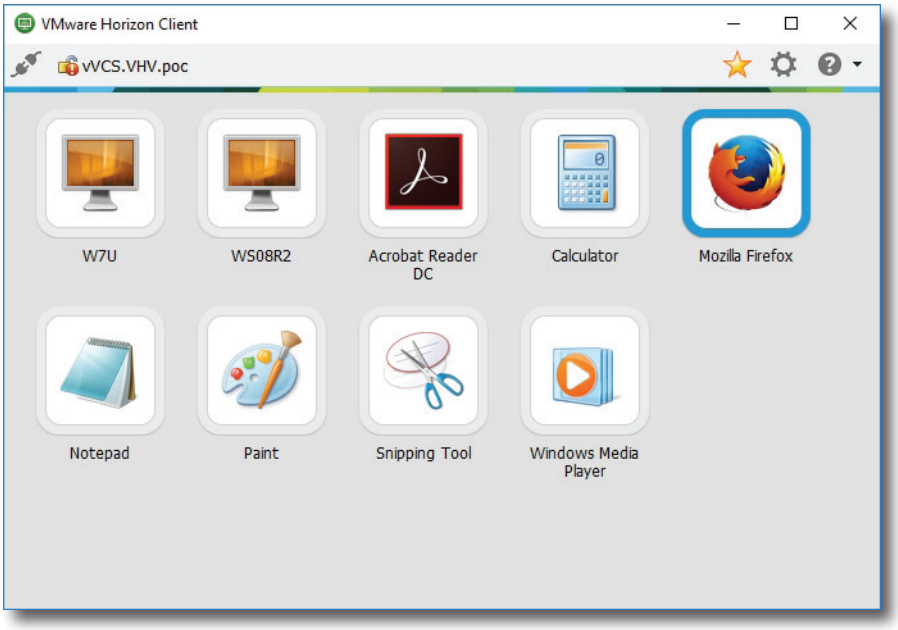
5. A window may appear with a certificate message about the remote server. Consult your IT administrator for details and ensure the connection is secure ***first***. To bypass, click **Continue**.



6. A window may appear with a Welcome message. Click **OK** to continue.
7. Provide your user name and password on the opened window, and then click **Login**.



8. A window appears with available desktops or applications for your credentials. Double-click to select the desired desktop or application.



9. The desktop or application will be displayed on the screen.

4

Configuring Client Settings

This chapter provides instructions on how to configure advanced settings and customize your mt178W with Atrust Client Setup.

4.1 Atrust Client Setup

Interface overview 31
Available settings at a glance 32

4.2 Configuring System Settings

System tab overview 33
Available settings at a glance 34

4.3 Configuring External Device Settings

Devices tab overview 54
Available settings at a glance 54

4.4 Configuring User Interface Settings

User Interface tab overview 57
Available settings at a glance 57

4.5 Configuring Service Access Settings

Applications tab overview 60
Available settings at a glance 61

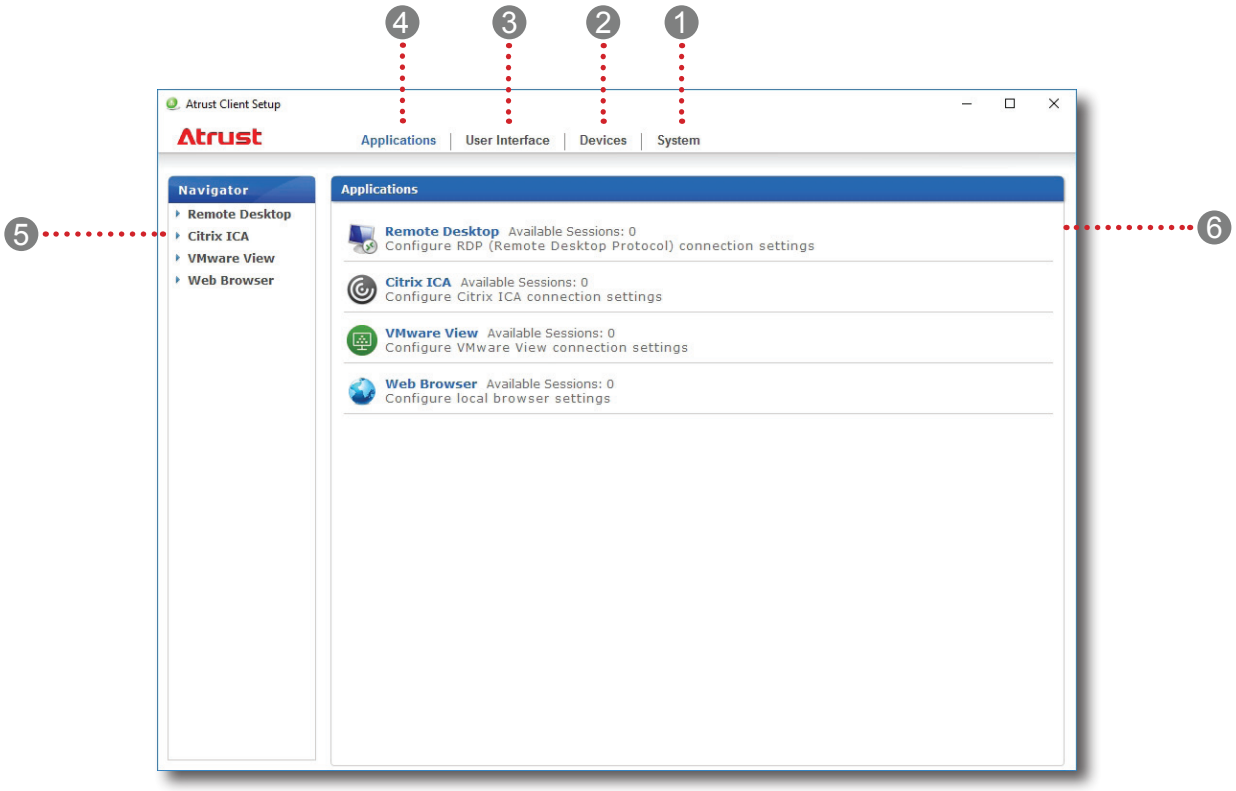
4.1 Atrust Client Setup

4.1.1 Interface Overview

To access Atrust Client Setup on your mt178W thin client, please do the following:

1. Log in to your mt178W with an administrator account (see page 9 for the default).
2. Click **Atrust Client Setup** on the Start screen.
3. The Atrust Client Setup window appears.

Interface Overview



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

4.1.2 Client Settings at a Glance

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

Tab	Setting Item	Section	Page
System	• Configuring passwords • Configuring remote assistance settings • Updating firmware • Taking snapshots • Enabling/Disabling the Appliance mode • Configuring UWF (Unified Write Filter) settings • Configuring Auto Registration	4.2 Configuring System Settings	33
Devices	• Configuring settings for USB storage devices • Configuring settings for audio devices	4.3 Configuring External Device Settings	54
User Interface	• Configuring the display of service access shortcuts • Configuring the Num Lock mode	4.4 Configuring User Interface Settings	57
Applications	• Configuring Microsoft RDP connection settings • Configuring Citrix ICA connection settings • Configuring VMware View connection settings • Configuring Web browser session settings	4.5 Configuring Service Access Settings	60

NOTE

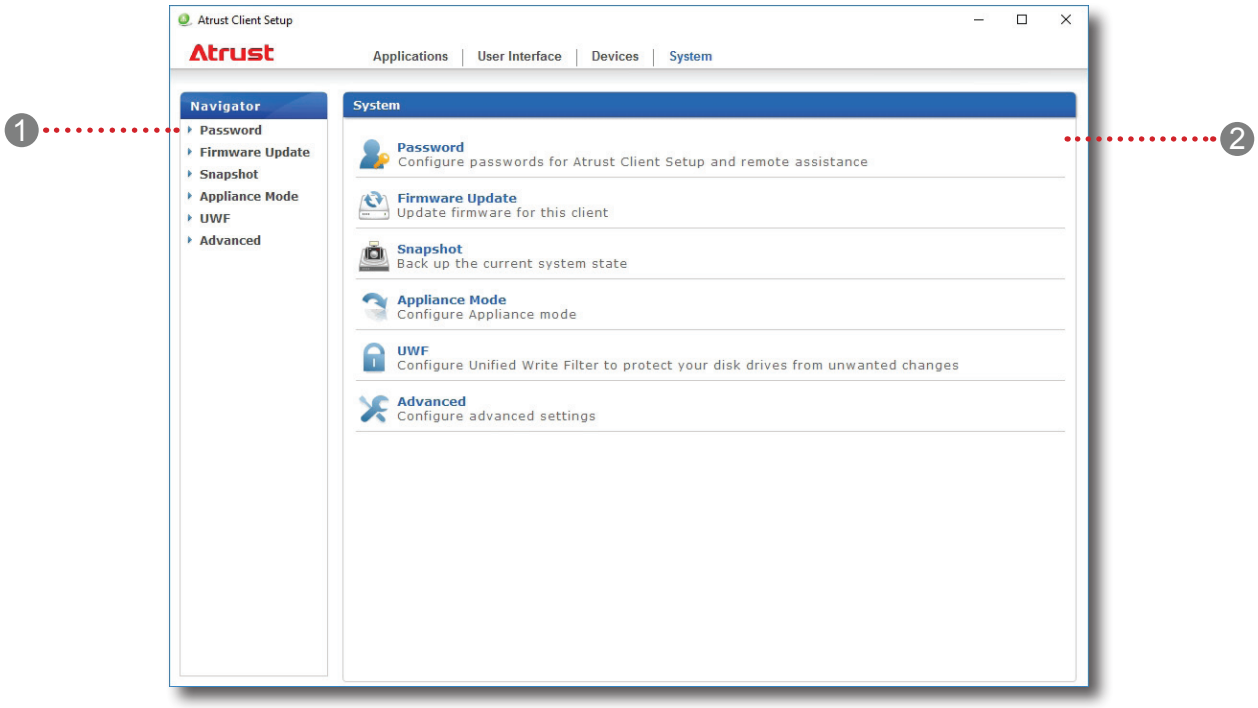
- The table above is only applicable to Atrust mt178W thin clients running Windows 10 IoT Enterprise. The available setting categories and items of the Atrust Client Setup console for other Windows 10 IoT Enterprise-based, Windows Embedded-based, Linux-based, and ARM Linux-based thin clients might be different.

4.2 Configuring System Settings

4.2.1 System Tab Overview

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

System Tab Overview



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

4.2.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
System	Password		Click to secure the access to Atrust Client Setup. Click to configure settings for remote assistance.	4.2.3 4.2.4	35 36
	Firmware Update		Click to update firmware locally with the help of a remote management computer. This feature is only applicable when the client is managed by the Atrust Device Manager console.	4.2.5	38
	Snapshot		Click to take a snapshot (system image) of the client for mass deployment or system recovery.	4.2.6 4.2.7 4.2.8	40 41 44
	Appliance Mode		Click to enable/disable the Appliance mode to allow/ disallow the automatic RDP / ICA / View sessions. In Appliance mode, the client starts up with the desired RDP / ICA / View session and performs the configured action after exiting the session.	4.2.9	47
	UWF		Click to configure UWF (Unified Write Filter) settings. Enabling UWF option will redirect all writes targeted for disk volumes to a RAM cache. All system changes will only affect the session where the changes are made.	4.2.10	51
	Advanced		Click to configure advanced settings such as Auto Registration.	4.2.11	53

NOTE

- Atrust Device Manager is a remote and mass client management console, helping you remotely mange 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.

4.2.3 Securing the Access to Atrust Client Setup

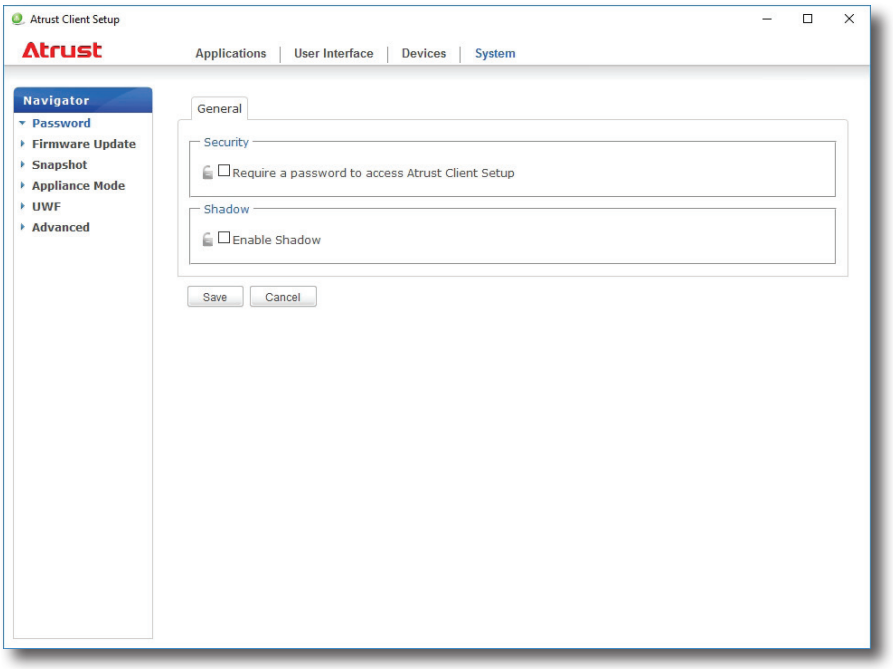
You can password protect the access to Atrust Client Setup by the **Password** setting.

To secure the access to Atrust Client Setup, please do the following:

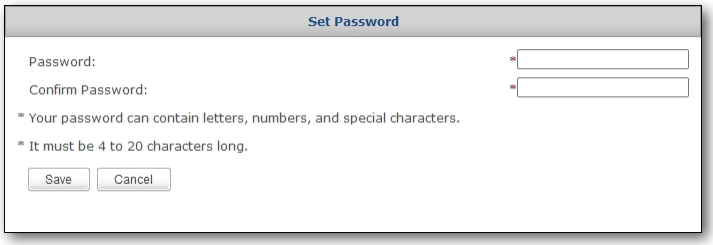
NOTE

- System administrators (and only administrators) are allowed to access Atrust Client Setup. If you don't secure the access to Atrust Client Setup, administrator privileges are sufficient to access Atrust Client Setup. If a password is set here, administrators will need that password to enter Atrust Client Setup.

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



2. Under the Security section, click to check **Require a password to access Atrust Client Setup**.
3. A window appears prompting you to set the password.



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

4.2.4 Configuring Shadow Settings for Remote Assistance

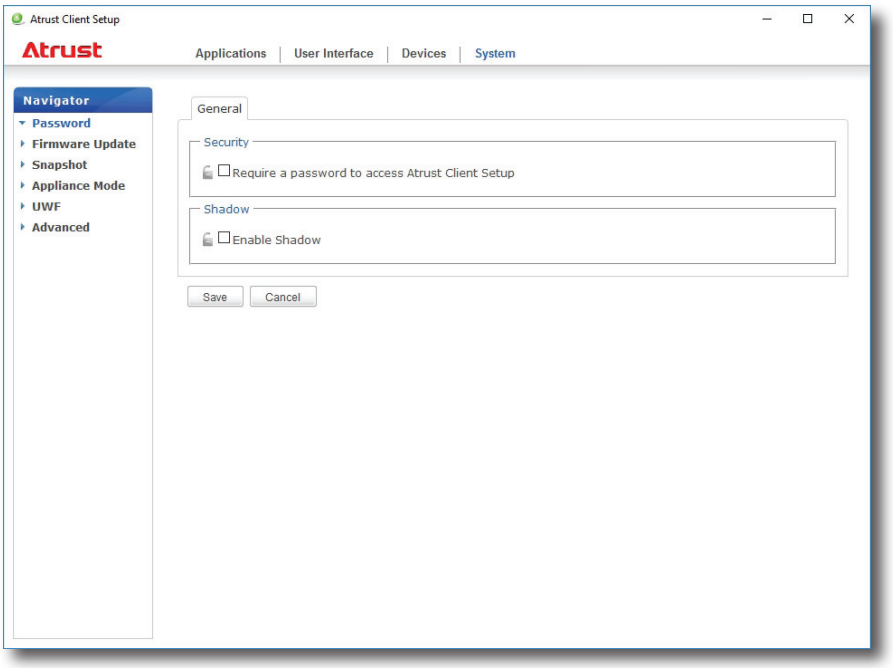
The Shadow feature allows an administrator to remotely assist client users in resolving problems or configuring local settings. When this feature is enabled, an administrator can monitor and control a client from a remote computer just like a local user.

NOTE

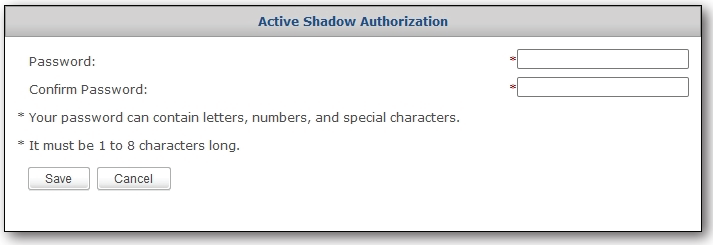
- To use the Shadow feature on a remote computer, you need to install the Atrust Device Manager and also Java software on the remote computer, and add your client into a managed group under Atrust Device Manager. For detailed instructions, please refer to the User's Manual for Atrust Device Manager.

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

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



2. Under the Shadow section, click **Enable Shadow**.
3. The Shadow feature is enabled and a window appears for you to set the password for remote assistance.



NOTE

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

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

NOTE

- When the Shadow feature is enabled, on mt178W, the icon will appear in the Notification area of the Task bar. If this feature is currently being performed from a remote computer, the icon will change its color to yellow .

4.2.5 Updating Firmware from the Management Computer

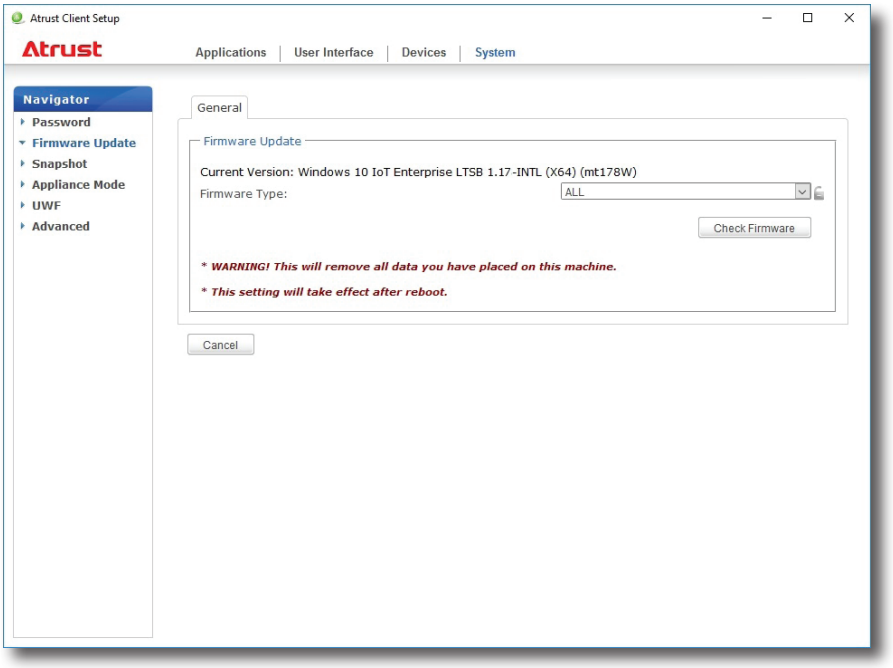
Update Firmware allows users to update client firmware from the remote management computer to get the client device up-to-date.

NOTE

- Ensure that your client 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's Manual for Atrust Device Manager.

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

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

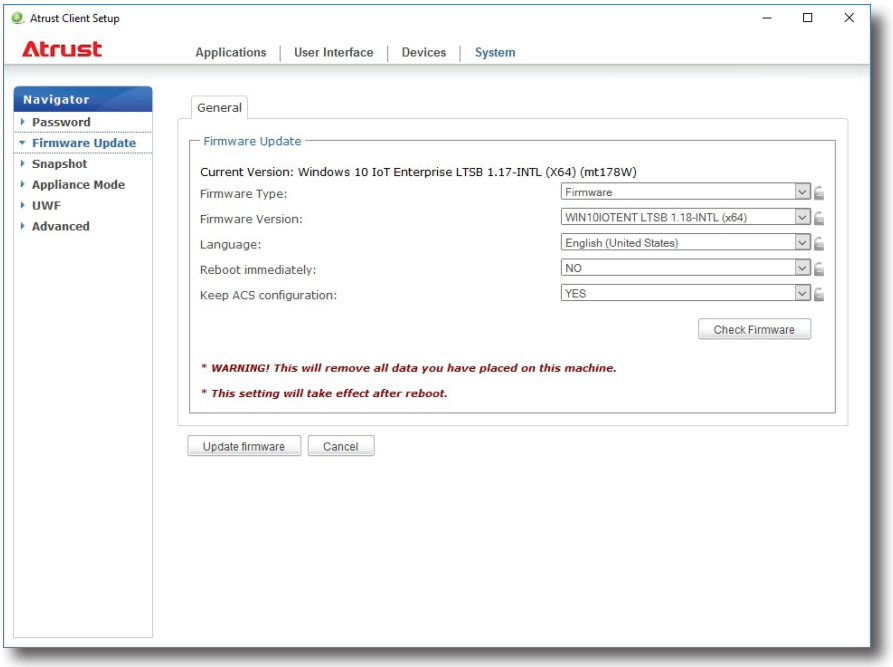


2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Firmware**, and then click **Check Firmware**.
3. On completion, a window appears notifying you that the Firmware list has been loaded. Click **OK** to continue.

NOTE

- The available firmware versions depend on how many versions have been imported into the remote Atrust Device Manager.

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



Firmware Update Options	
Item	**Description**
Firmware Type	Click to select the desired firmware type. **Type** / **Description** ALL — All firmware types, **Firmware** and **Snapshot**. Firmware — The system image of a client. Snapshot — The system image of a client coming from another client of the same model. **NOTE:** Options may not be available for the firmware version of your model.
Firmware Version	Click to select the desired firmware version from the Firmware list.
Language	Click to select the interface language of the system, including the Atrust Client Setup console. **NOTE:** Available languages may vary with the firmware version.
Reboot immediately	Click to choose whether to restart the system immediately for firmware update or manually restart the system later.
Keep ACS configuration	Click to choose whether to keep client settings under Atrust Client Setup. **NOTE:** If **Yes** is selected, all client settings under Atrust Client Setup will remain unchanged after firmware update. If **No** is selected, all settings will be restored to the factory default. **NOTE:** If the client is managed by Atrust Device Manager and here **No** is selected, Atrust Device Manager will fail to manage the client after firmware update. For more information on Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

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

4.2.6 Taking Snapshots for Mass Deployment or System Recovery

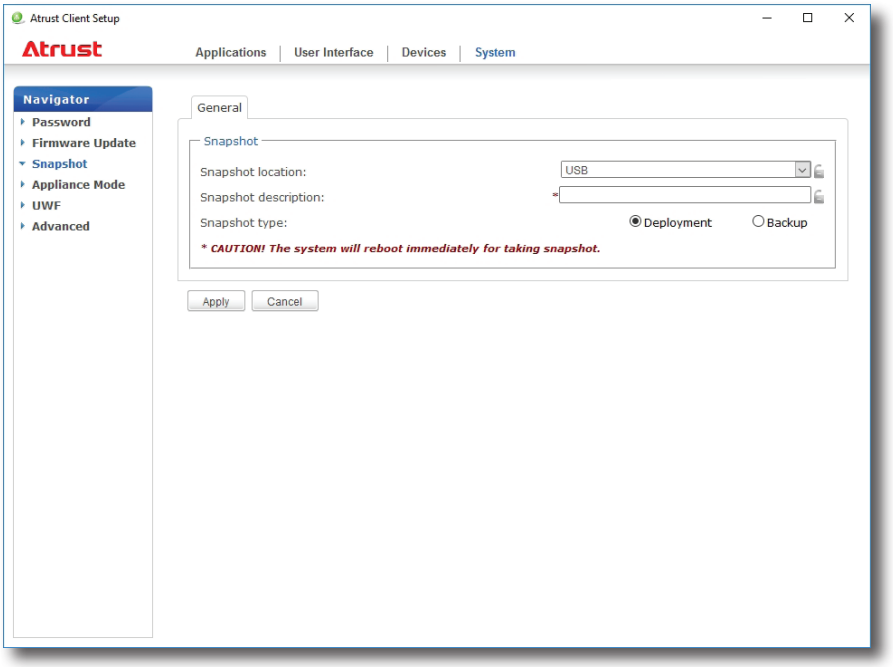
A snapshot is the system image of a client, allowing you to use that image for mass deployment or system recovery. This image can be stored on a remote management computer or a locally attached USB flash drive.

NOTE

- To store the system image on a remote computer, ensure that Atrust Device Manager has been installed on that computer, and that the client has been added into a managed group under Atrust Device Manager.

To take a snapshot from a client, please do the following:

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



2. Under the Snapshot section, click the drop-down menu to select where to store the snapshot. Two options are available: **Network** and **USB**.

   - To store the snapshot file set on the remote computer, please select **Network**.
   - To store the snapshot file set on the locally attached USB flash drive, please select **USB**.

3. Type in the desired description for the snapshot, and then select its type: **Deployment** or **Backup**.

NOTE

- Taking a snapshot for mass deployment (**Deployment** is selected) will reset the startup behavior to the default (auto-login with the default standard user account). For details, please see "About the Behavior of System Startup" on page 9.
- Additionally, all system specific information, including the Computer Security Identifier (SID) and computer name, will be reset or removed from the system image by performing the System Preparation (**Sysprep**) tool automatically.

4. Click **Apply** to start taking the snapshot.
5. A message will appear prompting for confirmation. Click **Yes** to confirm.
6. The system will restart to complete the process ***automatically***.

NOTE

- Please wait for the process to complete ***automatically***. Taking a snapshot needs several minutes and requires system reboot more than one time. In addition, if **Deployment** is selected, the **Sysprep** process will not be shown on the desktop but only be performed in the background.

4.2.7 Deploying Systems with a Created Snapshot

Your snapshots may be stored on a remote computer over the network or on a USB flash drive. Depending on where your snapshot is located, you can deploy a system image either through the network or a USB flash drive.

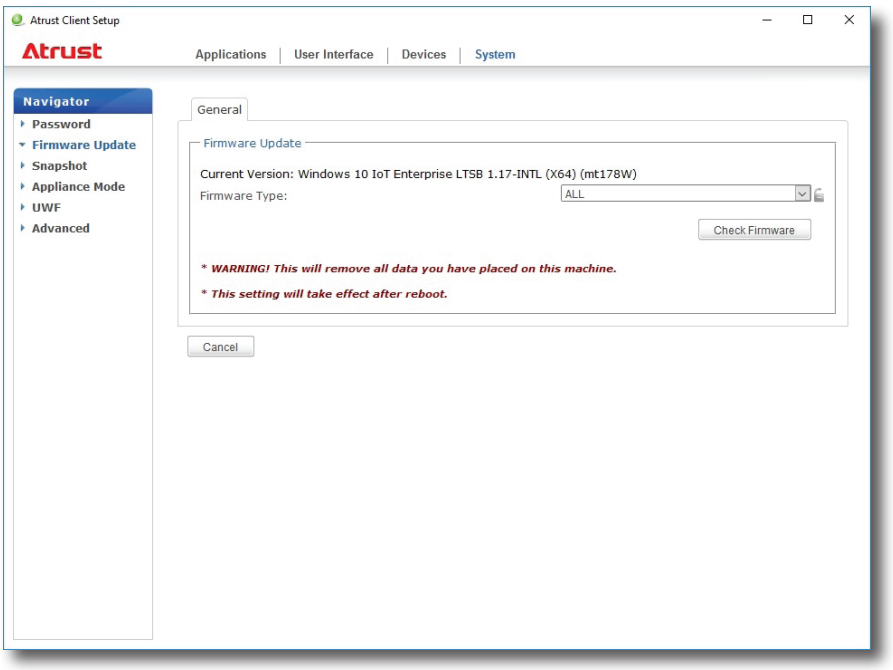
NOTE

- For detailed information on how to take a snapshot, please refer to section "4.2.6 Taking Snapshots for Mass Deployment or System Recovery" on page 40.

With a Snapshot on a Remote Computer

To deploy a system image on your mt178W with a snapshot on a remote computer, please do the following:

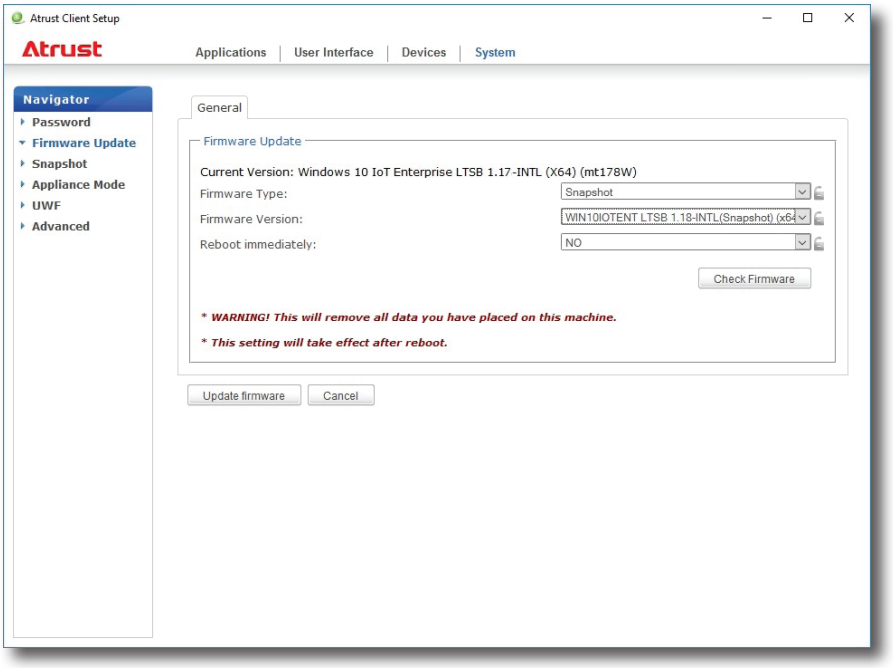
1. On Atrust Client Setup, click **System** > **Firmware Update**.



2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Snapshot**. The system will automatically download the Snapshot list from the remote computer.
3. Upon completion, a message appears notifying you that the Snapshot list has been loaded.

> **NOTE**
>
> - Client snapshots stored on the remote computer are managed by Atrust Device Manager. For more information on how to manage client snapshots with Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

4. Click **OK** to continue.
5. Click drop-down menus to select the desired snapshot and other options.



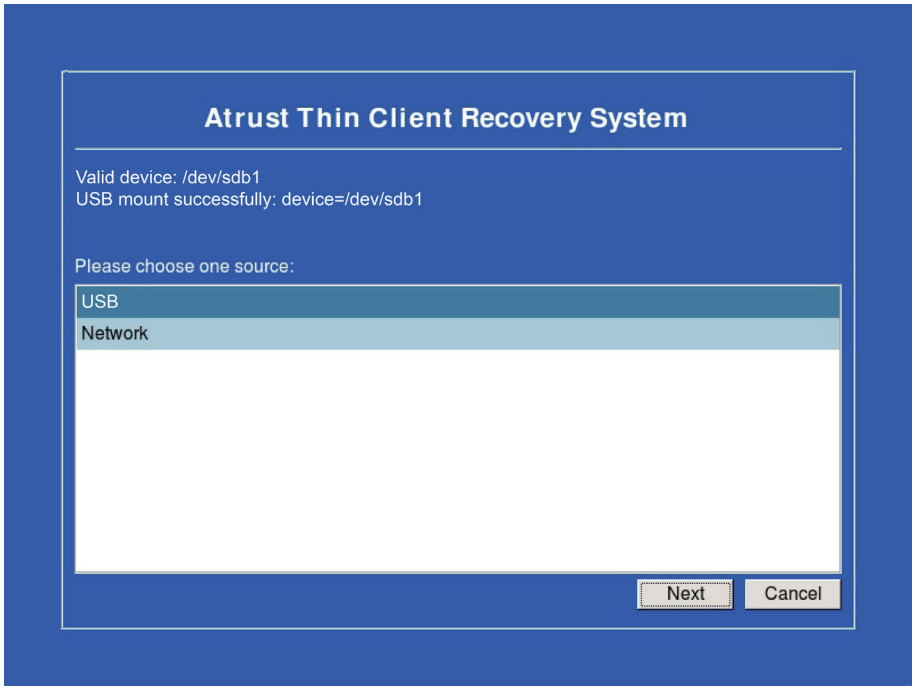
Options for Deploying a Snapshot	
Item	**Description**
Firmware Version	Click to select the desired snapshot from the Snapshot list.
Reboot immediately	Click to choose whether to restart the system immediately for firmware update or manually restart the system later.

6. Click **Update firmware** to confirm your selections. The system will start deploying the snapshot after restart.

With a Snapshot on a USB Flash Drive

To deploy a system image on your mt178W with a snapshot on a USB flash drive, please do the following:

1. Plug the USB flash drive into a free USB port of the client.
2. Start up or restart the client.
3. During the period of POST (Power-On Self-Test), press **F7** to enter the Boot Device menu.
4. Select to boot from the attached USB flash drive.
5. The Atrust Thin Client Recovery System is launched.
6. Select **USB**, and then click **Next** to continue.



7. The recovery system start deploying the snapshot to the client.
8. After completion, click **Finish** to restart the client.

4.2.8 Restoring Systems with a Created Snapshot

Your snapshots may be stored on a remote computer over the network or on a USB flash drive. Depending on where your snapshot is located, you can restore a system image either through the network or a USB flash drive.

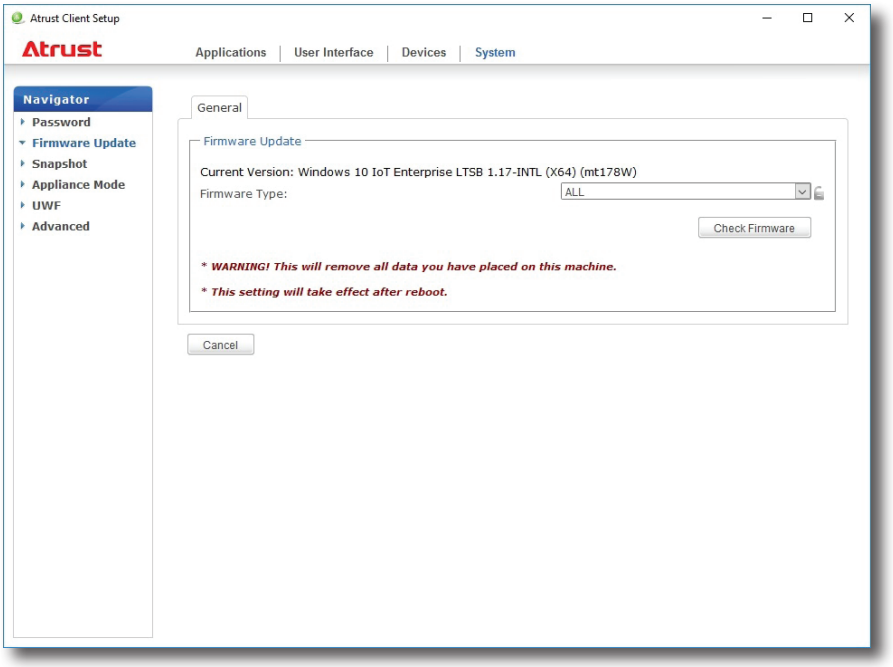
NOTE

- For detailed information on how to take a snapshot, please refer to section "4.2.6 Taking Snapshots for Mass Deployment or System Recovery" on page 40.

With a Snapshot on a Remote Computer

To restore a system image to your mt178W with a snapshot on a remote computer, please do the following:

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

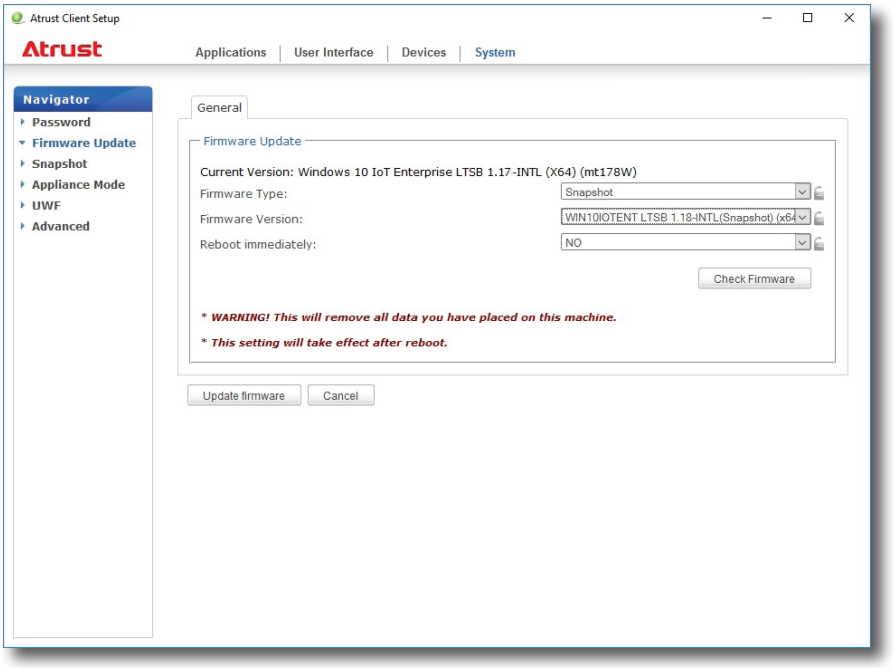


2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Snapshot**. The system will automatically download the Snapshot list from the remote computer.
3. Upon completion, a message appears notifying you that the Snapshot list has been loaded.

NOTE

- Client snapshots stored on the remote computer are managed by Atrust Device Manager. For more information on how to manage client snapshots with Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

4. Click **OK** to continue.
5. Click drop-down menus to select the desired snapshot and other options.



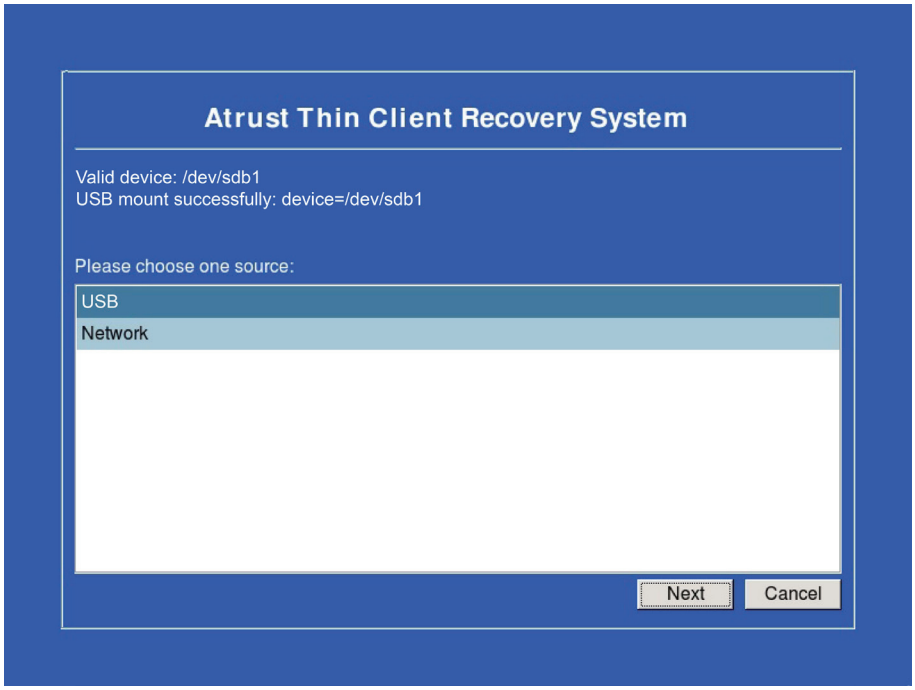
Options for Restoring a Snapshot	
Item	**Description**
Firmware Version	Click to select the desired snapshot from the Snapshot list.
Reboot immediately	Click to choose whether to restart the system immediately for firmware update or manually restart the system later.

6. Click **Update firmware** to confirm your selections. The system will start restoring the snapshot after restart.

With a Snapshot on a USB Flash Drive

To restore a system image to your mt178W with a snapshot on a USB flash drive, please do the following:

1. Plug the USB flash drive into a free USB port of the client.
2. Start up or restart the client.
3. During the period of POST (Power-On Self-Test), press **F7** to enter the Boot Device menu.
4. Select to boot from the attached USB flash drive.
5. The Atrust Thin Client Recovery System is launched.
6. Select **USB**, and then click **Next** to continue.



7. The recovery system start restoring the snapshot to the client.
8. After completion, click **Finish** to restart the client.

4.2.9 Enabling or Disabling the Appliance Mode

The Appliance mode allows your thin client to start up directly with the desired Microsoft Remote Desktop, Citrix ICA, VMware View or Horizon View session. After exiting a session, the client will perform the configured action.

NOTE

- There are two similar but different modes for your thin client:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired RDP / ICA / View session and perform the configured action after exiting the session. Available actions include: • Re-launching a new session • Restarting the thin client • Turning off the thin client
2	Autostart	The client will start up directly with the desired RDP / ICA / View session and perform the configured action after exiting the session. Available actions include: • Returning to the local desktop • Re-launching a new session • Restarting the thin client • Turning off the thin client

- For more information on above modes, please refer to sections:
  - ✧ 4.2.9 on page 47 (Appliance mode)
  - ✧ 4.5.5 on page 74 (Autostart mode for RDP sessions)
  - ✧ 4.5.8 on page 99 (Autostart mode for ICA sessions)
  - ✧ 4.5.11 on page 114 (Autostart mode for View sessions)

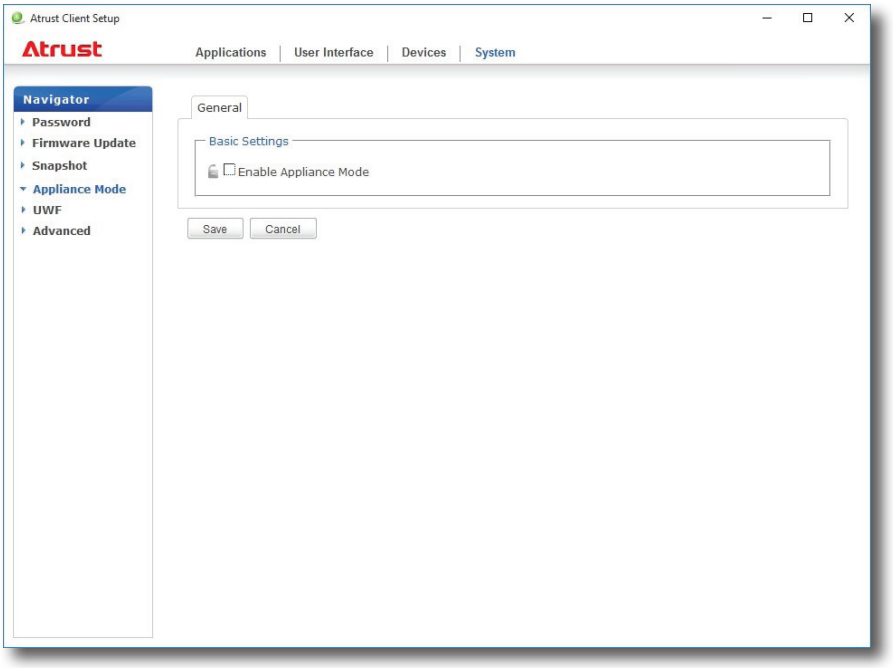
Enabling the Appliance Mode

To enable the Appliance mode, please do the following:

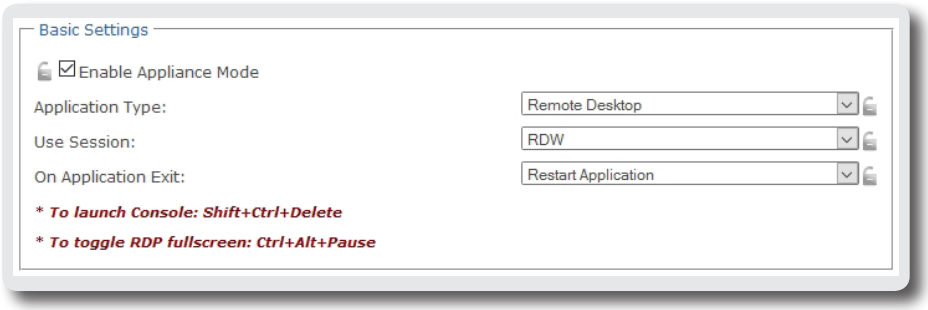
NOTE

- Ensure that you have configured the connection settings for the desired Microsoft Remote Desktop, Citrix ICA, VMware View or Horizon View 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:
  - ✧ "4.5.3 Configuring Basic RDP Connection Settings" on page 62
  - ✧ "4.5.6 Configuring Basic ICA Connection Settings" on page 87
  - ✧ "4.5.9 Configuring Basic VMware View Connection Settings" on page 110

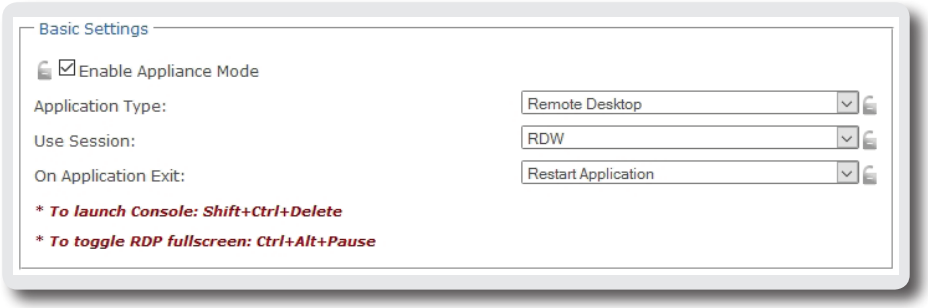
1. On Atrust Client Setup, click **System** > **Appliance Mode**.

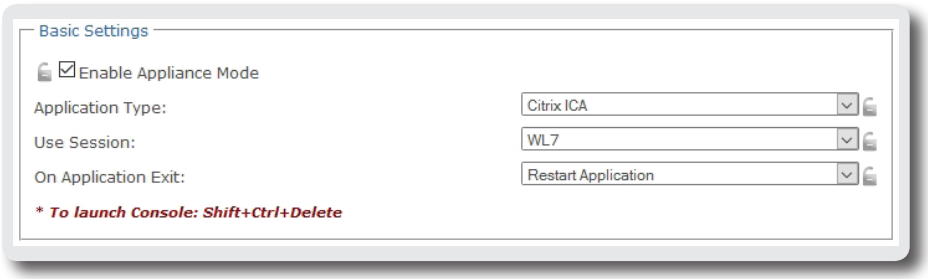


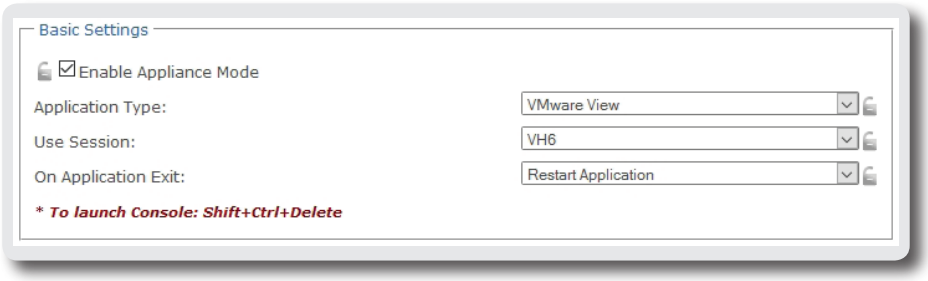
2. Click to check **Enable Appliance Mode**.
3. Other settings of the Appliance mode appear.



4. Click drop-down menus to select the application (or service) type: **Citrix ICA**, **Remote Desktop**, or **VMware View**, and the specific service available in that type.







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

NOTE

- To disable the Appliance mode or to access Atrust Client Setup under the Appliance mode, please refer to "Disabling the Appliance Mode" on page 50.

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 session, 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 + Pause**.
   - To exit the Full Screen mode of the ICA session, use the XenDesktop toolbar at the top (You may not in the Full Screen mode).
   - To release the keyboard and mouse from the View session (virtual desktop), press **Ctrl + Alt**.

   NOTE

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

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

   NOTE

   - You cannot access the local desktop 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 session:

   - To return to the current RDP / ICA session, use **Alt + Tab** (press and hold **Alt**, and then press **Tab** to switch between different items) to select and restore the current RDP / ICA session.
   - To return to the current View session, click any place of the View session (virtual desktop) on the background.

6. Log off from the current RDP / ICA / View session.
7. The client might shut down then. Restart your client manually.

4.2.10 Configuring UWF (Unified Write Filter)

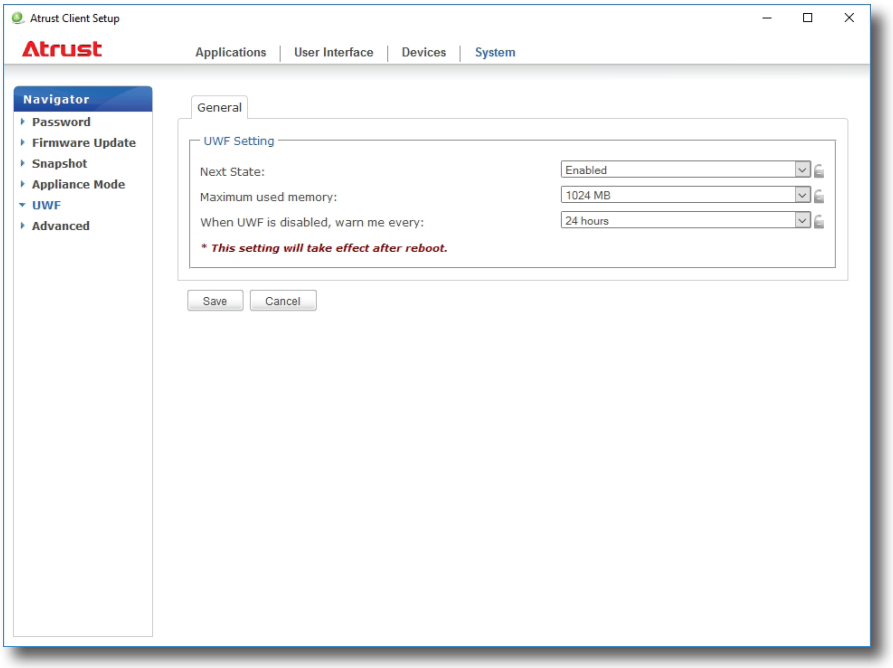
Your mt178W is UWF-enabled by default. Unified Write Filter (UWF) is a sector-based write filter intercepting all write attempts to a protected volume and redirecting those write attempts to a RAM cache. With UWF, all system changes will only affect the session where the changes are made. After restart, all changes will be discarded.

WARNING

- The UWF feature is enabled by factory default. ***Except for changes to ACS settings***, all the changes made in a session will not be kept after the system restart. Ensure that you choose the desired settings here before making any changes to the system.
- An icon in the Notification area of the Taskbar will indicate the current UWF state of your system. For details, please refer to the description at the end of this section.

To configure the UWF settings, please do the following:

1. On Atrust Client Setup, click **System** > **UWF**.
2. Click the State drop-down menu to enable/disable the UWF feature.



3. Click to select other options if needed.

UWF Options	
Item	**Description**
Next State	Click to enable / disable UWF. A restart is required for switching.
Maximum used memory	Click to select the maximum memory used for UWF.
When UWF is disabled, warn me every	Click to select how often the system warns you when UWF is disabled.

4. Click **Save** to confirm your selections.
5. You may need to restart the system for the change(s) to take effect.

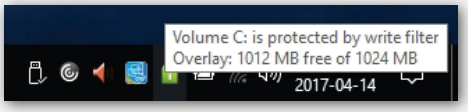
WARNING

- You need to restart the system for switching between the UWF enabled and disabled states. An icon will appear in the Notification area of the Taskbar to indicate the current UWF state of the system. The following table provides a description of each icon:

Icon	Name	Description
	Green Lock	The UWF is currently enabled. Except for changes to ACS settings, all the other changes made to the system in current session will not be kept after the system restart.
	Orange Lock	The UWF state was changed and will take effect after the system restart.
	Red Lock	The UWF is currently disabled.

TIP

- When UWF is enabled, you can move the mouse pointer over the UWF icon to check currently free memory (overlay) for UWF. A tooltip as below will be shown.



NOTE

- As a thin client device, your mt178W is mainly for access to remote or virtual desktops on servers. With the limited and protected (UWF-enabled) hard disk space, it's ***not*** recommended to save data on your mt178W. Instead, you can use storage spaces over remote / virtual desktops, removable storage devices, or networks.
- In case that you need to copy a file to the protected volume, ensure that its size is smaller than the free memory (overlay) space. Otherwise, your system may have unexpected results or become unresponsive.

4.2.11 Enabling or Disabling Auto Registration

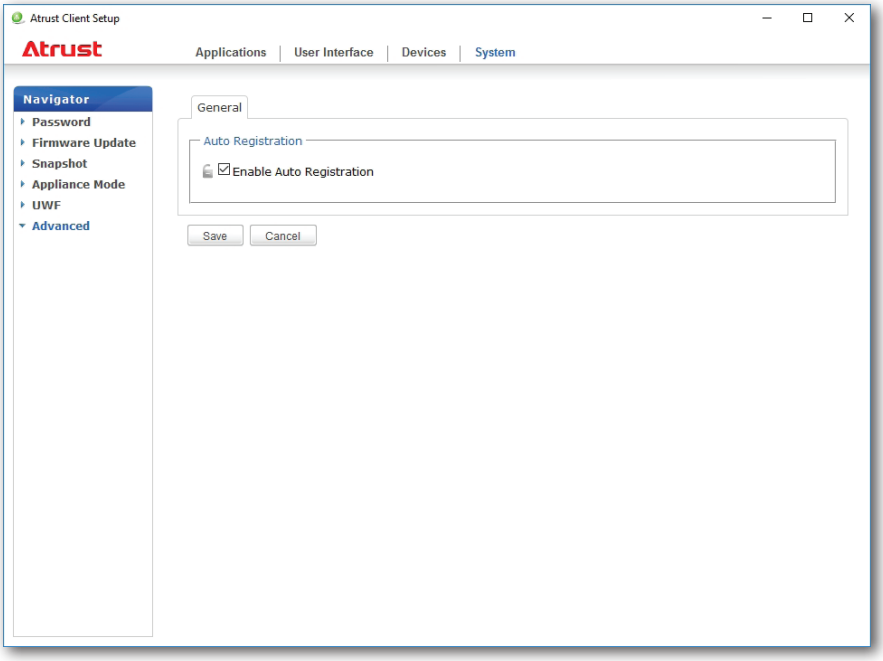
Auto Registration allows that thin clients automatically register with Atrust Device Manager when they are online and then become managed by Atrust Device Manager.

NOTE

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

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

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



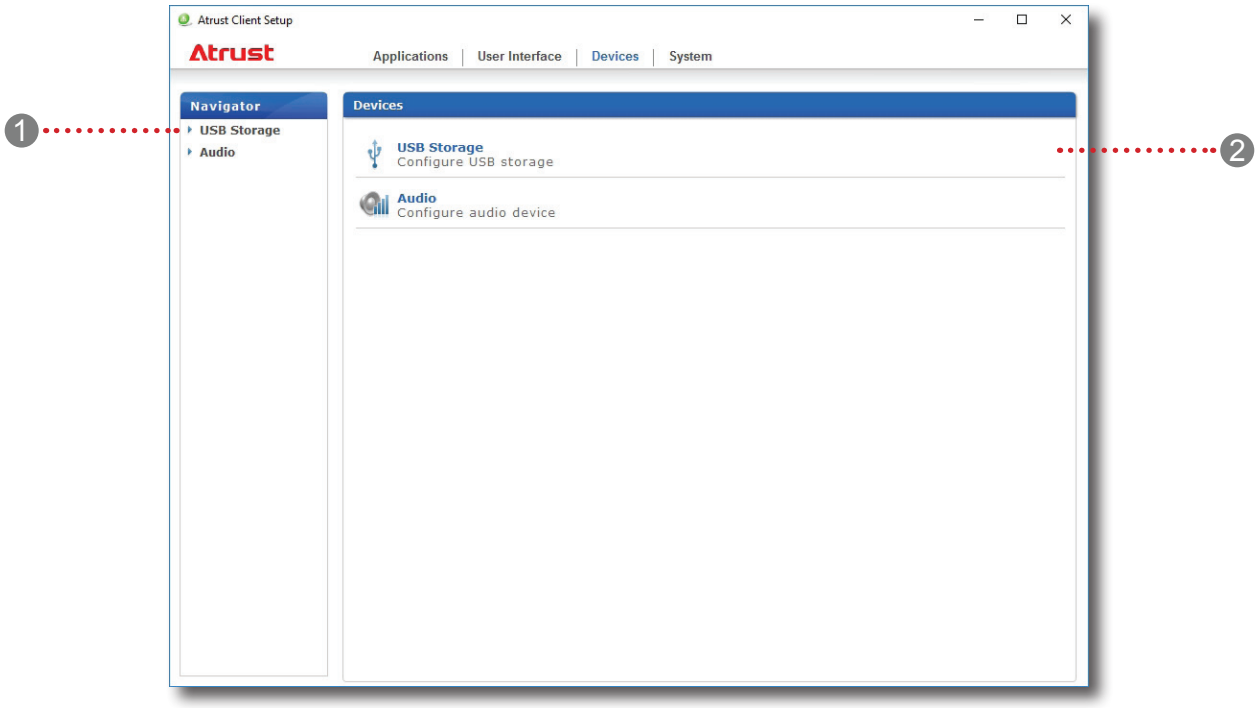
3. Click **Save** to apply.

4.3 Configuring External Device Settings

4.3.1 Devices Tab Overview

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

Devices Tab Overview



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

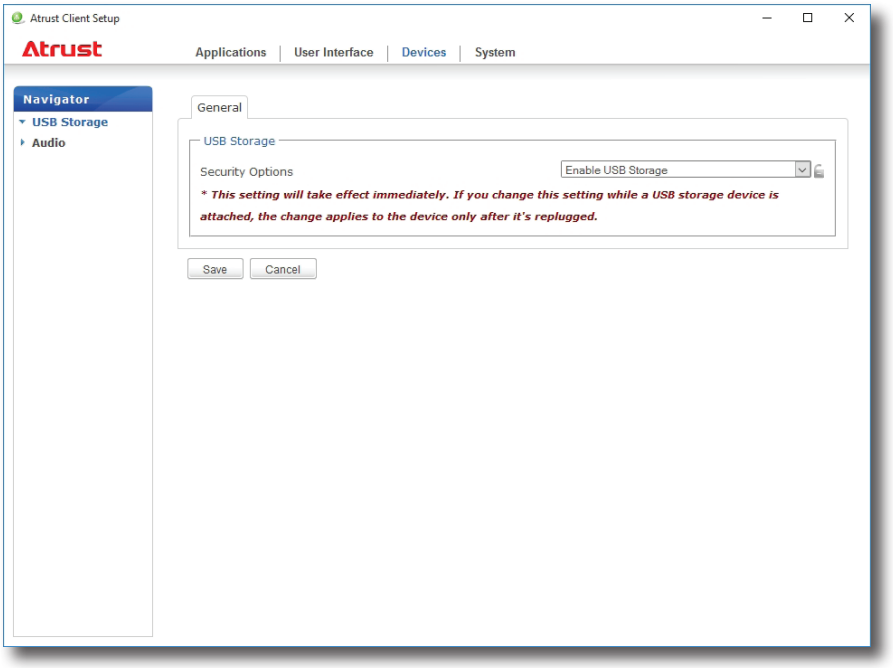
4.3.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
Devices	USB Storage		Click to configure settings for USB storage devices.	4.3.3	55
	Audio		Click to configure settings for audio devices.	4.3.4	56

4.3.3 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**.



2. Click the drop-down menu to select the desired setting. Three options are available: **Enable USB Storage**, **Read-Only Access**, and **Disable USB Storage**.

NOTE

- When **Enable USB Storage** is selected, settings of RDP / ICA connection entries under **Applications** tab may affect if you can use ***mapped*** USB storage devices in remote / virtual desktop sessions. For details, please refer to sections:
  - ✧ "4.5.5 Configuring Advanced RDP Connection Settings" on page 74
  - ✧ "4.5.8 Configuring Advanced ICA Connection Settings" on page 99
- When **Disable USB Storage** is selected, Citrix ICA and VMware View / Horizon View sessions may still allow users to use locally attached USB storage devices through ***redirection***. To really prevent the use of USB storage devices in virtual desktop sessions, some configurations in Citrix and VMware service delivery environments are required.

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

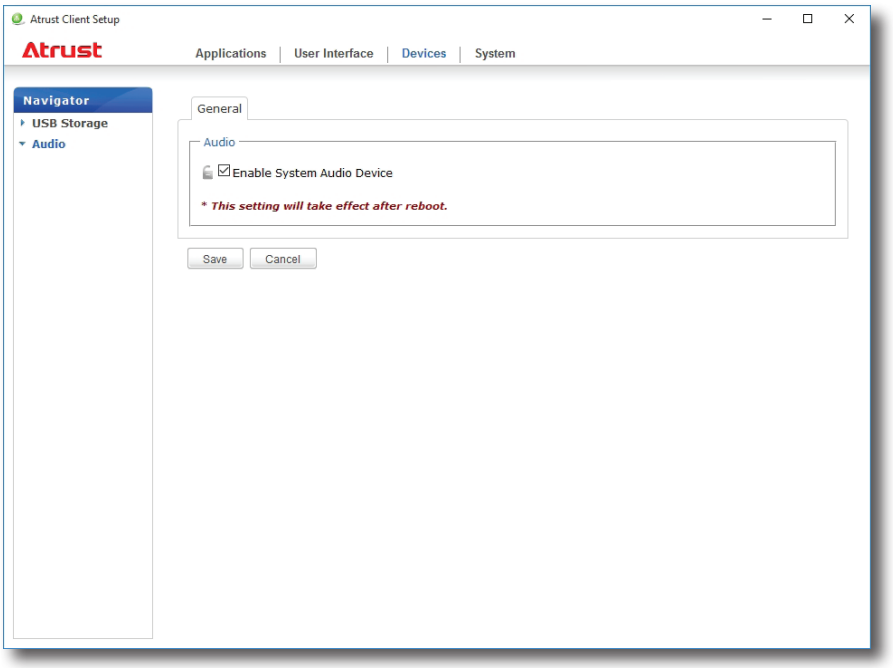
4.3.4 Disabling or Enabling Attached Audio Devices

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

NOTE

- If you disable locally attached audio devices, client users are not allowed to perform audio playback or recording with these devices in an RDP / ICA / View session.
- To perform audio playback or recording with local audio devices in an RDP / ICA / View session, you need to enable locally attached audio devices here (the **Audio** setting item under **Devices** tab) and configure audio related settings (if any) in the RDP / ICA / View connection settings. For detailed instructions, please refer to sections:
  - ✧ "4.5.5 Configuring Advanced RDP Connection Settings" on page 74
  - ✧ "4.5.8 Configuring Advanced ICA Connection Settings" on page 99
  - ✧ "4.5.11 Configuring Advanced View Connection Settings" on page 114

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



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

NOTE

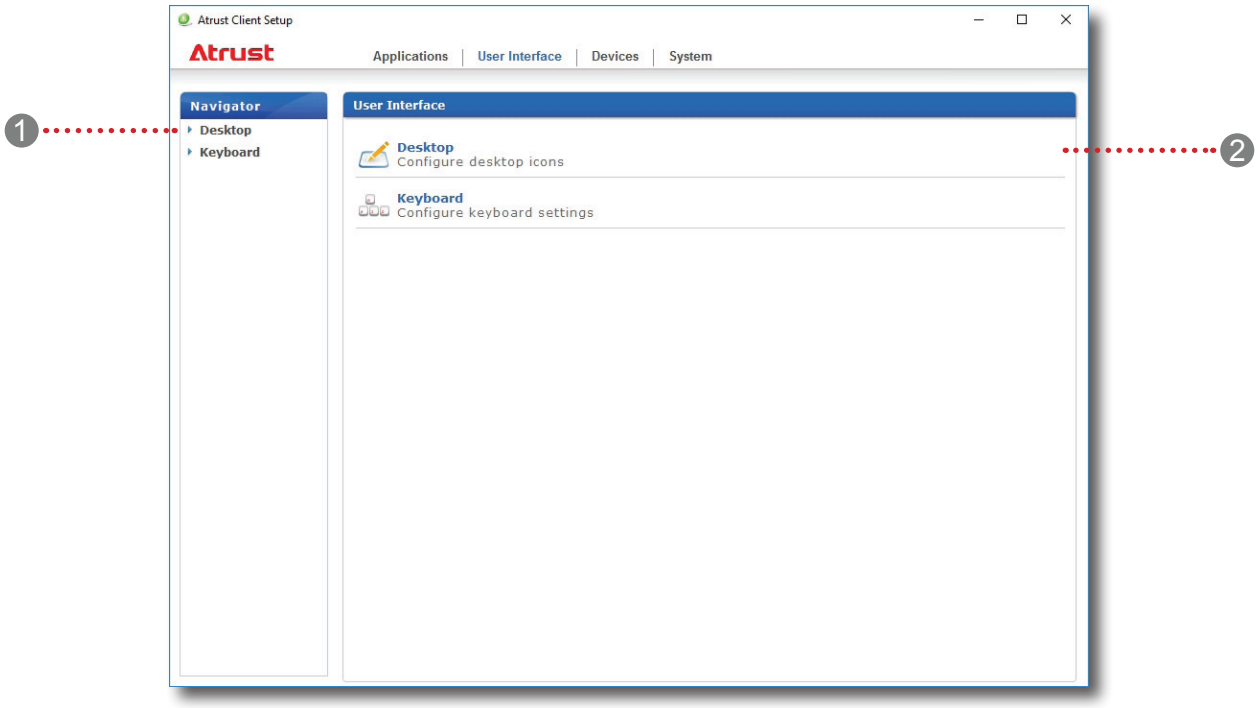
- The change will not take effect until the client has been restarted.

4.4 Configuring User Interface Settings

4.4.1 User Interface Tab Overview

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

User Interface Tab Overview



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

4.4.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
User Interface	Desktop		Click to configure the display of standard desktop shortcuts for quick service access.	4.4.3	58
	Keyboard		Click to configure the Num Lock mode.	4.4.4	31

4.4.3 Configuring the Display of Standard Desktop Shortcuts for Quick Access

The **Desktop** setting enables you to display or hide the standard desktop shortcuts for service quick access. Three standard desktop shortcuts are available: **Citrix Receiver**, **Remote Desktop Connection**, and **VMware Horizon View Client**, separately for quick service access of Citrix XenApp / XenDesktop / VDI-in-a-Box, Microsoft Remote Desktop / Remote Application (RemoteApp), and VMware View / VMware Horizon View.

Remote Desktop Connection

Citrix Receiver

VMware Horizon View Client

TIP

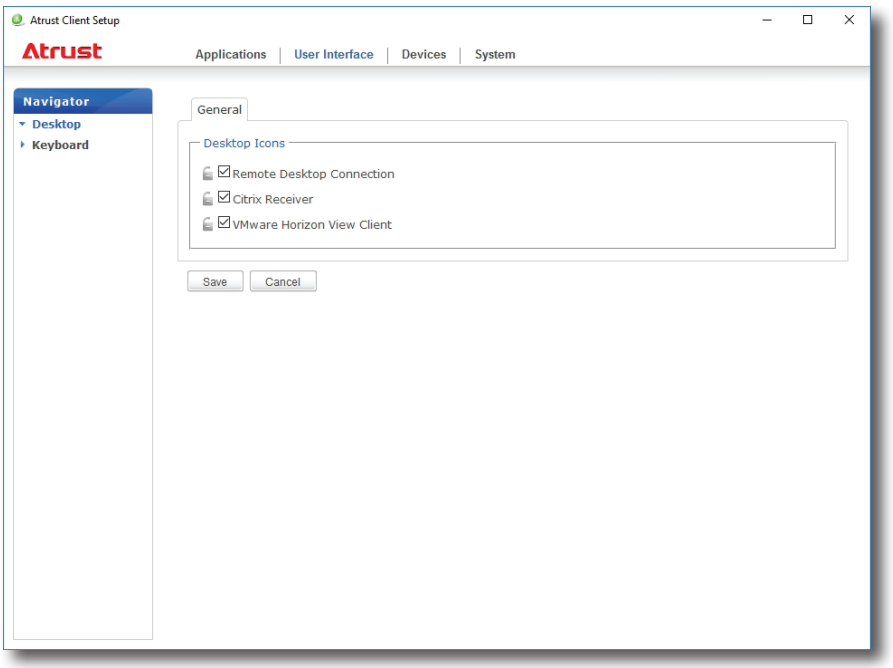
- You can use these standard desktop shortcuts to quickly access services.
  For detailed instructions, please refer to chapter 3 "Getting Started" on page 15.

NOTE

- You can also customize your desktop shortcuts for quick service access. For detailed instructions on how to create and customize your own desktop shortcuts, please refer to section "4.5 Configuring Service Access Settings" on page 60.

To display or hide the standard desktop shortcuts for quick service access, please do the following:

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

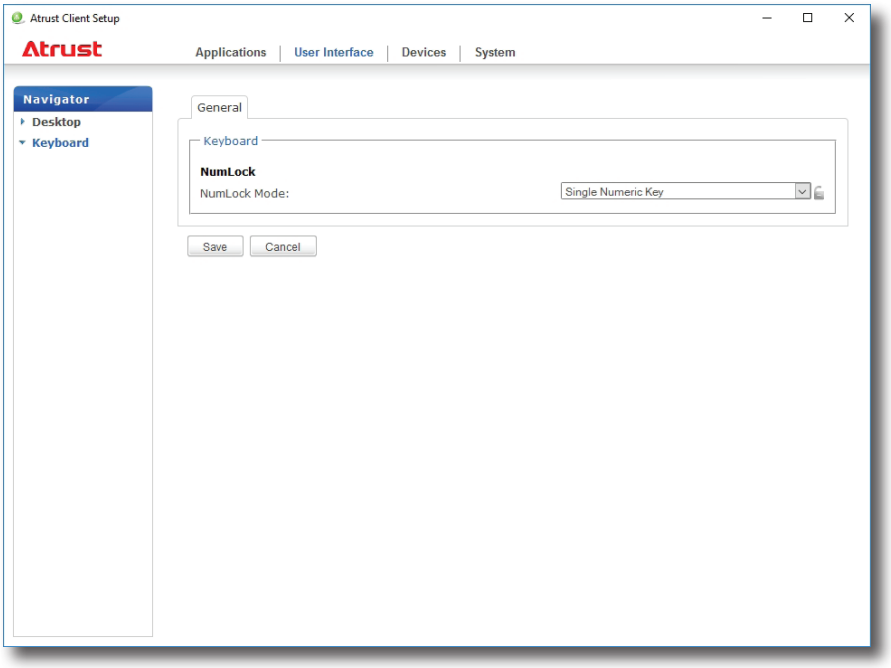


2. Click to check/uncheck **Remote Desktop Connection**, **Citrix Receiver**, or **VMware Horizon View Client**.
3. Click **Save** to apply.

4.4.4 Configuring the Num Lock Mode

To configure the Num Lock mode, please do the following:

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



2. Click the drop-down menu to configure the Num Lock mode. Two options are available: **Single Numeric Key** or **Fn + Numeric Key**.

Keyboard		
Item		**Description**
NumLock Mode	Single Numeric Key	In NumLock mode, single numeric key is sufficient to enter a number.
	Fn + Numeric Key	In NumLock mode, Fn plus numeric key is required to enter a number.

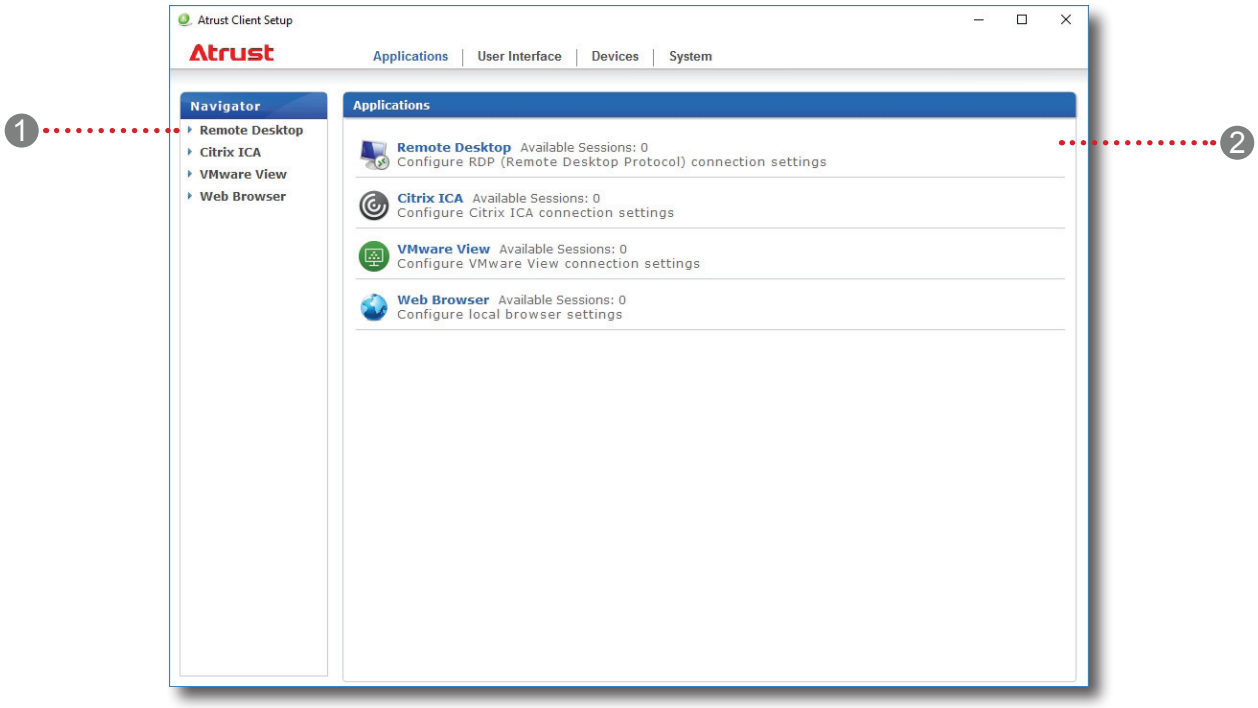
3. Click **Save** to apply.

4.5 Configuring Service Access Settings

4.5.1 Applications Tab Overview

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

Applications Tab Overview



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

4.5.2 Available Settings at a Glance

Tab	Setting	Icon	Description	Section	Page
Applications	Remote Desktop		Click to configure RDP (Remote Desktop Protocol) connection settings and create access shortcuts on the desktop for RDP sessions.	4.5.3 4.5.4 4.5.5	62 69 74
	Citrix ICA		Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create access shortcuts on the desktop for ICA sessions.	4.5.6 4.5.7 4.5.8	87 95 99
	VMware View		Click to configure VMware View connection settings and create access shortcuts on the desktop for View sessions.	4.5.9 4.5.10 4.5.11	110 112 114
	Web Browser		Click to configure browser session settings and create access shortcuts on the desktop for browser sessions.	4.5.12	116

4.5.3 Configuring Basic RDP Connection Settings

The **Remote Desktop** setting allows you to configure RDP (Remote Desktop Protocol) connection settings and create shortcuts on the desktop or Start screen for Remote Desktop services. You can access services for work simply through these shortcuts.

NOTE

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

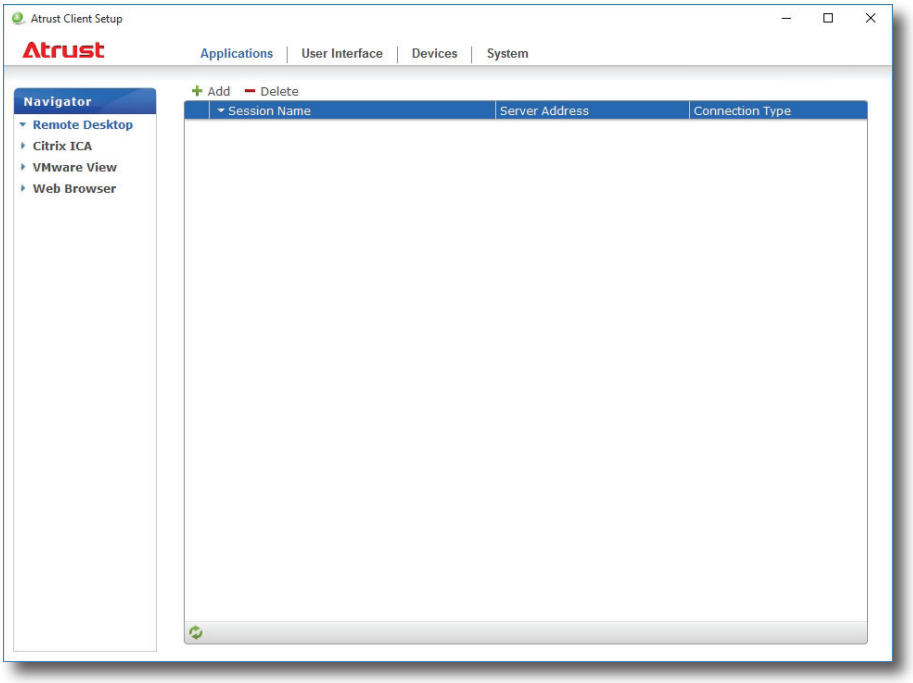
Three connection types are available:

Connection Type	Description	Page
Remote Desktop	Select to access remote desktops/applications.	63
Remote Web Access	Select to access remote desktops/applications through a Web browser.	65
Web Feed	Select to access remote applications through published Start screen tiles.	67

Connection Type: Remote Desktop

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

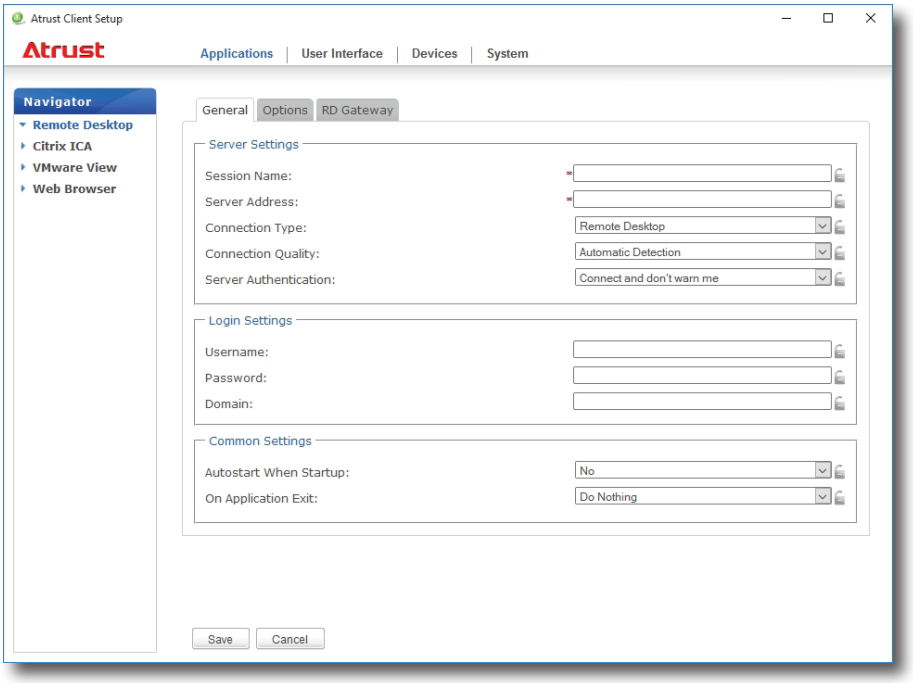
1. On Atrust Client Setup, click **Applications** > **Remote Desktop**.



2. The RDP Connection list appears in the Configuration area.

> **NOTE**
>
> - If you haven't create any entry, the RDP Connection list will be empty.

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



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

NOTE

- The red asterisks indicate the required fields.
- The remote 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.

5. Click **Save** to add this RDP connection entry.
6. The shortcut for Remote Desktop connection is automatically created on the desktop.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced RDP connection settings for service access. For more information on other available settings, please refer to section "4.5.5 Configuring Advanced RDP Connection Settings" on page 74.

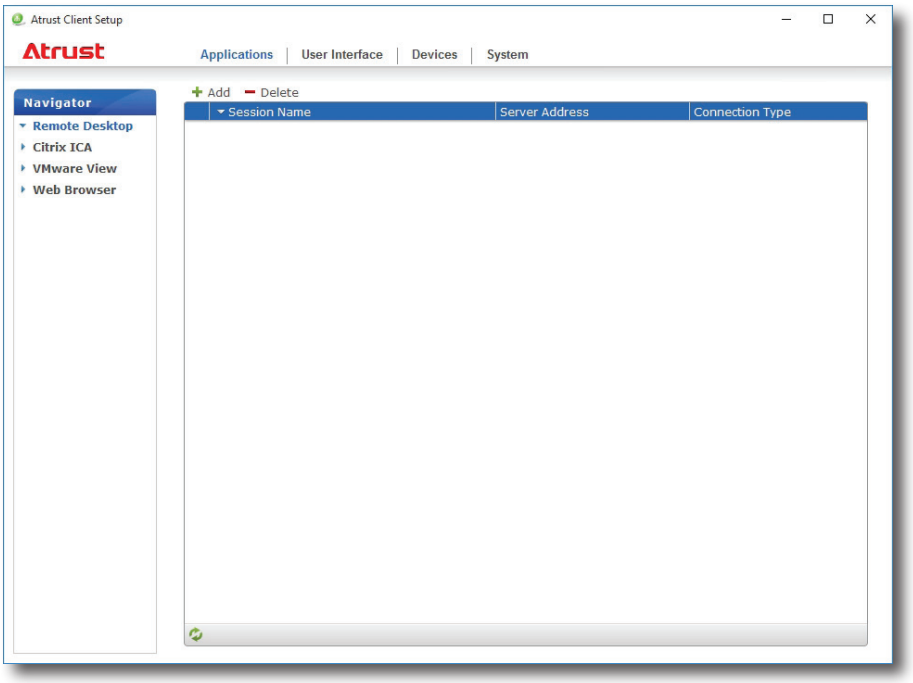
Connection Type: Remote Web Access

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

NOTE

- Your mt178W supports only RD Web Access based on Windows Server 2012 R2; Windows Server 2008 R2 based is not supported.

1. On Atrust Client Setup, click **Applications** > **Remote Desktop**.

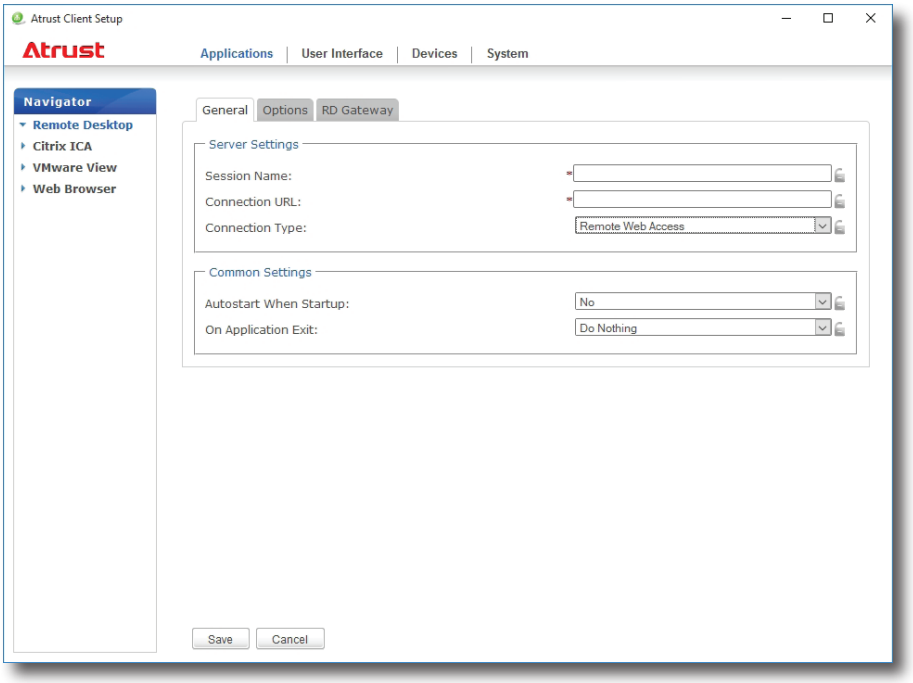


2. The RDP Connection list appears in the Configuration area.

NOTE

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

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



4. On **General** sub-tab, click the Connection Type drop-down menu to select **Remote Web Access**.
5. Type in the session name and connection URL through which Web-based remote applications/desktops is accessible.

NOTE

- The red asterisks indicate the required fields.
- Consult your IT administrator for the appropriate connection URL.

6. Click **Save** to add this RDP connection entry.
7. The shortcut for Remote Web Access connection is automatically created on the desktop.

NOTE

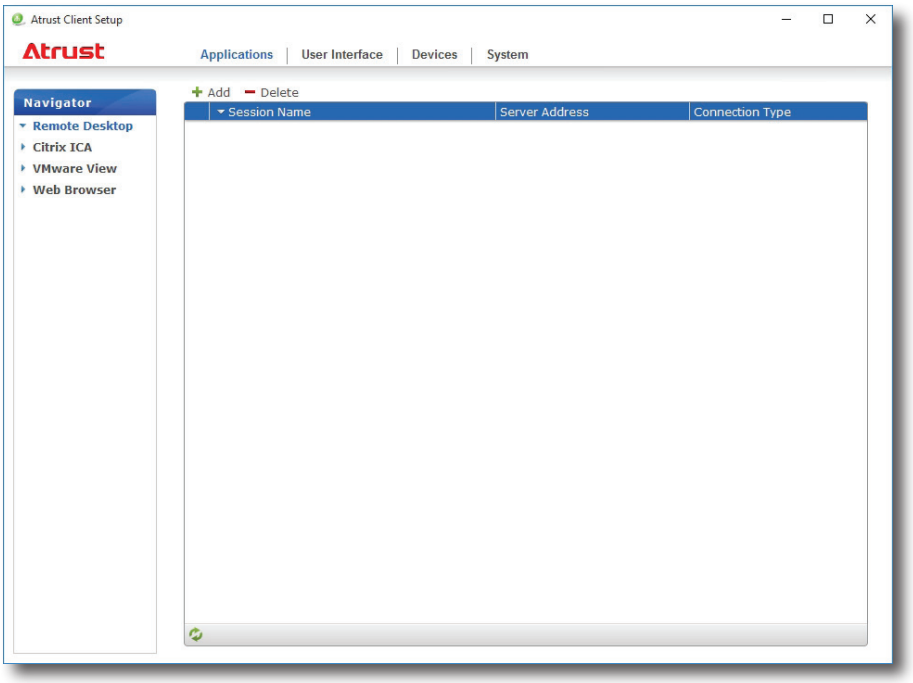
- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced RDP connection settings for service access. For more information on other available settings, please refer to section "4.5.5 Configuring Advanced RDP Connection Settings" on page 74.

Connection Type: Web Feed

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

> **NOTE**
>
> - Your mt178W supports only RD Web Feed based on Windows Server 2012 R2; Windows Server 2008 R2 based is not supported.

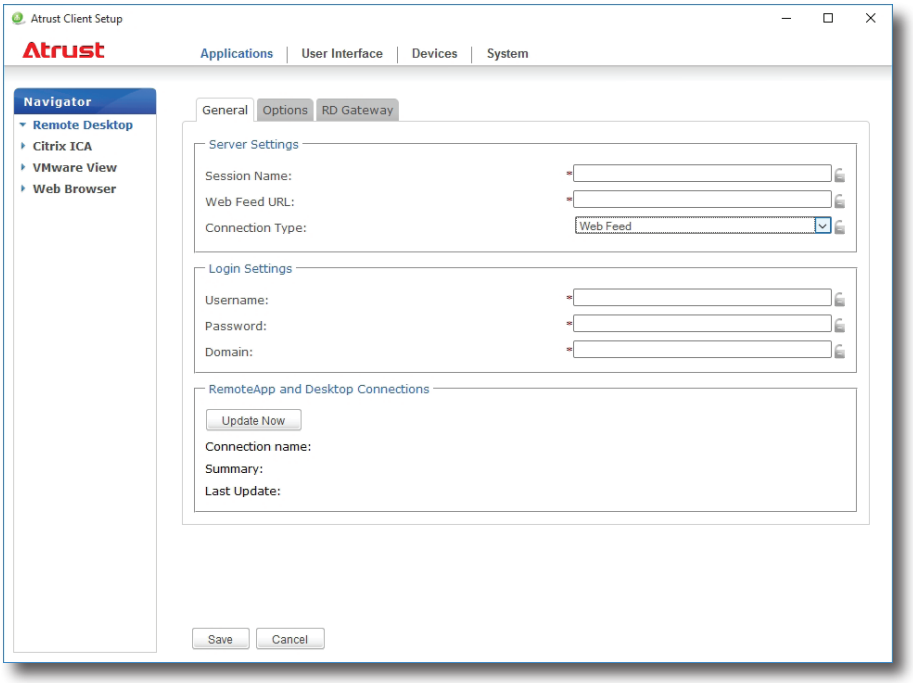
1. On Atrust Client Setup, click **Applications** > **Remote Desktop**.



2. The RDP Connection list appears in the Configuration area.

> **NOTE**
>
> - If you haven't create any entry, the RDP Connection list will be empty.

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



4. On **General** sub-tab, click the Connection Type drop-down menu to select **Web Feed**.
5. Type in the session name, the Web Feed URL through which remote applications is accessible, and your credentials for Web Feed.

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

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

7. Click **Save** to add this RDP connection entry.
8. The application tiles for Web Feed are automatically created on the Start screen.

> **NOTE**
>
> - Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced RDP connection settings for service access. For more information on other available settings, please refer to section "4.5.5 Configuring Advanced RDP Connection Settings" on page 74.

4.5.4 Accessing Remote Desktop Services

Connection Type: Remote Desktop

To access Remote Desktop services, please do the following:

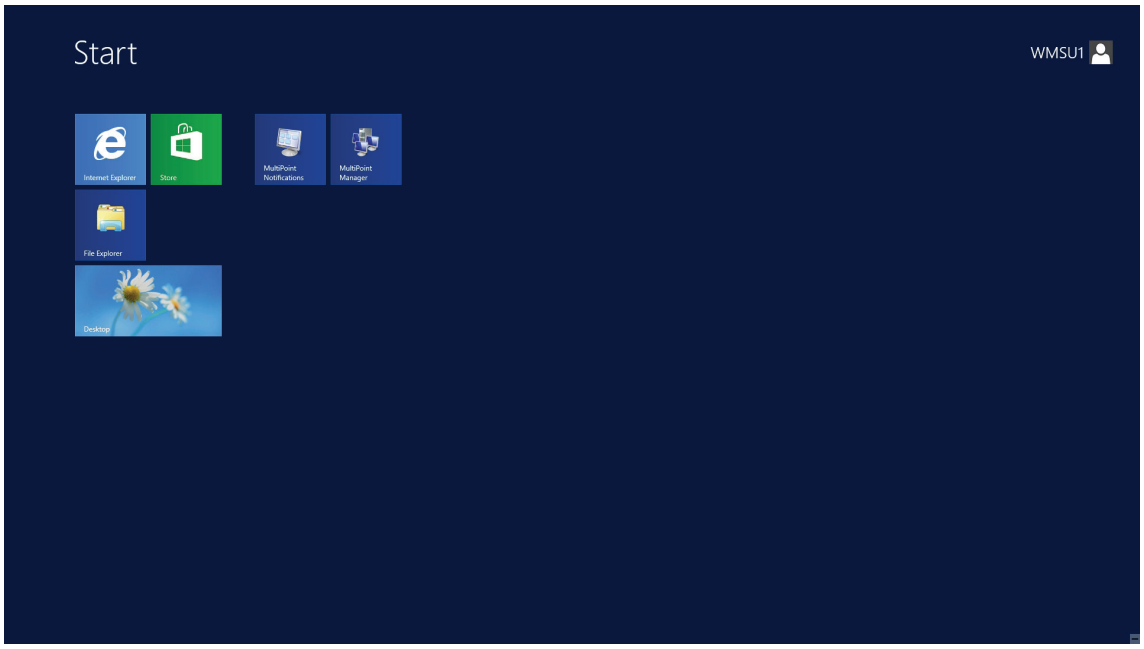
1. Double click the created (customized) shortcut on the desktop.

> **NOTE**
>
> - You can also access Remote Desktop services through the standard desktop shortcut **Remote Desktop Connection**. For detailed instructions on how to access services via this standard shortcut, please refer to section "3.3 Accessing Microsoft Remote Desktop Services" on page 24.

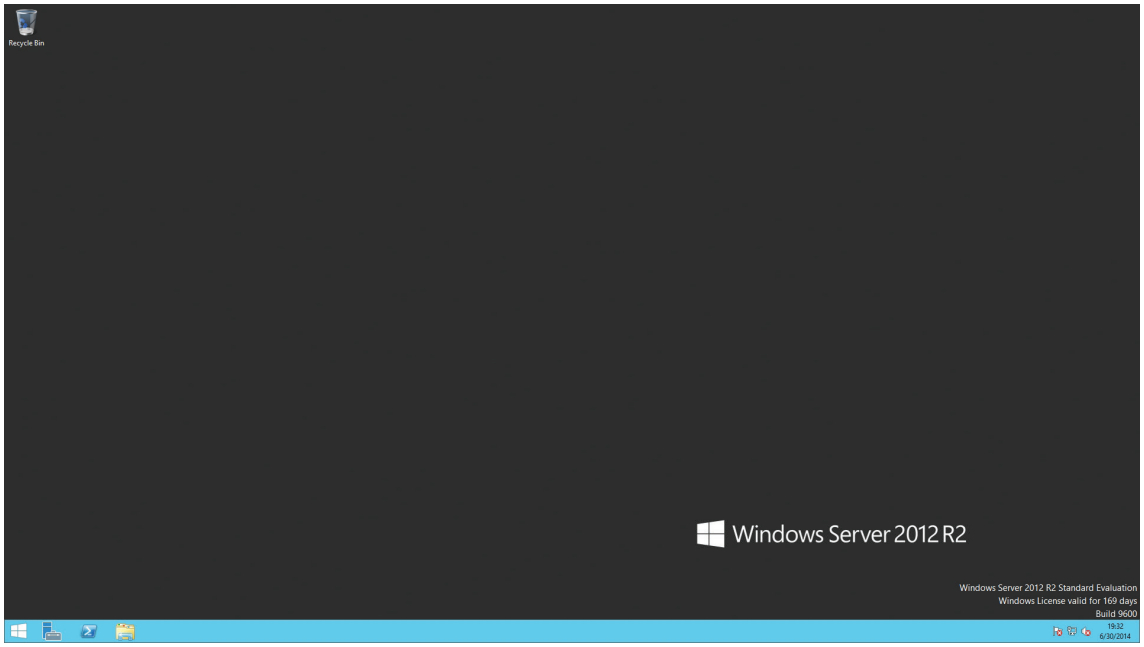
2. Follow the on-screen instructions and provide required credentials if needed.
3. The desired remote desktop will be displayed on the desktop in full screen (by default).

> **NOTE**
>
> - The connection type of Remote Desktop also allows you to launch ***application-only*** sessions; only a specific application is launched rather than a full desktop. For details, please refer to "4.5.5 Configuring Advanced RDP Connection Settings" on page 74.

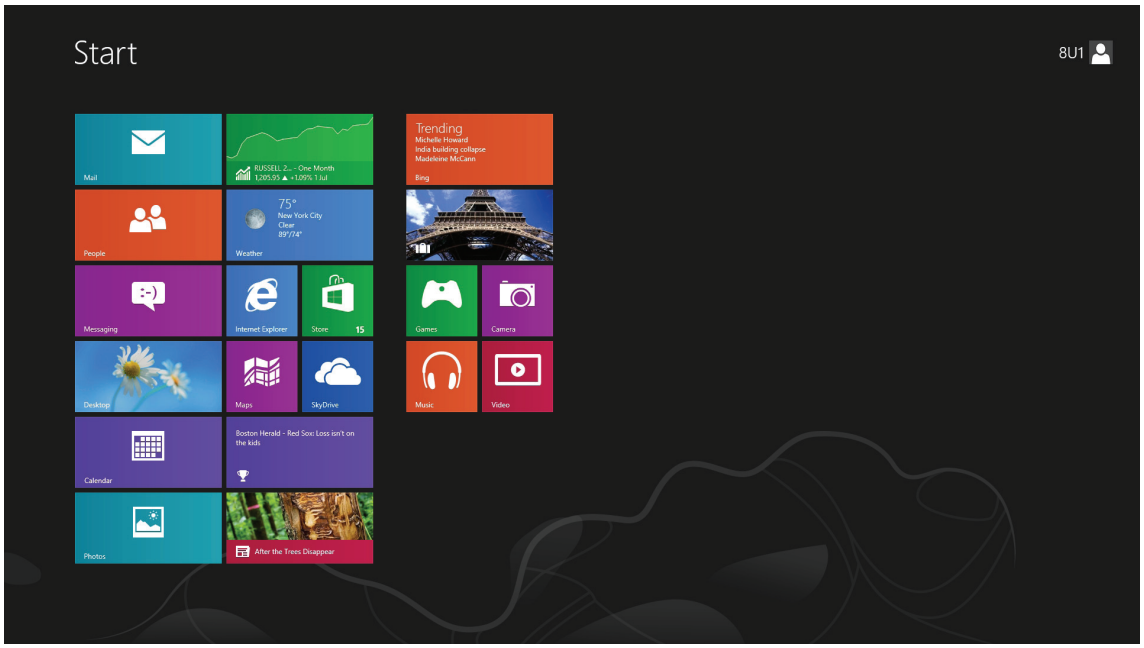
Example: Windows MultiPoint Server 2012



Example: Windows Server 2012



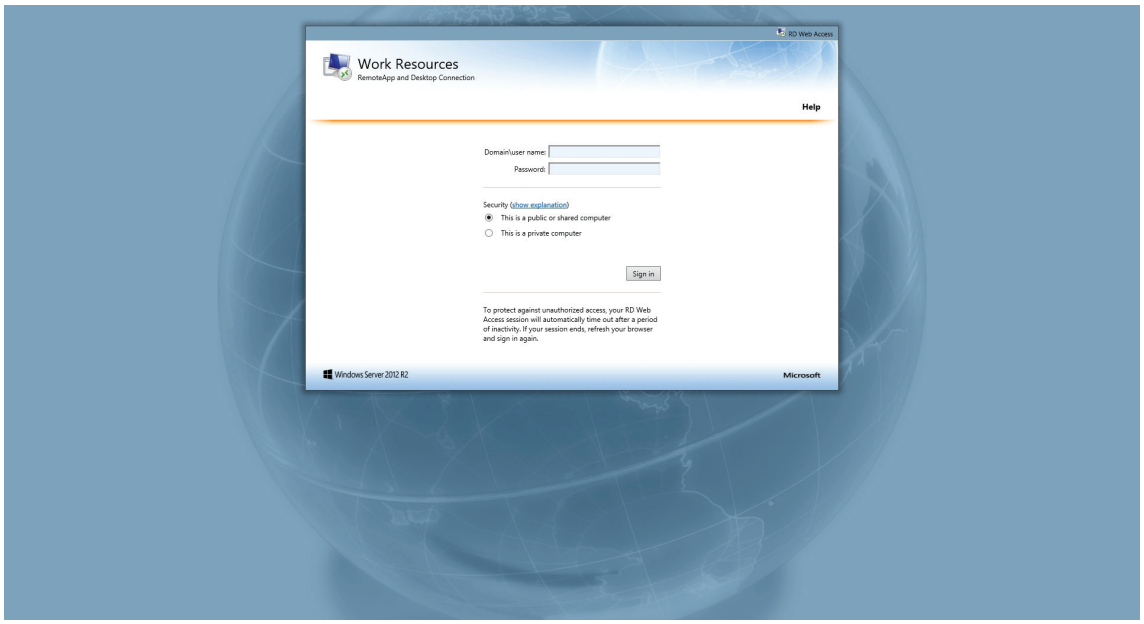
Example: Windows 8 Enterprise



Connection Type: Remote Web Access

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

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

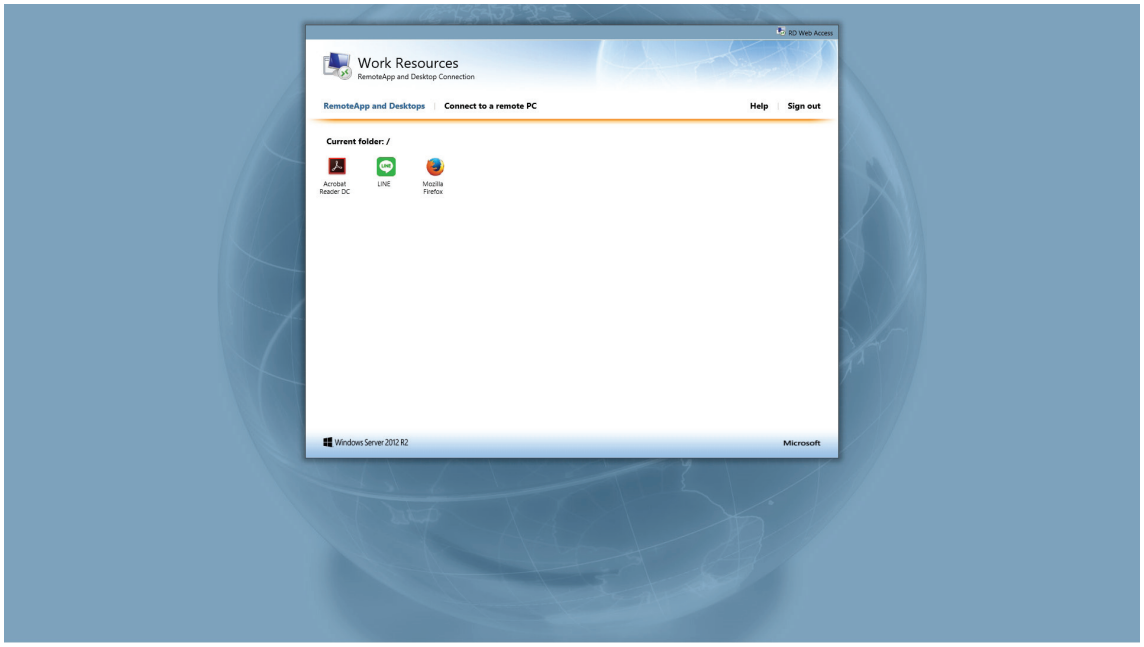


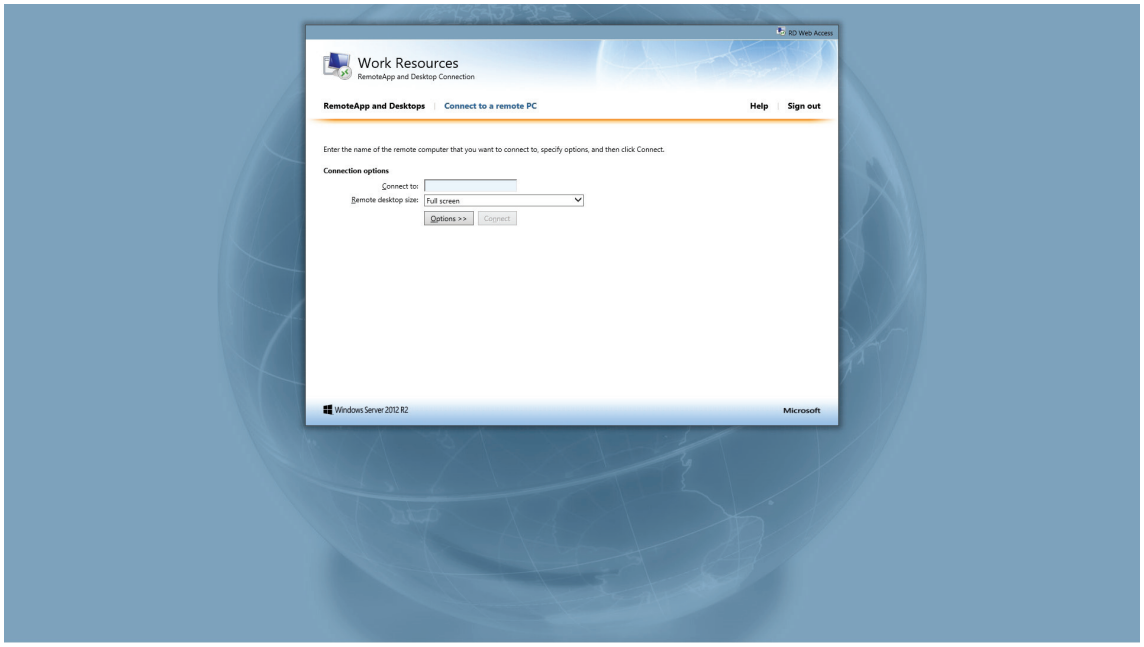
NOTE

- A warning message about security might appear. Consult your IT administrator for details and ensure the connection is secure ***first***. To by pass, click **Continue to this website**.
- Click to select **Allow** to enable ActiveX Control when a popup message appears at the bottom of the page.

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

4. Click to select **RemoteApp and Desktops** or **Connect to a remote PC**.



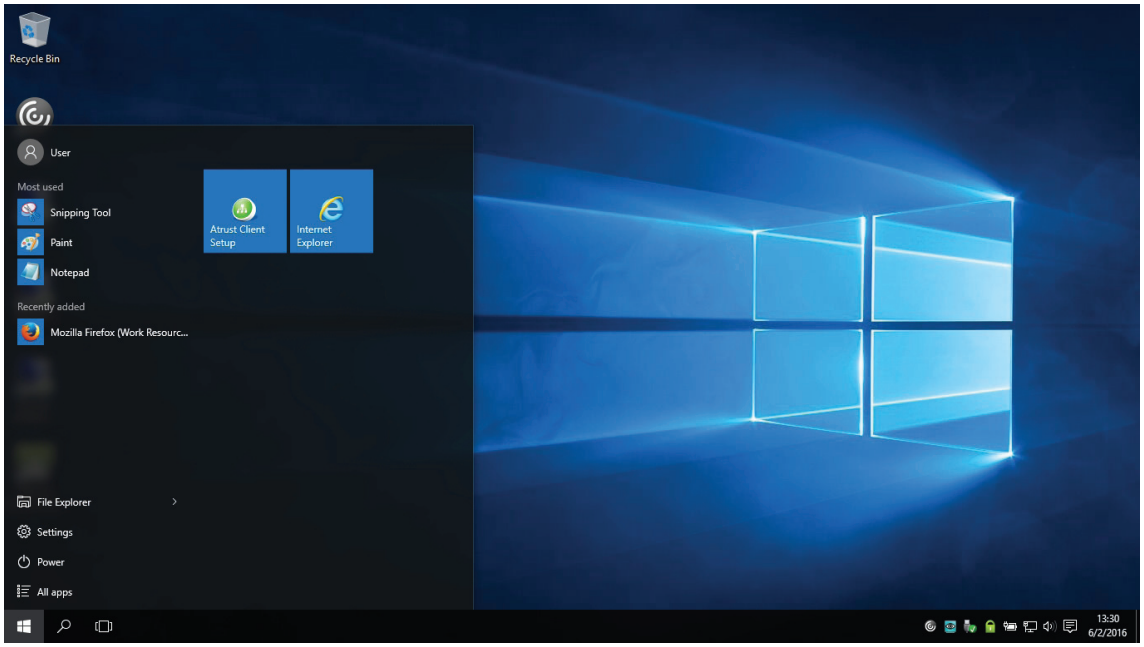


5. Click icons or follow the on-screen instructions to launch applications or desktops.

Connection Type: Web Feed

To access remote applications, please do the following:

1. On Start screen, click **All apps**.



2. Click to launch the desired application.

4.5.5 Configuring Advanced RDP Connection Settings

The table below provides a description of each setting item for RDP connections. Please see this table to configure advanced settings and customize your mt178W desktop shortcuts or Start screen tiles for service access.

NOTE

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

Settings for the Connection Type of Remote Desktop

NOTE

- For descriptions of settings for the connection type of Remote Web Access, please refer to "Settings for the Connection Type of Remote Web Access" on page 81.
- For descriptions of settings for the connection type of Web Feed, please refer to "Settings for the Connection Type of Web Feed" on page 83.

General Sub-tab

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

Three connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Remote Desktop</td><td>Provides access to remote desktops/applications.</td></tr><tr><td>Remote Web Access</td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr><tr><td>Web Feed</td><td>Provides access to remote applications through published Start screen tiles.</td></tr></table></td></tr>
<tr><td>Connection Quality</td><td>Select the setting that best describes the quality of your network connection. Three options are available: Very Fast (LAN), Fast (Broadband), Slow (Modem), and Automatic Detection.</td></tr>
</table>

<table>
<tr><td>Server Authentication</td><td>Select what to do next if the client cannot verify the identity of the remote computer. Three options are available: Connect and don’t warn me, Warn me, and Do not connect.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Connect and don’t warn me</td><td>Connects anyway without any warning.</td></tr><tr><td>Warn me</td><td>Warns and allows users to choose whether to connect or not.</td></tr><tr><td>Do not connect</td><td>Disallows the connection.</td></tr></table></td></tr>
<tr><td colspan="2">Login Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.

NOTE: Leave this field blank if the server doesn’t belong to any domain.</td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a Remote Desktop session automatically or not when Windows 10 IoT Enterprise starts.

If Yes is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.</td></tr>
<tr><td>On Application Exit</td><td>Select what to do when a Remote Desktop session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.
<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Windows 10 IoT Enterprise desktop.</td></tr><tr><td>Restart Application</td><td>Opens a Remote Desktop session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
</table>

Options Sub-tab

<table>
<tr><th colspan="2">Programs</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Start the following program on connection</td><td>Click the drop-down menu to enable/disable the Application mode. You can 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 application hosted server. For detailed instructions on how to add a desired application to the RemoteApp Programs list on the server, please visit Microsoft Support website at support.microsoft.com.</td></tr>
<tr><td>Start in the following folder</td><td>Type in the location of the desired application (on the host server) if Start the following program on connection is enabled.

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

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

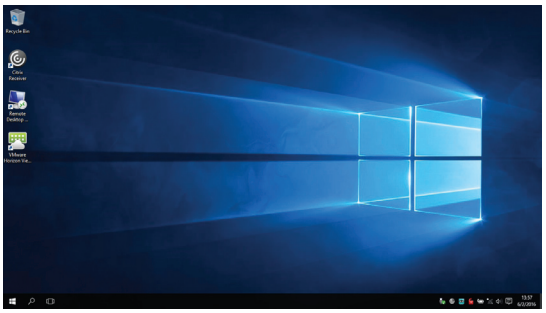
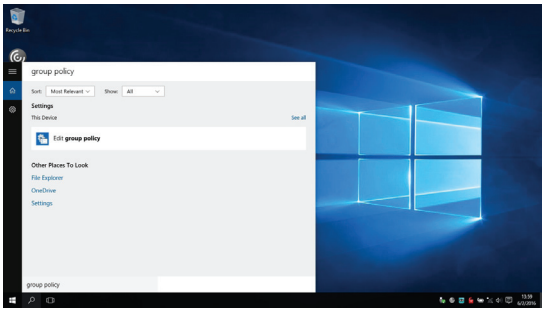
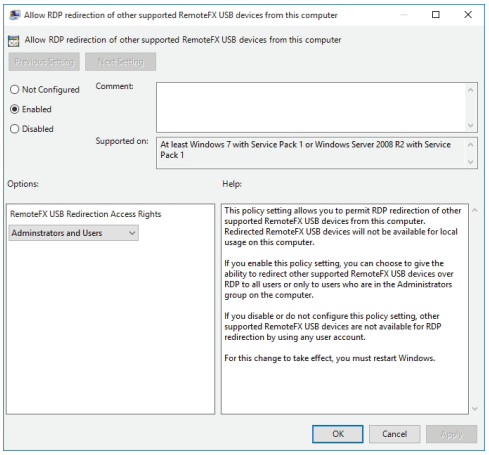
NOTE: You can configure the upper limit of the color depth for a Remote Desktop session on the host server. In this case, no matter which color depth you choose here, the value cannot exceed the defined limit.</td></tr>
<tr><td>Resolution</td><td>Click the drop-down menu to select the desired display resolution on a Remote Desktop session. Twelve options are available: Fullscreen, 1920x1200, 1920x1080, 1680x1050, 1400x1050, 1440x900, 1280x1024, 1280x768, 1280x720, 1024x768, 800x600, and 640x480.</td></tr>
</table>

Multi-Monitor	Click the drop-down menu to enable/disable multiple displays in a Remote Desktop session.
Display the connection bar when I use the full screen	Click the drop-down menu to select if the Connection bar is displayed or not in full-screen mode.
Connection Settings	
Item	**Description**
Printer Mapping	Click the drop-down menu to enable/disable printer mapping. When **Enable** is selected, users can access a local or network printer in a Remote Desktop session. **NOTE:** You need to add the desired local or network printer(s) for your thin client first, and then enable this feature here to use that printer in a Remote Desktop session. **NOTE:** To add a local or network printer for your Windows 10 IoT Enterprise-based thin client, go to Control Panel, click **Hardware and Sound** > **Devices and Printers** > **Add a printer**, and then follow the on-screen instructions to add the desired local or network printer.
Clipboard Redirection	Click the drop-down menu to enable/disable Clipboard redirection. **NOTE:** When **Enable** is selected, Clipboard can be used across local and remote desktops (in both directions).
Smart Card Mapping	Click the drop-down menu to enable/disable smart card mapping. When **Enable** is selected, users can access smart cards through a smart card reader in a Remote Desktop session.
Port Mapping	Click the drop-down menu to enable/disable port mapping. When **Enable** is selected, users can access attached devices using locally available ports, in a Remote Desktop session. **NOTE:** The types and availability of device ports on thin clients may vary, depending on your product models.
Local Resources Settings	
Item	**Description**
Remote Audio Playback	Click the drop-down menu to configure the computer sounds and audio playback setting in a Remote Desktop session. Three options are available: **Bring to this computer**, **Do not play**, and **Leave at remote computer**.

Option	Description
Bring to this computer	Allows computer sounds and audio playback in a Remote Desktop session using locally attached audio devices.
Do not play	Disables computer sounds and audio playback in a Remote Desktop session.
Leave at remote computer	Leave computer sounds and audio playback at the remote computer.

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

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Recording from this computer</td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr><tr><td>Do not record</td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr></table>
NOTE: When Leave at remote computer is selected on the drop-down menu of Remote Audio Playback, this setting item will be grayed out.</td></tr>
<tr><td>Apply Windows key combinations</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On this computer, On the remote computer, Only when using the full screen.</td></tr>
<tr><td>Drives</td><td>Click the drop-down menu to enable/disable locally attached drives in a Remote Desktop session.</td></tr>
<tr><td>Supported plug and play devices</td><td>Click the drop-down menu to enable/disable the supported plug and play devices in a Remote Desktop session.</td></tr>
</table>

RemoteFX USB redirection	Click to enable/disable locally attached RemoteFX USB devices. **NOTE:** To use RemoteFX USB devices in remote desktops, you need to configure the policy setting about device redirection to allow RemoteFX USB Device Redirection as well. To do so, please follow the steps below: 1. Log in to your mt178W with an administrative account. 2. Disable UWF (Unified Write Filter) through Atrust Client Setup (See "4.2.10 Configuring UWF (Unified Write Filter)" on page 51). 3. On the ***desktop***, click in the bottom-left corner.  4. On the appeared Search window, type **group policy**, and then click to select **Edit group policy**.  5. On the opened window, select **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Connection Client** > **RemoteFX USB Device Redirection** > **Allow RDP redirection of other supported RemoteFX USB devices from this computer**. 6. Select **Enabled** and to which users this setting applies: **Administrators Only** or **Administrators and Users**, and then click **OK**.  7. Enable UWF through Atrust Client Setup.

RD Gateway Sub-tab

<table>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>RD Gateway Server Settings</td><td>Click the drop-down menu to choose if a RD Gateway server is used, automatically detected, or manually configured. Three options are available: Automatically detect RD Gateway server settings, Use these RD Gateway server settings, and Do not use an RD Gateway server.</td></tr>
<tr><td>Sever Name</td><td>Type the IP address / URL / FQDN of the RD Gateway server.

NOTE: Consult your network administrator for details.</td></tr>
<tr><td>Logon method</td><td>Click the drop-down menu to select the logon method. Three options are available: Allow me to select later, Ask for password (NTLM), and Smart card.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Allow me to select later</td><td>Users can select a logon method while connecting to the server.</td></tr><tr><td>Ask for password (NTLM)</td><td>Users will be prompted for a password while connecting to the server.</td></tr><tr><td>Smart card</td><td>Users will be prompted for a smart card while connecting to the server.</td></tr></table></td></tr>
<tr><td>Bypass RD Gateway server for local addresses</td><td>Check to prevent traffic to and from local network addresses from being routed through the RD Gateway server and make a connection faster.</td></tr>
<tr><th colspan="2">Logon Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Use my RD Gateway credentials for the remote computer</td><td>Check to use the same set of credentials for authenticating to both the RD Gateway server and the remote computer.</td></tr>
</table>

Settings for the Connection Type of Remote Web Access

NOTE

- For descriptions of settings for the connection type of Remote Desktop, please refer to "Settings for the Connection Type of Remote Desktop" on page 74.
- For descriptions of settings for the connection type of Web Feed, please refer to "Settings for the Connection Type of Web Feed" on page 83.

General Sub-tab

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

Three connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Remote Desktop</td><td>Provides access to remote desktops/applications.</td></tr><tr><td>Remote Web Access</td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr><tr><td>Web Feed</td><td>Provides access to remote applications through published Start screen tiles.</td></tr></table></td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a Remote Desktop session automatically or not when Windows 10 IoT Enterprise starts.

If Yes is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.</td></tr>
<tr><td>On Application Exit</td><td>Select what to do when a Remote Desktop session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Windows 10 IoT Enterprise desktop.</td></tr><tr><td>Restart Application</td><td>Opens a Remote Desktop session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
</table>

Options Sub-tab

NOTE

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

RD Gateway Sub-tab

NOTE

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

Settings for the Connection Type of Web Feed

NOTE

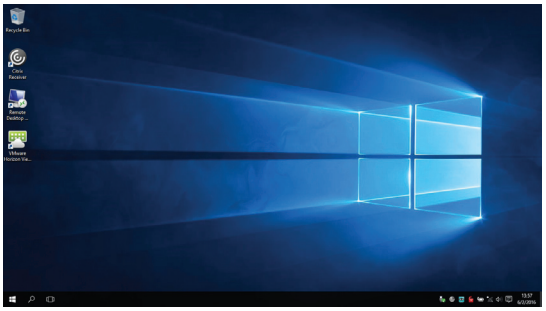
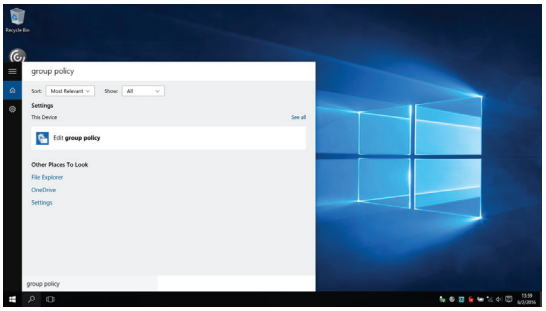
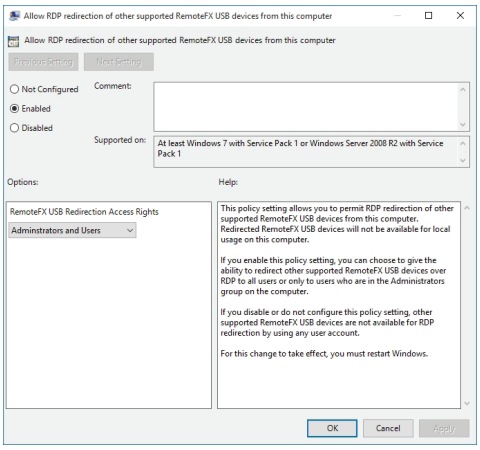
- For descriptions of settings for the connection type of Remote Desktop, please refer to "Settings for the Connection Type of Remote Desktop" on page 74.
- For descriptions of settings for the connection type of Remote Web Access, please refer to "Settings for the Connection Type of Remote Web Access" on page 81.

General Sub-tab

Server Settings	
Item	**Description**
Session Name	Type in the name for Web Feed sessions.
Web Feed URL	Type in the URL through which RD Web Feed is accessible.
Connection Type	This table only provides descriptions for available settings when **Web Feed** is selected. Three connection types are available: **Option** / **Description** Remote Desktop — Provides access to remote desktops/applications. Remote Web Access — Provides access to remote desktops/applications through a Web browser (Internet Explorer). Web Feed — Provides access to remote applications through published Start screen tiles.
Login Settings	
Item	**Description**
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server. **NOTE:** Leave this field blank if the server doesn't belong to any domain.
RemoteApp and Desktop Connection	
Item	**Description**
Update Now	Click to fetch and update the published applications list from the server.

Options Sub-tab

Window Settings	
Item	**Description**
Color Depth	Click the drop-down menu to select the desired color depth for a Remote Desktop session. Four options are available: **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:** 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.
Resolution	Click the drop-down menu to select the desired display resolution on a Remote Desktop session. Twelve options are available: **Fullscreen**, **1920x1200**, **1920x1080**, **1680x1050**, **1400x1050**, **1440x900**, **1280x1024**, **1280x768**, **1280x720**, **1024x768**, **800x600**, and **640x480**.
Multi-Monitor	Click the drop-down menu to enable/disable multiple displays in a Remote Desktop session.
Display the connection bar when I use the full screen	Click the drop-down menu to select if the Connection bar is displayed or not in full-screen mode.
Local Resources Settings	
Item	**Description**
Apply Windows key combinations	Click the drop-down menu to select where to apply Windows key combinations. Three options are available: **On this computer**, **On the remote computer**, **Only when using the full screen**.

RemoteFX USB redirection	Click to enable/disable locally attached RemoteFX USB devices. **NOTE:** To use RemoteFX USB devices in remote desktops, you need to configure the policy setting about device redirection to allow RemoteFX USB Device Redirection as well. To do so, please follow the steps below: 1. Log in to your mt178W with an administrative account. 2. Disable UWF (Unified Write Filter) through Atrust Client Setup (See "4.2.10 Configuring UWF (Unified Write Filter)" on page 51). 3. On the ***desktop***, click in the bottom-left corner.  4. On the appeared Search window, type **group policy**, and then click to select **Edit group policy**.  5. On the opened window, select **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Connection Client** > **RemoteFX USB Device Redirection** > **Allow RDP redirection of other supported RemoteFX USB devices from this computer**. 6. Select **Enabled** and to which users this setting applies: **Administrators Only** or **Administrators and Users**, and then click **OK**.  7. Enable UWF through Atrust Client Setup.

RD Gateway Sub-tab

NOTE

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

4.5.6 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 for service access. You can access virtual desktops and applications for work simply through these shortcuts.

NOTE

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

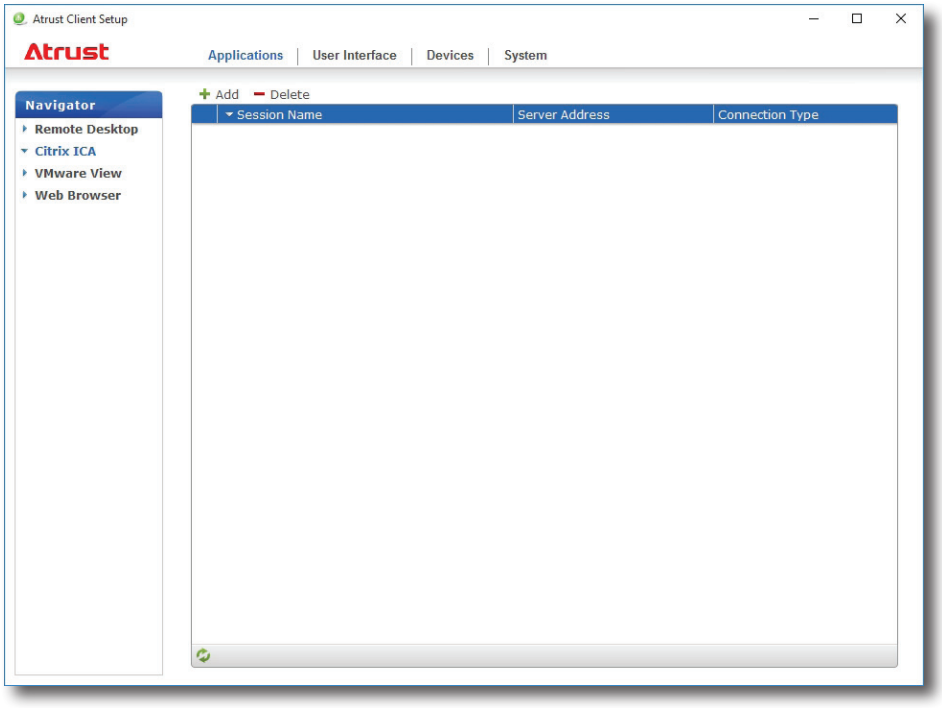
NOTE

- You can also access Citrix services through the Internet Explorer or the standard desktop shortcut **Citrix Receiver**. For detailed instructions on how to access services via this standard desktop shortcut, please refer to section "3.2 Accessing Citrix Services" on page 18.
- The following topics in this section will guide you through the steps of creating and customizing your own service access shortcuts on the desktop and Start menu.
- To configure connection settings for ***Citrix VDI-in-a-Box***, you can choose **Web Logon** or **XenDesktop** connection type.

Connection Type: Web Logon

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

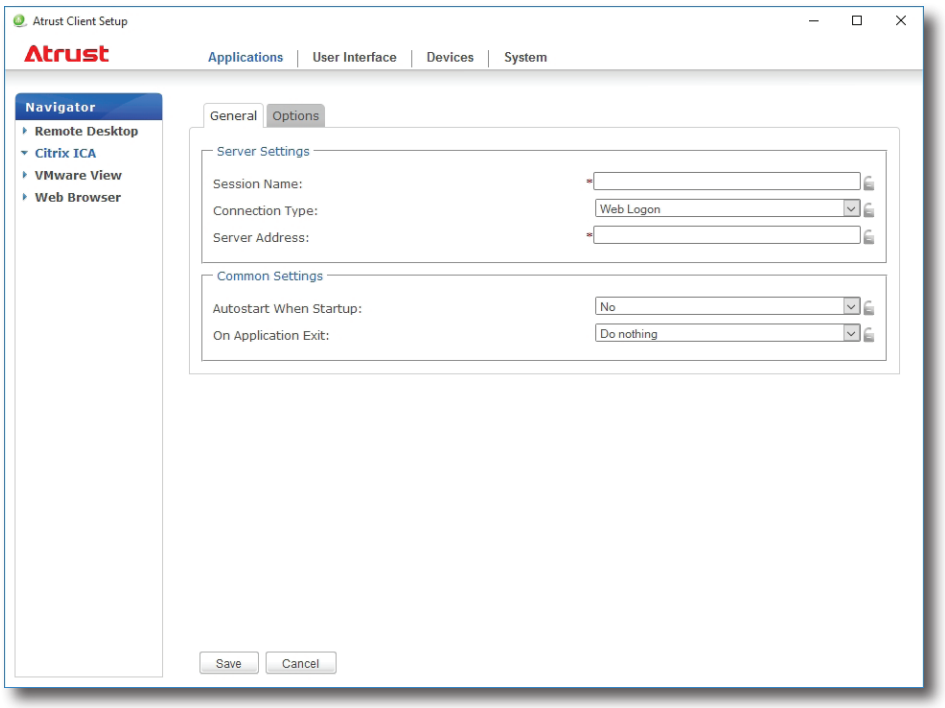
1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.



NOTE

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

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.
4. On **General** sub-tab, leave the connection type as **Web Logon** as default, and then type in the desired session name and the IP address / URL / FQDN of the server through which Citrix services are accessible under the Server Settings section.



NOTE

- The applicable or best suitable information type of the server side may vary with your Citrix environment. Consult your IT administrator for more information.

5. Click **Save** to add this ICA connection entry. The access shortcut will be created automatically on the desktop.

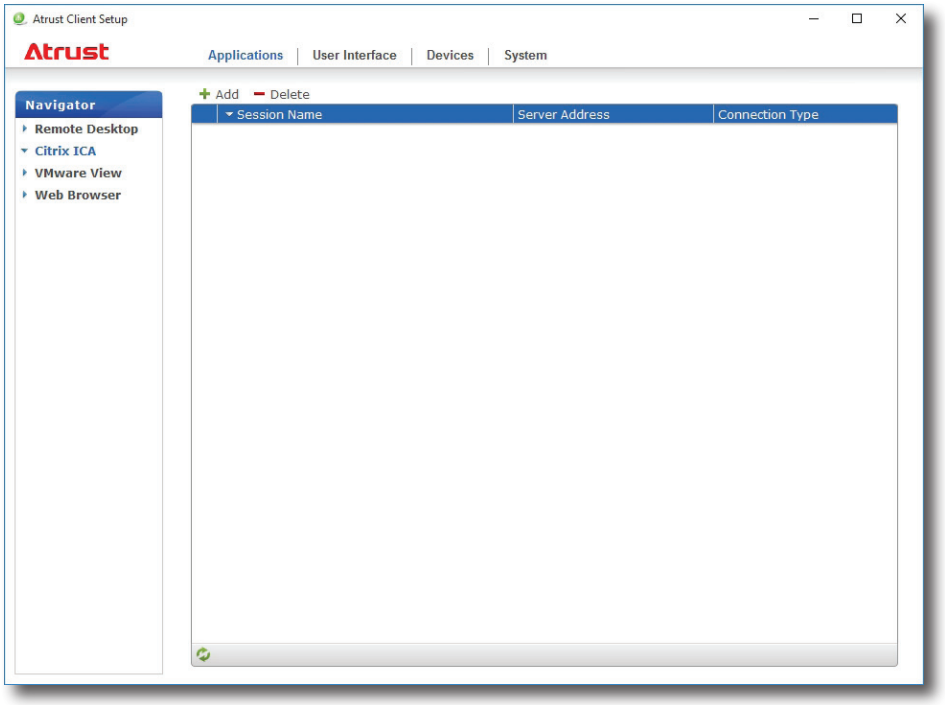
NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "4.5.8 Configuring Advanced ICA Connection Settings" on page 99.

Connection Type: XenDesktop

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

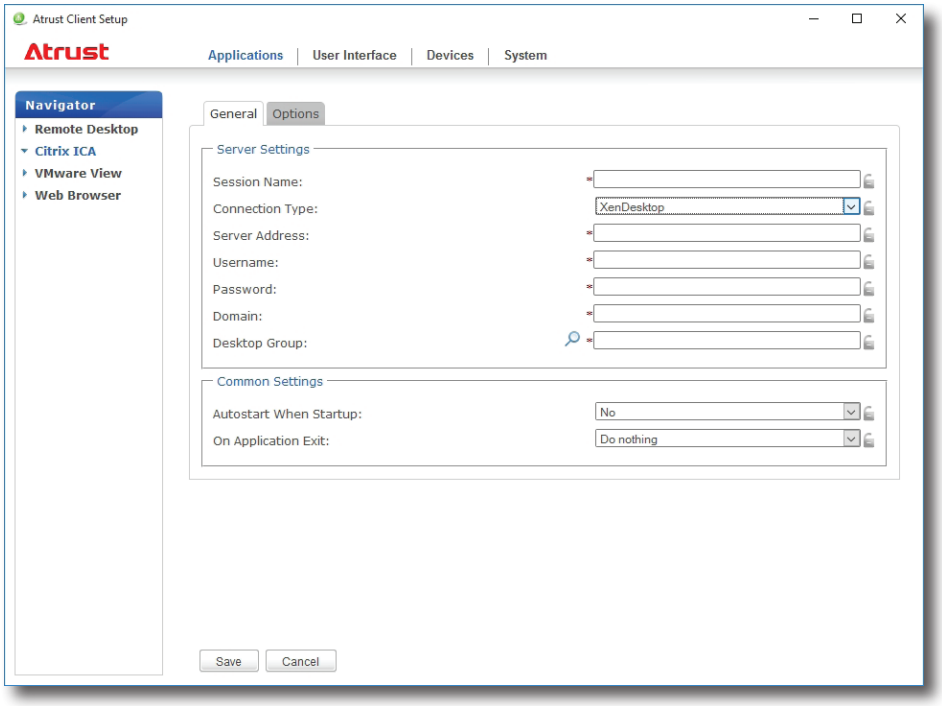
1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.



NOTE

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

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.
4. On **General** sub-tab, click the Connection Type drop-down menu to select **XenDesktop**.

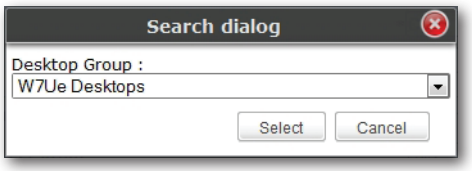


5. Type the session name, the IP address / FQDN of the server through which XenDesktop is accessible, user credentials, the domain of the server, and then click the Search icon to discover available desktop groups.

NOTE

- The applicable or best suitable information type of the server side may vary with your Citrix environment. Consult your IT administrator for more information.
- The Search icon works only when required data (fields marked with a red asterisk) have been provided.

6. Upon completion, the Search Dialog window appears for you to select the desktop group. Click the drop-down menu to select the desired desktop group, and then click **Select** to confirm.



7. The selected desktop group name automatically appears in the Desktop Group field.
8. Click **Save** to confirm. The access shortcut will be created automatically on the desktop.

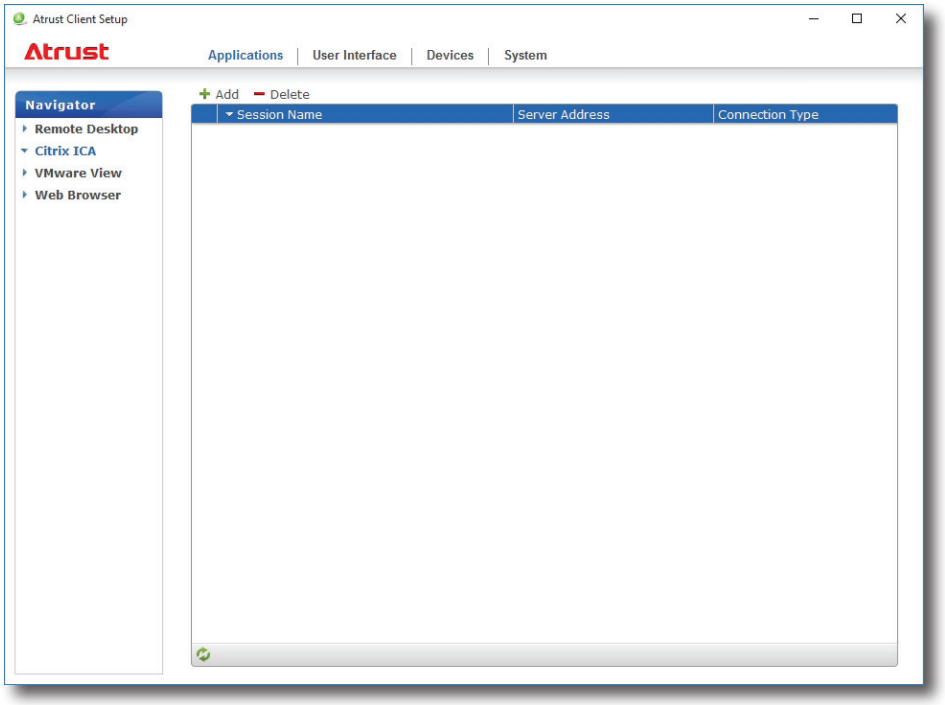
NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "4.5.8 Configuring Advanced ICA Connection Settings" on page 99.

Connection Type: XenApp

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

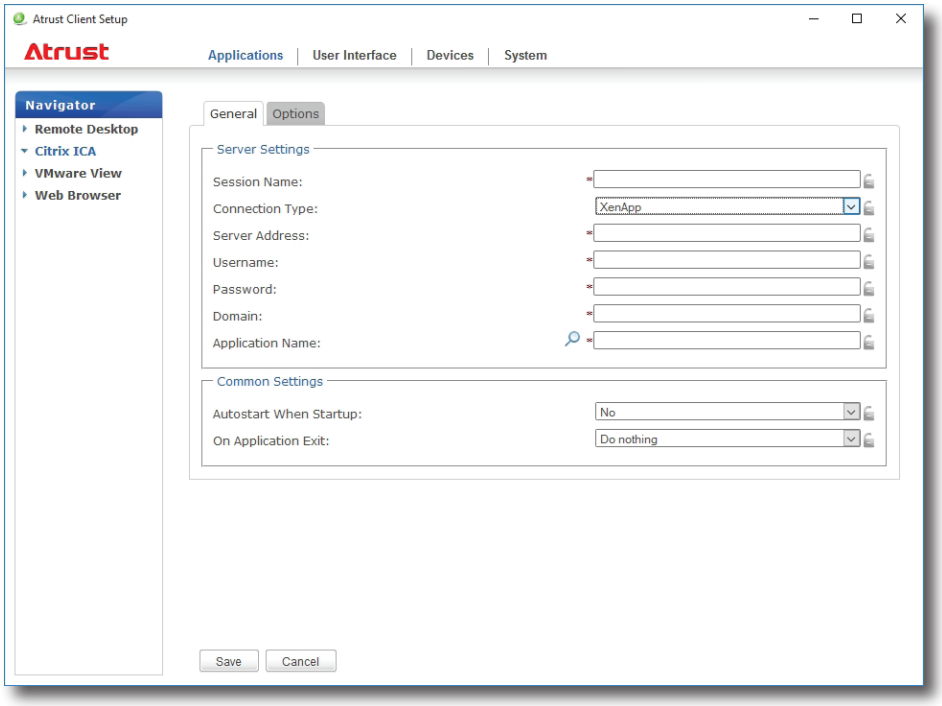
1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.



NOTE

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

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.
4. On **General** sub-tab, click the Connection Type drop-down menu to select **XenApp**.

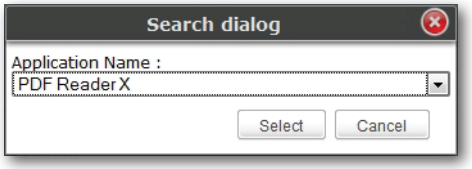


5. Type the session name, the IP address / FQDN of the server through which XenApp is accessible, user credentials, the domain of the server, and then click the Search icon to discover available applications.

NOTE

- The applicable or best suitable information type of the server side may vary with your Citrix environment. Consult your IT administrator for more information.
- The Search icon works only when required data (fields marked with a red asterisk) have been provided. If your XenApp server doesn't belong to any domain, just type its computer name in the Domain field.

6. Upon completion, the Search Dialog window appears for you to select the application. Click the drop-down menu to select the desired application, and then click **Select** to confirm.



7. The selected application name automatically appears in the Application Name field.
8. Click **Save** to confirm. The access shortcut will be created automatically on the desktop.

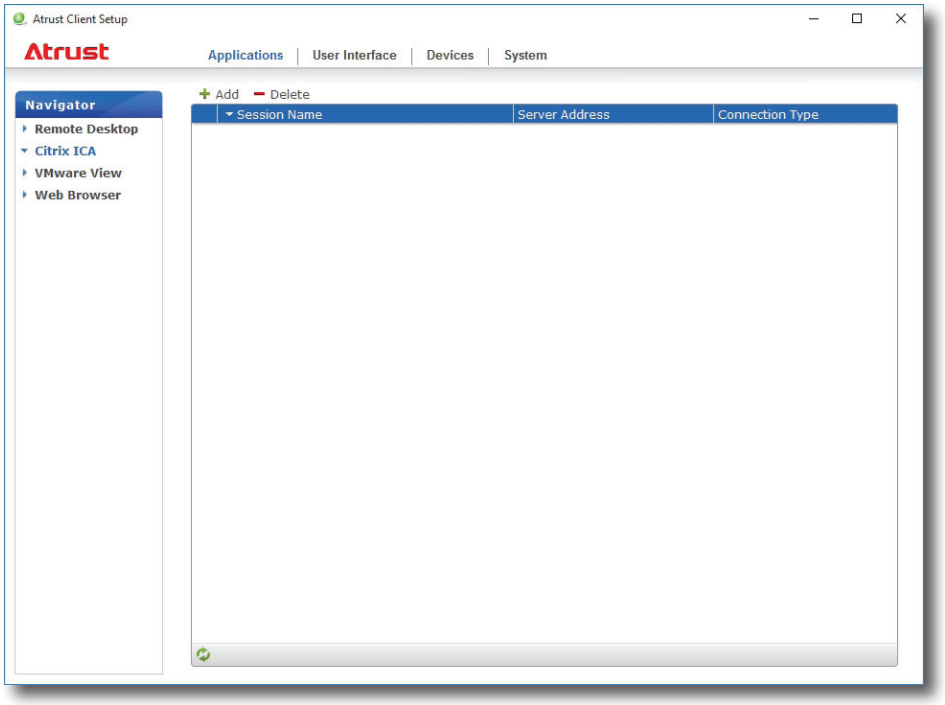
NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section "4.5.8 Configuring Advanced ICA Connection Settings" on page 99.

Connection Type: Server Connection

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

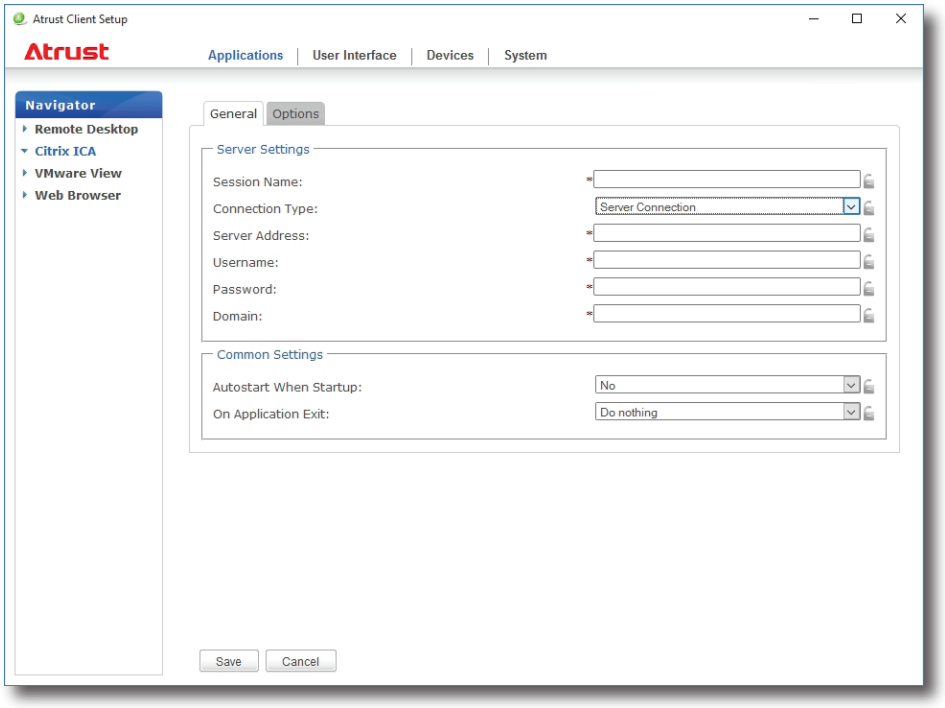
1. On Atrust Client Setup, click **Applications** > **Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.



NOTE

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

3. Click **Add** on the top of the ICA Connection list to create a new entry of ICA connection.
4. On **General** sub-tab, click the Connection Type drop-down menu to select **Server Connection**.



5. Type the session name, the IP address / FQDN of the server, user credentials, and the domain of the server.

NOTE

- The applicable or best suitable information type of the server side may vary with your Citrix environment. Consult your IT administrator for more information.
- Only connections to XenApp servers are supported by this connection type.

6. Click **Save** to confirm. The access shortcut will be created automatically on the desktop.

NOTE

- Depending on your plan of service delivery and the configuration of your server(s), you may need to configure other advanced ICA connection settings for service access. For more information on other available settings, please refer to section “4.5.8 Configuring Advanced ICA Connection Settings” on page 99.

4.5.7 Accessing Citrix Services

For Connection Types of XenDesktop, XenApp, and Server Connection

To access Citrix services, please do the following:

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

> **NOTE**
>
> - You can also access Citrix services through the standard desktop shortcut **Citrix Receiver**. For details on how to access services via the standard desktop shortcut, please refer to section "3.2 Accessing Citrix Services" on page 18.

2. The desired application or desktop is displayed on the screen.

For Connection Types of Web Logon

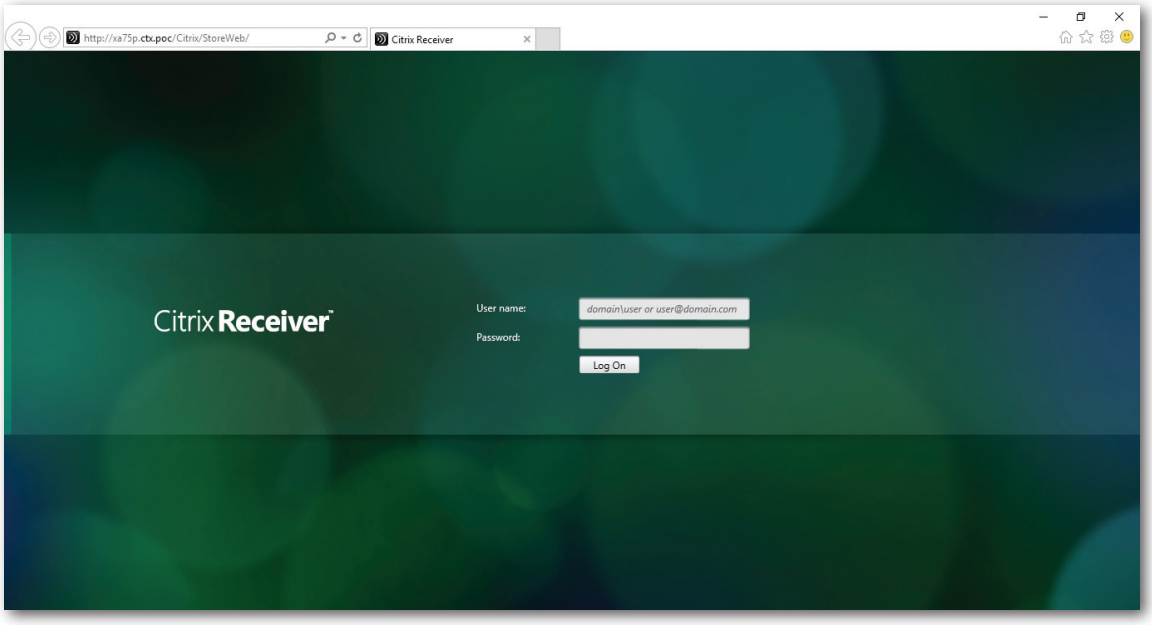
To access Citrix services, please do the following:

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

> **NOTE**
>
> - You can also access Citrix services through the standard desktop shortcut **Citrix Receiver**. For details on how to access services via the standard desktop shortcut, please refer to section "3.2 Accessing Citrix Services" on page 18.

2. The Web browser is launched with the Citrix Logon screen.

Logon Screen Example: XenApp and XenDesktop 7.5 Platinum

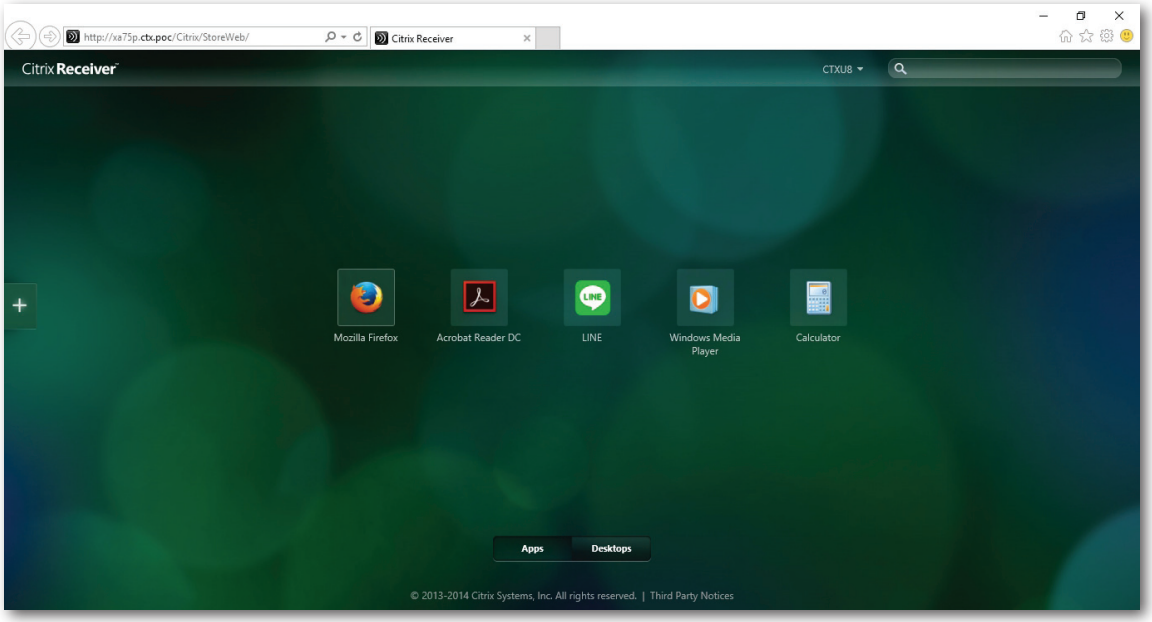


3. Type in the required credentials and domain name, and then click **Log On**.

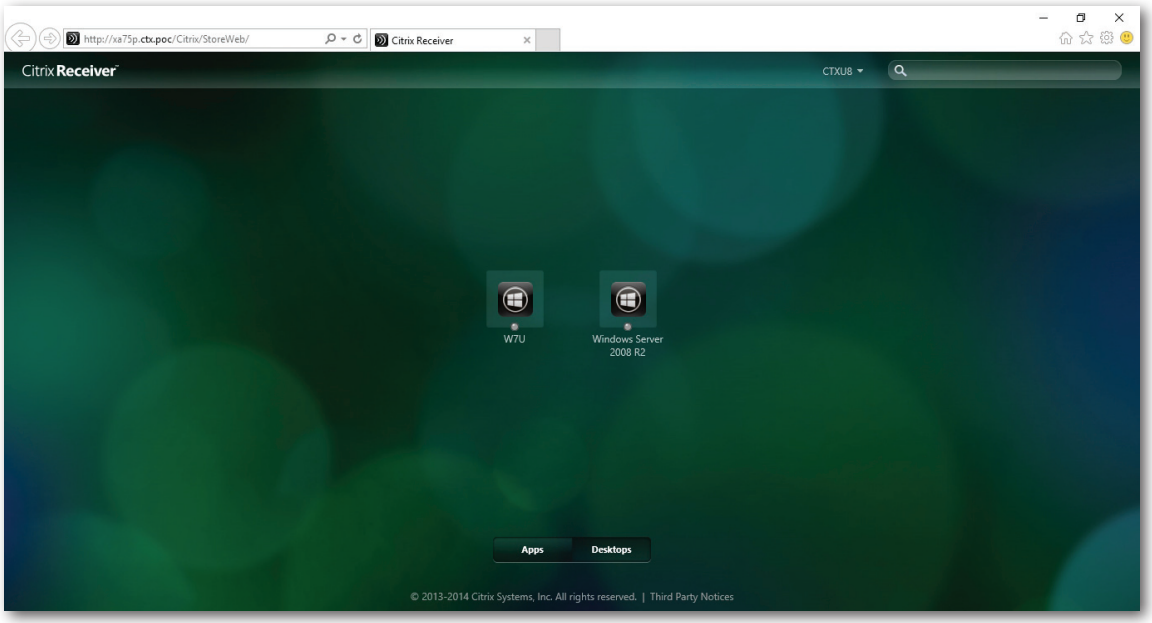
> **NOTE**
>
> - If your service-hosted server doesn't belong to any domain, type in the server name instead if required.

4. Click to select the desired application(s) or desktop(s).

Screen for On-Demand Applications: XenApp 7.5 Platinum



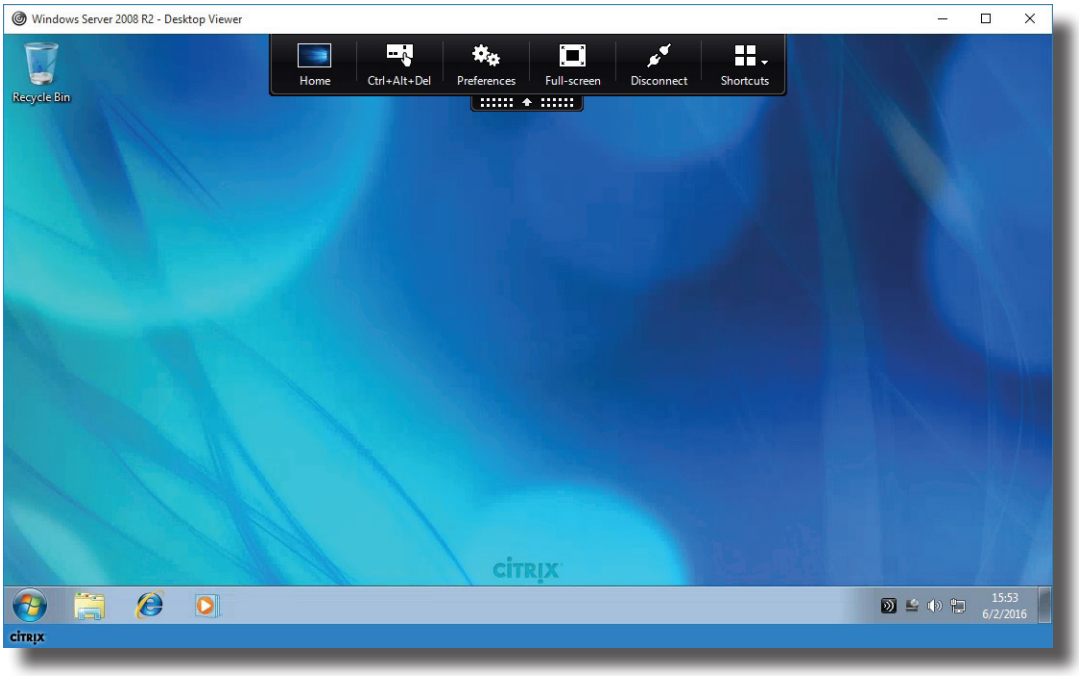
Screen for On-Demand Desktops: XenDesktop 7.5 Platinum



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

Example: Applications Delivered by XenApp 7.5 Platinum
LINE, Mozilla Firefox, Adobe Reader, and Calculator

Example: Desktop Delivered by XenDesktop 7.5 Platinum
Windows Server 2008 R2



Example: Desktop Delivered by XenDesktop 7.5 Platinum
Windows 7 Ultimate

4.5.8 Configuring Advanced ICA Connection Settings

The table below provides a description of each setting item for ICA connections. Please refer to this table to configure advanced settings and customize shortcuts on the desktop and Start menu for service access.

NOTE

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

Settings for the Connection Type of Web Logon

NOTE

- For descriptions of available settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 101.
- For descriptions of available settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 104.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 107.

General Sub-tab

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

Four connection types are available:

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Web Logon</td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr>
<tr><td>XenDesktop</td><td>Provides desktop delivery services.</td></tr>
<tr><td>XenApp</td><td>Provides application delivery services.</td></tr>
<tr><td>Server Connection</td><td>Provides full server access services for administrators (XenApp servers only).</td></tr>
</table>

NOTE: When Web Logon is selected, your mt178W will use a Web browser for service access. The Internet Explorer is always used no matter if you have installed other browsers and which browser you have set as default. For more details, please refer to section "4.5.7 Accessing Citrix Services" on page 95.</td></tr>
<tr><td>Sever Address</td><td>Type in the IP address / URL / FQDN of the server through which Citrix services are accessible.</td></tr>
</table>

Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when Windows 10 IoT Enterprise starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	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 Windows 10 IoT Enterprise desktop. Restart Application — Opens a Citrix ICA session again. Reboot — Restarts your thin client. Shutdown — Turns off your thin client.

Options sub-tab

Web Settings	
Item	**Description**
Mode Setting	Click the drop-down menu to select the desired browser window mode. Two options are available: **Full Screen** and **Normal Mode**. **Option** / **Description** Full Screen — The browser is opened in the Full Screen mode. Normal Mode — The browser is opened in the Normal mode. **NOTE:** This setting item is available only when **Web Logon** is selected in the Connection Type field. This type of connection allows you to access services through the interface of the Web browser. **NOTE:** The used Web browser for service access is always the Internet Explorer, no matter which browser you set as the default.

Settings for the Connection Type of XenDesktop

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 99.
- For descriptions of available settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 104.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 107.

General Sub-tab

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

Four connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Web Logon</td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr><tr><td>XenDesktop</td><td>Provides desktop delivery services.</td></tr><tr><td>XenApp</td><td>Provides application delivery services.</td></tr><tr><td>Server Connection</td><td>Provides full server access services for administrators (XenApp servers only).</td></tr></table></td></tr>
<tr><td>Sever Address</td><td>Type in the IP address / FQDN of the server through which XenDesktop is accessible.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.</td></tr>
<tr><td>Desktop Group</td><td>Type in the desktop group.

NOTE: You can use the Search icon in front of the field to discover available desktop groups. For detailed instructions, please refer to "Connection Type: XenDesktop" on page 89.</td></tr>
</table>

Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when Windows 10 IoT Enterprise starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	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 Windows 10 IoT Enterprise desktop. Restart Application — Opens a Citrix ICA session again. Reboot — Restarts your thin client. Shutdown — Turns off your thin client.

Options sub-tab

Window Settings	
Item	**Description**
Requested Color Quality	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **No preference**, **Better Speed (16-bit)**, and **Better Appearance (32-bit)**. **Option** / **Description** No preference — No preference for a specific color quality. Better Speed (16-bit) — The 16-bit color quality is used for better display speed. Better Appearance (32-bit) — The 32-bit color quality is used for better desktop appearance.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: **Default**, **Seamless**, **Full Screen**, **640 x 480**, **800 x 600**, **1024 x 768**, **1280 x 1024**, and **1600 x 1200**. **NOTE:** When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size. **NOTE:** For more information about how to disable the XenDesktop toolbar, please visit Citrix websites at support.citrix.com or www.citrix.com for online help. **NOTE:** In case that you don't want to disable the toolbar, you can use the toolbar or your mouse to resize the launched window if needed.

<table>
<tr><th colspan="2">Device Mapping</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Mapping Local Drive</td><td>Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If Yes is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions.</td></tr>
<tr><td>Mapping Local Serial Ports</td><td>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.</td></tr>
<tr><td>Mapping local Printers</td><td>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.</td></tr>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Network Protocol</td><td>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.</td></tr>
<tr><td>Audio Quality</td><td>Click the drop-down menu to disable audio playback or choose the desired sound quality in a Citrix ICA session.

Click the drop-down menu to disable audio playback or to configure the quality setting for audio playback in a Citrix ICA session. Four options are available: High - high definition audio, Medium - optimized for speech, Low - for low-speed connections, and Off.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>High - high definition audio</td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr>
<tr><td>Medium - optimized for speech</td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr>
<tr><td>Low - for low-speed connections</td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr>
<tr><td>Off</td><td>Disables audio playback in opened ICA sessions.</td></tr>
</table></td></tr>
<tr><td>Encryption</td><td>Click the drop-down menu to select the desired encryption method. Five options are available: Not configured, Basic, RC5 128 bit (login only), RC5 40 bit, RC5 56 bit, RC5 128 bit.</td></tr>
<tr><td>Apply Windows key combinations</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On the local desktop, On the remote desktop, In full screen desktops only.</td></tr>
</table>

Settings for the Connection Type of XenApp

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 99.
- For descriptions of available settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 101.
- For descriptions of settings for the connection type of Server Connection, please refer to "Settings for the Connection Type of Server Connection" on page 107.

General Sub-tab

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

Four connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Web Logon</td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr><tr><td>XenDesktop</td><td>Provides desktop delivery services.</td></tr><tr><td>XenApp</td><td>Provides application delivery services.</td></tr><tr><td>Server Connection</td><td>Provides full server access services for administrators (XenApp servers only).</td></tr></table></td></tr>
<tr><td>Sever Address</td><td>Type in the IP address / FQDN of the server through which XenApp is accessible.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.

NOTE: Type in the full computer/server name if your XenApp server doesn't belong to any domain.</td></tr>
<tr><td>Application Name</td><td>Type in the application name.

NOTE: You can use the Search icon in front of the field to discover available applications. For detailed instructions, please refer to "Connection Type: XenApp" on page 91.</td></tr>
</table>

Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when Windows 10 IoT Enterprise starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	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 Windows 10 IoT Enterprise desktop.
Restart Application	Opens a Citrix ICA session again.
Reboot	Restarts your thin client.
Shutdown	Turns off your thin client.

Options Sub-tab

Window Settings	
Item	**Description**
Requested Color Quality	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **No preference**, **Better Speed (16-bit)**, and **Better Appearance (32-bit)**.

Option	Description
No preference	No preference for a specific color quality.
Better Speed (16-bit)	The 16-bit color quality is used for better display speed.
Better Appearance (32-bit)	The 32-bit color quality is used for better desktop appearance.

Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: **Default**, **Seamless**, **Full Screen**, **640 x 480**, **800 x 600**, **1024 x 768**, **1280 x 1024**, and **1600 x 1200**.
Device Mapping	
Item	**Description**
Mapping Local Drive	Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If **Yes** is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.
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.

<table>
<tr><td>Mapping local Printers</td><td>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 through this connection.</td></tr>
<tr><td colspan="2">Connection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Network Protocol</td><td>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.</td></tr>
<tr><td>Audio Quality</td><td>Click the drop-down menu to disable audio playback or choose the desired sound quality in a Citrix ICA session.

Click the drop-down menu to disable audio playback or to configure the quality setting for audio playback in a Citrix ICA session. Four options are available: High - high definition audio, Medium - optimized for speech, Low - for low-speed connections, and Off.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>High - high definition audio</td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr>
<tr><td>Medium - optimized for speech</td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr>
<tr><td>Low - for low-speed connections</td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr>
<tr><td>Off</td><td>Disables audio playback in opened ICA sessions.</td></tr>
</table></td></tr>
<tr><td>Encryption</td><td>Click the drop-down menu to select the desired encryption method. Five options are available: Not configured, Basic, RC5 128 bit (login only), RC5 40 bit, RC5 56 bit, RC5 128 bit.</td></tr>
<tr><td>Apply Windows key combinations</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On the local desktop, On the remote desktop, In full screen desktops only.</td></tr>
</table>

Settings for the Connection Type of Server Connection

NOTE

- For descriptions of available settings for the connection type of Web Logon, please refer to "Settings for the Connection Type of Web Logon" on page 99.
- For descriptions of available settings for the connection type of XenDesktop, please refer to "Settings for the Connection Type of XenDesktop" on page 101.
- For descriptions of settings for the connection type of XenApp, please refer to "Settings for the Connection Type of XenApp" on page 104.

General Sub-tab

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

Four connection types are available:

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Web Logon</td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr><tr><td>XenDesktop</td><td>Provides desktop delivery services.</td></tr><tr><td>XenApp</td><td>Provides application delivery services.</td></tr><tr><td>Server Connection</td><td>Provides full server access services for administrators (XenApp servers only).</td></tr></table></td></tr>
<tr><td>Sever Address</td><td>Type in the IP address / URL / FQDN of the XenApp server.

NOTE: Server Connection only supports connections to XenApp servers.</td></tr>
<tr><td>Username</td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td>Domain</td><td>Type in the domain of the server.

NOTE: Type in the full computer/server name if the server doesn't belong to any domain.</td></tr>
</table>

Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when Windows 10 IoT Enterprise starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	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 Windows 10 IoT Enterprise desktop. Restart Application — Opens a Citrix ICA session again. Reboot — Restarts your thin client. Shutdown — Turns off your thin client.

Options Sub-tab

Window Settings	
Item	**Description**
Requested Color Quality	Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: **No preference**, **Better Speed (16-bit)**, and **Better Appearance (32-bit)**. **Option** — **Description** No preference — No preference in a specific color quality. Better Speed (16-bit) — The 16-bit color quality is used for better display speed. Better Appearance (32-bit) — The 32-bit color quality is used for better desktop appearance.
Window Size	Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: **Default**, **Seamless**, **Full Screen**, **640 x 480**, **800 x 600**, **1024 x 768**, **1280 x 1024**, and **1600 x 1200**.
Device Mapping	
Item	**Description**
Mapping Local Drive	Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If **Yes** is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.
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.

<table>
<tr><td>Mapping local Printers</td><td>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 through this connection.</td></tr>
<tr><td colspan="2">Connection Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Network Protocol</td><td>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.</td></tr>
<tr><td>Audio Quality</td><td>Click the drop-down menu to disable audio playback or choose the desired sound quality in a Citrix ICA session.

Click the drop-down menu to disable audio playback or to configure the quality setting for audio playback in a Citrix ICA session. Four options are available: High - high definition audio, Medium - optimized for speech, Low - for low-speed connections, and Off.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>High - high definition audio</td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr>
<tr><td>Medium - optimized for speech</td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr>
<tr><td>Low - for low-speed connections</td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr>
<tr><td>Off</td><td>Disables audio playback in opened ICA sessions.</td></tr>
</table></td></tr>
<tr><td>Encryption</td><td>Click the drop-down menu to select the desired encryption method. Five options are available: Not configured, Basic, RC5 128 bit (login only), RC5 40 bit, RC5 56 bit, RC5 128 bit.</td></tr>
<tr><td>Apply Windows key combinations</td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: On the local desktop, On the remote desktop, In full screen desktops only.</td></tr>
</table>

4.5.9 Configuring Basic VMware View Connection Settings

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

NOTE

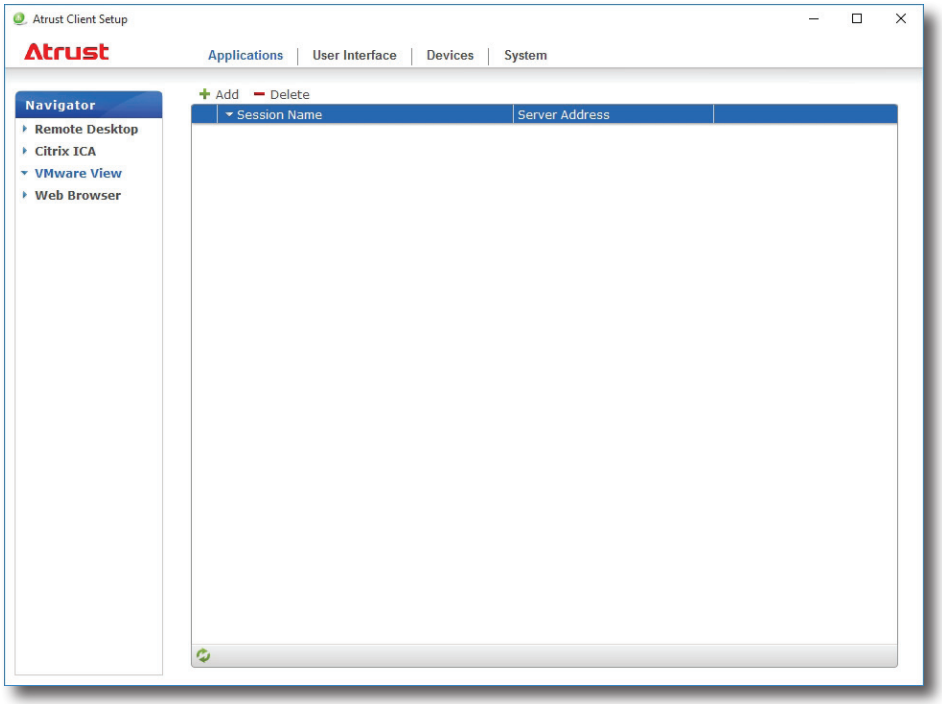
- For more information on VMware desktop virtualization solutions, please visit VMware website at www.vmware.com.

NOTE

- You can also access VMware View or Horizon View services through the standard desktop shortcut **VMware Horizon View Client**. For detailed instructions on how to access services via the standard desktop shortcut, please refer to chapter 3 "Getting Started" on page 15 or the Quick Start Guide for mt178W.
- The following sections will guide you through the steps of creating your own service access shortcuts on the desktop.

To quickly configure VMware View connection settings, please do the following:

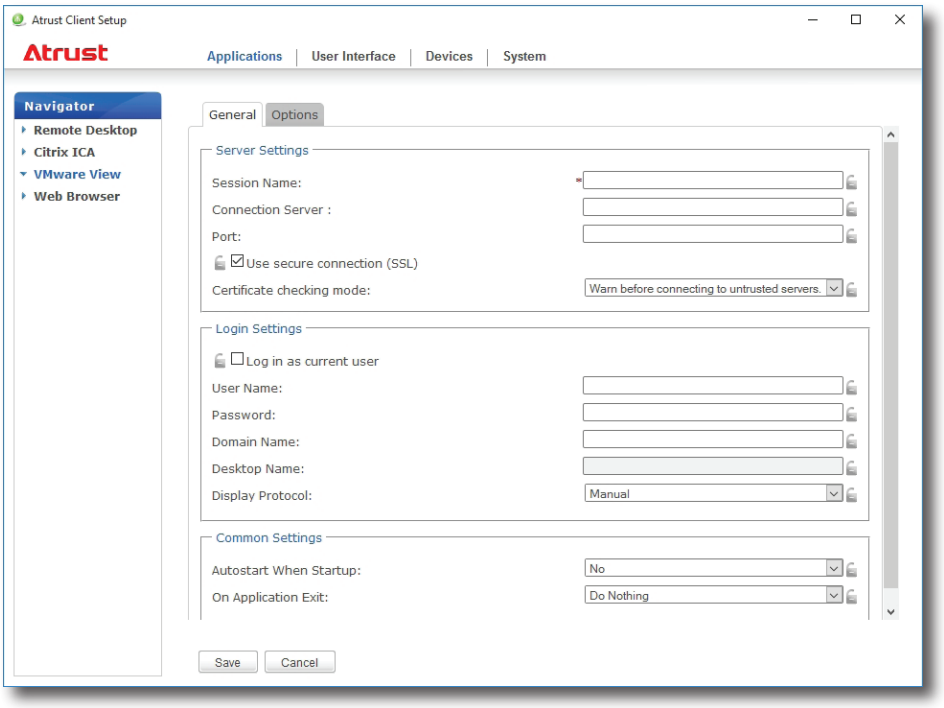
1. On Atrust Client Setup, click **Applications** > **VMware View**.
2. The View Connection list appears in the Configuration area.



NOTE

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

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



4. Type in the desired session name, and then click **Save** to confirm.

NOTE

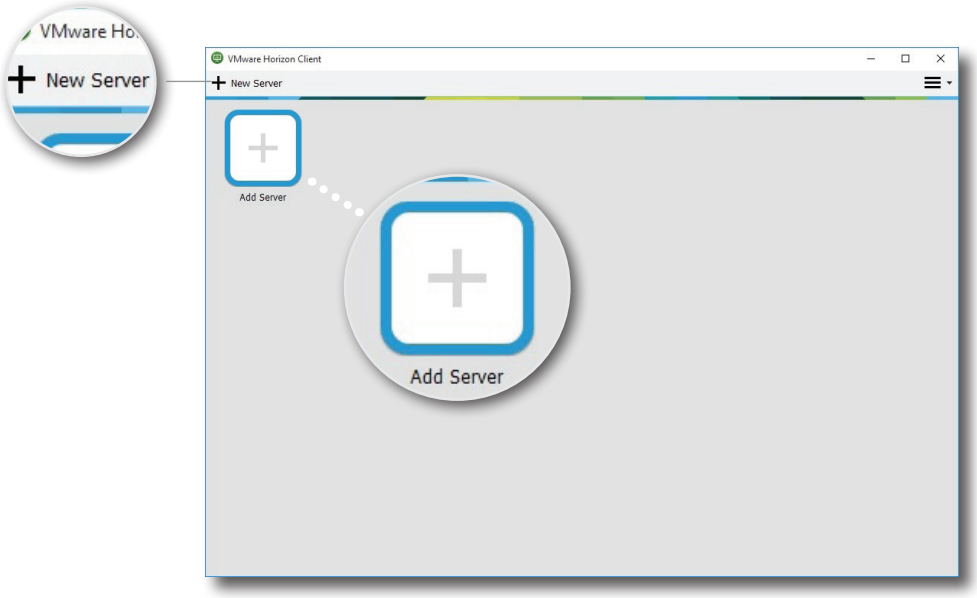
- This is the only required field for the creation of a service access shortcut on the desktop. Other data can be provided during the period of service access. Depending on your needs, you might choose to type in more other data.

5. The new entry is added to the View Connection list and the access shortcut is created automatically on the desktop.

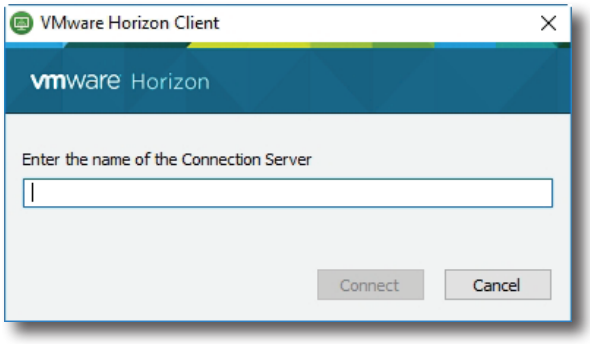
4.5.10 Accessing VMware View or Horizon View Services

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

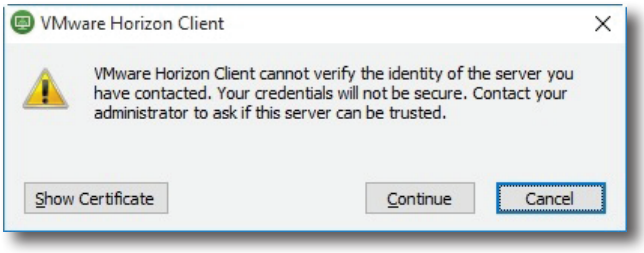
1. Double click the created (customized) access shortcut on the desktop.
2. A window appears allowing you to add the name or IP address of the View Connection Server.
3. Double-click **Add Server** icon or click **New Server** in the top-left corner.



4. A window appears prompting for the name or IP address of the View Connection Server. Enter the required information, and then click **Connect**.

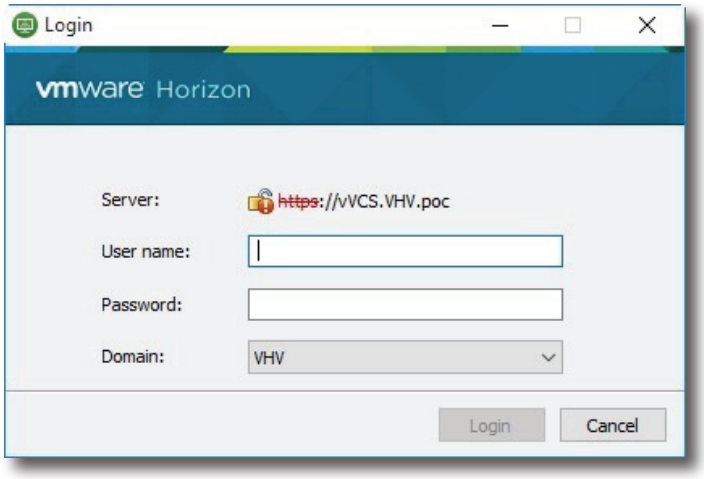


5. A window may appear with a certificate message about the remote server. Consult your IT administrator for details and ensure the connection is secure ***first***. To bypass, click **Continue**.

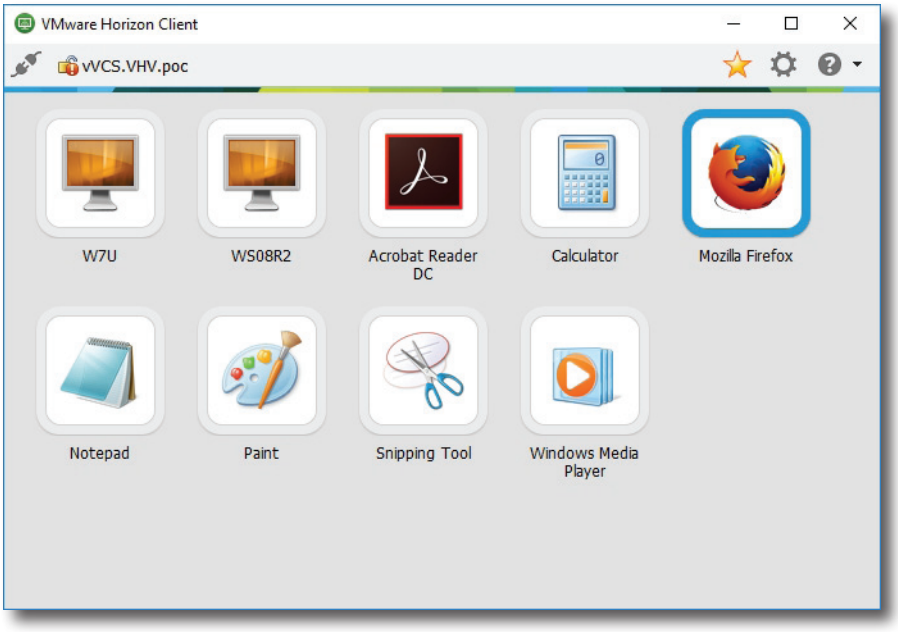


6. A window may appear with a Welcome message. Click **OK** to continue.

7. Provide your user name and password on the opened window, and then click **Login**.



8. A window appears with available desktops or applications for your credentials. Double-click to select the desired desktop or application.



9. The desktop or application will be displayed on the screen.

4.5.11 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 desktop and Start menu for service access.

General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Session Name</td><td>Type in the name for VMware View or Horizon View sessions.</td></tr>
<tr><td>Connection Server</td><td>Type in the computer name or IP address of the View Connection Server.

NOTE: For more information on View Connection Sever, please visit VMware website at www.vmware.com.</td></tr>
<tr><td>Port</td><td>Type in the port number used to communicate with the View Connection Server. To use the default value, simply leave it blank.</td></tr>
<tr><td>Use secure connection (SSL)</td><td>Check/Uncheck to enable/disable secure connection.</td></tr>
<tr><td>Certificate checking mode</td><td>Click to select whether to verify the identity of the remote server and whether to connect to an untrusted server. Three options are available: Do not verify server identity certificates, Warn before connecting to untrusted servers, and Never connect to untrusted servers.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Do not verify server identity certificates</td><td>Do not verify the identity of the remote server and connect to it anyway.</td></tr>
<tr><td>Warn before connecting to untrusted servers</td><td>Warns and allows users to choose whether to connect or not.</td></tr>
<tr><td>Never connect to untrusted servers</td><td>Disallows untrusted connections.</td></tr>
</table>
</td></tr>
<tr><th colspan="2">Login Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Log in as current user</td><td>Check to log in to VMware View or Horizon View services with the current user credentials. When checked, the User Name, Password, and Domain Name fields will be grayed out.</td></tr>
<tr><td>User Name</td><td>Type in the user name for authentication.</td></tr>
<tr><td>Password</td><td>Type in the password for authentication.</td></tr>
<tr><td>Domain Name</td><td>Type in the domain name of the View Connection Sever.</td></tr>
<tr><td>Desktop Name</td><td>Type in the desktop name. Or, leave it blank for users to select one.

NOTE: If Manual is selected for the Display Protocol field below, this field will be grayed out.</td></tr>
</table>

<table>
<tr><td>Display Protocol</td><td>Click the drop-down menu to select the display protocol. Three options are available: Manual, Microsoft RDP, and PCoIP.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Manual</td><td>Manually select the desired display protocol.</td></tr><tr><td>Microsoft RDP</td><td>Use Microsoft RDP as the display protocol.</td></tr><tr><td>PCoIP</td><td>Use VMware PCoIP as the display protocol.</td></tr></table></td></tr>
<tr><td colspan="2">Common Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Autostart When Startup</td><td>Select whether to open a VMware View or Horizon View session automatically or not when Windows 10 IoT Enterprise starts.

If Yes is selected, when you log in to the system, the VMware View or Horizon View session will be opened automatically.</td></tr>
<tr><td>On Application Exit</td><td>Select what to do when a VMware View or Horizon View session is ended. Four options are available: Do Nothing, Restart Application, Reboot, and Shutdown.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Do Nothing</td><td>Returns to the Windows 10 IoT Enterprise desktop.</td></tr><tr><td>Restart Application</td><td>Opens a View or Horizon View session again.</td></tr><tr><td>Reboot</td><td>Restarts your thin client.</td></tr><tr><td>Shutdown</td><td>Turns off your thin client.</td></tr></table></td></tr>
</table>

Options Sub-tab

<table>
<tr><td colspan="2">Window Settings</td></tr>
<tr><td>Item</td><td>Description</td></tr>
<tr><td>Display</td><td>Click the drop-down menu to select the desired display size of a View desktop. Five options are available: Full Screen, Multi Monitor, Large Window, and Small Window.

<table><tr><th>Option</th><th>Description</th></tr><tr><td>Full Screen</td><td>Opens the selected View desktop in full screen.</td></tr><tr><td>Multi Monitor</td><td>Opens the selected View desktop in multiple displays.</td></tr><tr><td>Large Window</td><td>Opens the selected View desktop in a large window.</td></tr><tr><td>Small Window</td><td>Opens the selected View desktop in a small window.</td></tr></table></td></tr>
</table>

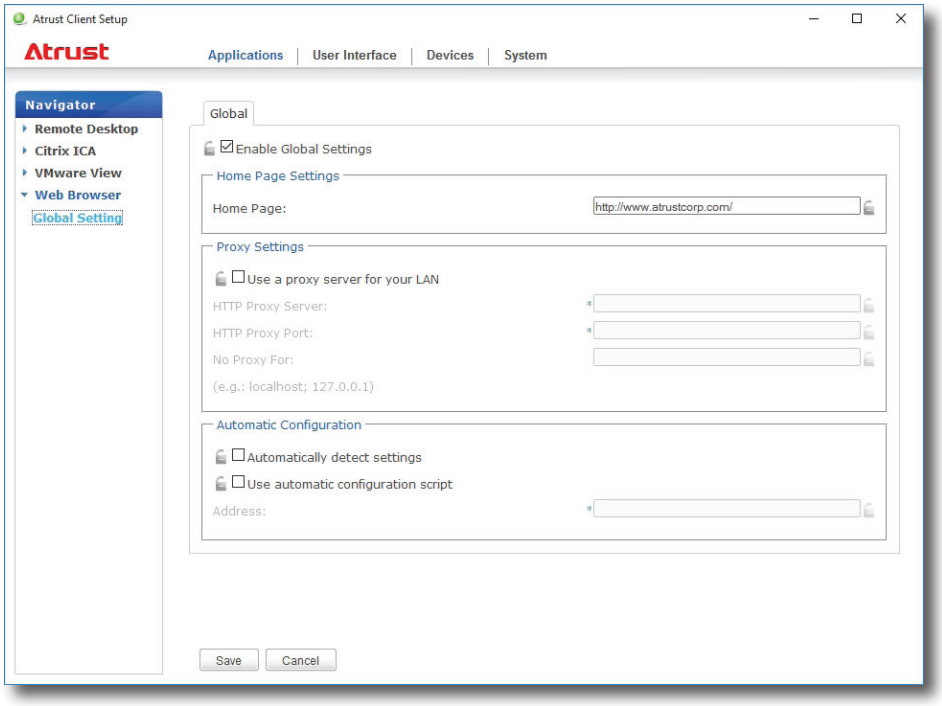
4.5.12 Configuring Web Browser Settings

The **Web Browser** setting item allows you to configure browser session settings and create shortcuts on the desktop or Start menu for browser sessions.

Configuring General Browser Session Settings

To configure general browser session settings, please do the following:

1. On Atrust Client Setup, click **Applications** > **Web Browser** > **Global Setting**.



2. Refer to the table below to set up home page, proxy, and automatic configuration settings, and then click **Save** to apply.

Basic Settings	
Item	**Description**
Home Page	Type in the URL of a Web page for quick access via the Home button.
Proxy Settings	
Item	**Description**
Use a proxy server for your LAN	Check to use a proxy server in your local area network.
HTTP Proxy Server	Type in the IP address of the proxy server.
HTTP Proxy Port	Type in the communication port of the proxy server.
No Proxy For	Type in the IP address(es) to bypass the proxy server.

Automatic Configuration	
Item	**Description**
Automatically detect settings	Check to automatically detect browser settings.
Use automatic configuration script	Check to allow automatic configuration and indicate the IP address where a configuration file is located.
Address	Type in the IP address when **Use automatic configuration script** is selected.

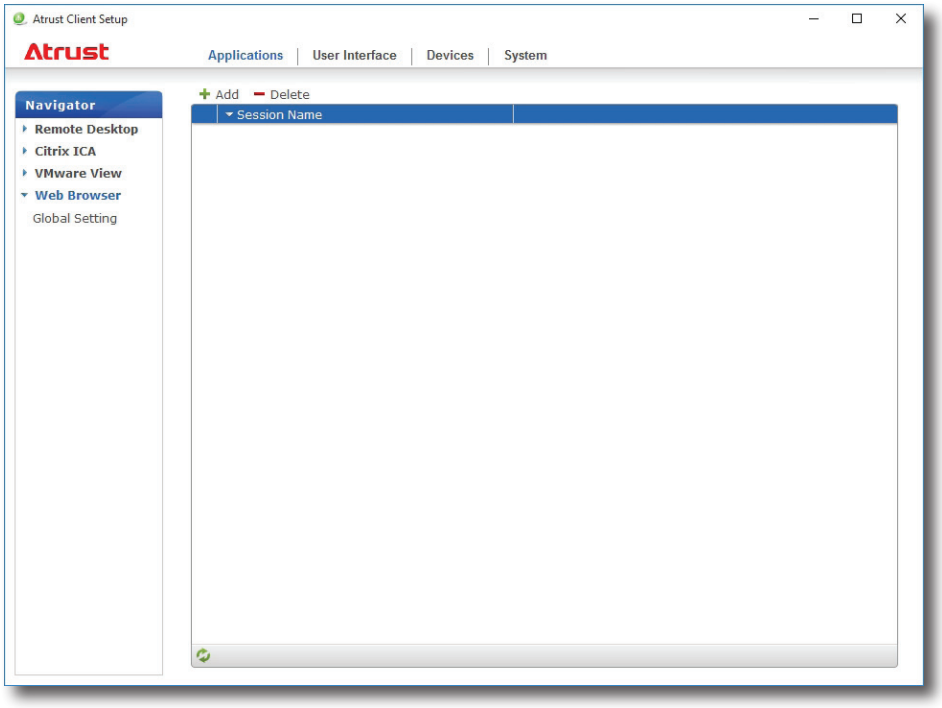
Configuring Specific Browser Session Settings

To configure specific browser session settings and create shortcuts on the desktop and Start menu, please do the following:

TIP

- You can use this feature to create a desktop shortcut for a specific web page, for example, your intranet home page.

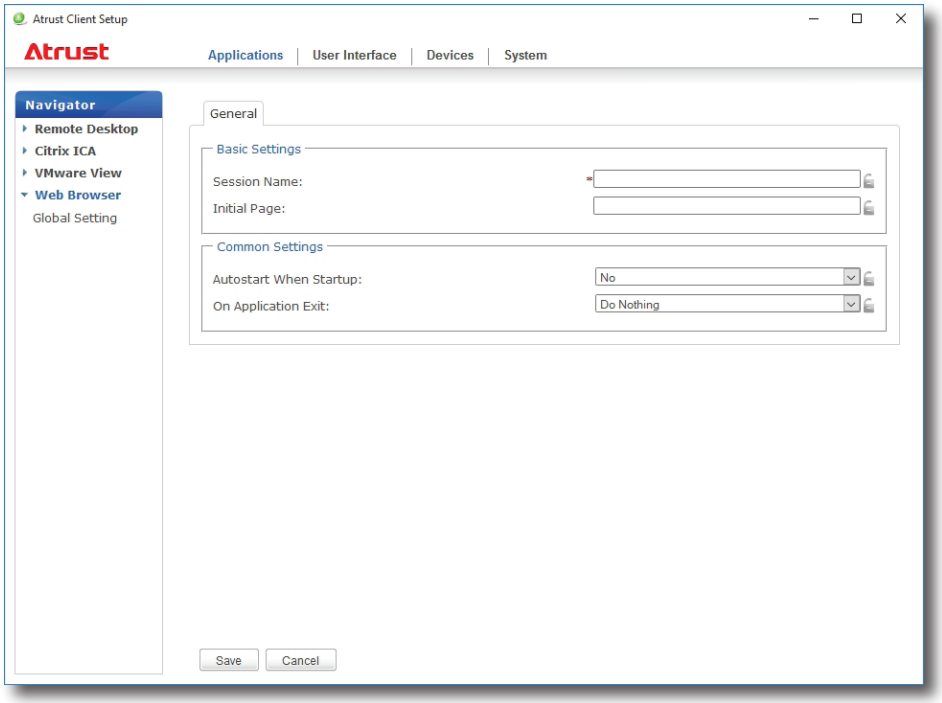
1. On Atrust Client Setup, click **Applications** > **Web Browser**.
2. The Browser Session list appears in the Configuration area.



NOTE

- If you haven't create any entry, the Browser Session list will be empty.

3. Click **Add** on the top of the Browser Session list.
4. On **General** sub-tab, type in the desired session name, the URL of the initial web page, and select other settings if needed (refer to the table below for descriptions).



Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a browser session automatically or not when Windows 10 IoT Enterprise starts. If **Yes** is selected, every time when you log in to the system, the browser session will be opened automatically.
On Application Exit	Select what to do when a browser session is ended. Four options are available: **Do Nothing**, **Restart Application**, **Reboot**, and **Shutdown**.

Option	**Description**
Do Nothing	Returns to the Windows 10 IoT Enterprise desktop.
Restart Application	Opens a browser session again.
Reboot	Restarts your thin client.
Shutdown	Turns off your thin client.

5. Click **Save** to confirm. The access shortcut will be created automatically on the desktop.

Appendices

This chapter provides instructions for the maintenance of your mt178W thin clients.

A.1 Resetting Your mt178W

How to reset your mt178W to the unmanaged state and its settings under Atrust Client Setup to factory defaults 121

A.2 Updating Firmware for Your mt178W

Four ways to update firmware for your mt178W 122

A.1 Resetting Your mt178W

Reset Mode enables you to restore settings under Atrust Client Setup to the factory defaults. Additionally, it also releases a managed mt178W from the management of Atrust Device Manager, a management console developed by Atrust for remote and mass client management.

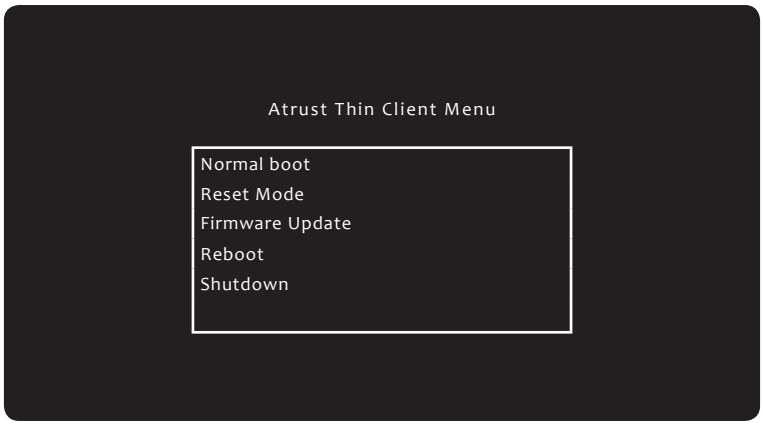
You can perform **Reset Mode** locally through Atrust Thin Client Menu.

NOTE

- You can also release a managed mt178W ***remotely*** from Atrust Device Manager. For details, please refer to the User's Manual for Atrust Device Manager.

To reset your mt178W, please do the following:

1. Restart your mt178W.
2. During the POST (Power-On Self-Test) period, press **Esc** on the keyboard to enter Atrust Thin Client Menu.



NOTE

- Five options are available on Atrust Thin Client Menu: **Normal boot**, **Reset Mode**, **Firmware Update**, **Reboot**, and **Shutdown**. See the table below for the description of each option:

Menu Option	Description
Normal boot	Powers up your mt178W as the normal startup procedure.
Reset Mode	Resets Atrust Client Setup settings and remote management status for your mt178W.
Firmware Update	Updates firmware for your mt178W through the network.
Reboot	Restarts your mt178W.
Shutdown	Powers off your mt178W.

3. Use arrow keys to select **Reset Mode**, and then press **Enter** to continue.
4. A message appears prompting you for confirmation. Type **y** to confirm.
5. Upon completion, press **Enter** to restart.

A.2 Updating Firmware for Your mt178W

Four ways are available to update firmware for your mt178W:

Method	Description
Atrust Thin Client Menu	Downloads firmware from a remote computer and updates firmware for your thin client.
USB Flash Drive	Updates firmware with a USB flash drive created by Recovery USB Disk Creator.
Atrust Client Setup	Initiates firmware update locally on the thin client with the help of Atrust Client Setup.
Atrust Device Manger	Initiates firmware update remotely on the remote computer with Atrust Device Manager.

Using Atrust Thin Client Menu

To update firmware using Atrust Thin Client Menu, please do the following:

1. Connect your thin client to the network, and then restart it.
2. During the POST (Power-On Self-Test) period, press **Esc** on the keyboard to enter Atrust Thin Client Menu.
3. Select **Firmware Update** and then follow the on-screen instructions to complete the task.

NOTE

- You need to specify the IP address of the firmware server over the network. A firmware server is the server where Atrust Device Manager is installed and client firmware files are imported through Atrust Device Manager.
- For more information about Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

Using a USB Flash Drive

To update firmware using a USB flash drive created by Recovery USB Disk Creator, please do the following:

NOTE

- For instructions on how to create a USB flash drive using Recovery USB Disk Creator, please refer to the Quick Guide for USB Creator.

1. Plug the USB flash drive, and then restart your thin client.
2. During the POST period, press **F7** to enter the Boot Device menu.
3. Select the USB flash drive on that menu to enter Atrust Thin Client Recovery System screen.
4. Follow the on-screen instructions to complete the task.

Using Atrust Client Setup

To update firmware using Atrust Client Setup, please refer to section "4.2.5 Updating Firmware from the Management Computer" on page 38.

Using Atrust Device Manager

To update firmware using Atrust Device Manager, please refer to the User's Manual for Atrust Device Manager.

Specifications

Atrust mt178W mobile thin client

Processor	Intel® Celeron® N2807, Dual-core, 1.58 GHz			
System Memory	4 GB DDR3			
Flash Memory	16 GB M.2 SSD (Optional: 32 / 64 GB)			
Display	Type: 13.3" 16:9 TFT Maximum Resolution: 1366 x 768			
Keyboard / Touchpad	Keyboard: 86 keys Touchpad: 2-button Glide pad			
Sound	1 x Built-in speaker			
I/O interfaces	Left side: 1 x USB 2.0 1 x Microphone port 1 x Headphone port	Right side: 1 x DC IN 1 x USB 2.0 1 x USB 3.0	Rear side: 1 x RJ-45 1 x VGA 1 x HDMI (TBD)	Display and base: 1 x Built-in microphone 1 x Webcam (optional) 1 x Built-in speaker
Networking	10/100/1000 Mb Ethernet Wi-Fi 802.11 ac/a/b/g/n (M.2 interface)			
AC Adapter	INPUT: 100-240 V, ~2.5 A, 50-60 Hz OUTPUT: 19 V, 2.1 A, 40 W			
Battery Pack	Rechargeable lithium-ion polymer battery 14.8 V, 2000 mAh, 29.6 Wh			
Operating system	Windows 10 IoT 2016 Enterprise			
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)319 x (D)223 x (H)20.5 mm			
Weight	1.2 kg (approx.)			
Environment	Operating Temperature: 5° C ~ 35° C Non-operating Temperature: -30° C ~ 60° C Operating Humidity (Rh): 10% ~ 90% (non-condensing) Non-operating Humidity (Rh): 5% ~ 95%			

Atrust