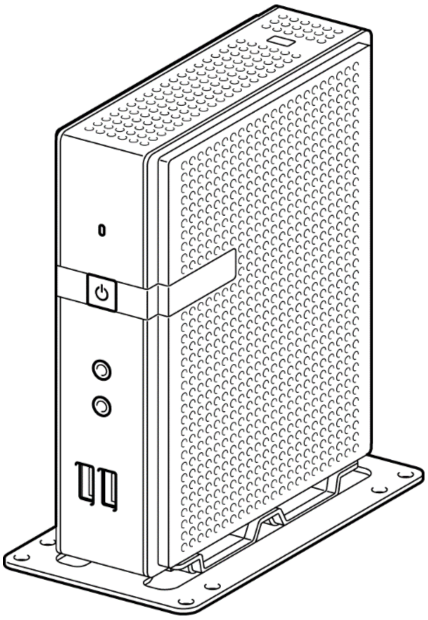
NEC



Express5800 Series

US320f User's Guide

FW Win10IoTEnt LTSB v.1.04-INTL

GZS-000949-001-00
Second Edition, JUNE 2018

Documents for US320f

Attached as a booklet or published on the website (http://www.58support.nec.co.jp/global/download/)

Safety Precautions and Regulatory Notices

For safe use, safety precautions for using this product are informed. Please be sure to read this guide.

Getting Started

Describes how to use this product, from unpacking to operations. Read this guide first for confirm an overview of US320f.

Published to the website (http://www.58support.nec.co.jp/global/download/)

User's Guide (this document)

Precautions for Use	*Be sure to read this section before using this device.* Follow the instructions described in this user's guide for your safe use of US320f.
Chapter 1: About US320f	Describes the names and features of US320f components, how to install it and connect peripherals, and system BIOS.
Chapter 2: Before Getting Started	Describes the features and information you should understand before using US320f.
Chapter 3: Using US320f	Describes the basics of how to use your US320f.
Chapter 4: Configuring Client Settings with Atrust Client Setup	Describes the client setting tools useful for US320f.
Chapter 5: Administrative Utilities and Settings	Describes the information related to administrative utilities and settings and how to use them.
Chapter 6: System Administration	Describes software for remote administration, and how to restore the system.
Chapter 7: Establishing a Server Environment	Describes the server environment required for using US320f.
Chapter 8: Software Information, Notes, and Restrictions	Describes US320f software information, and notes and restrictions on using US320f.
Chapter 9: Operation and Maintenance	Describes troubleshooting and how to keep US320f running smoothly.
Chapter 10: Appendix	

Contents

Notations Used in This Document

Notations used in the text

In addition to safety-related symbols urging caution, three other types of notations are used in this document.

These notations have the following meanings.

Important	Indicates critical items that must be observed when handling US320f or its software. If the procedures described are not followed, *hardware failure, data loss, and other serious malfunctions might occur*.
Note	Indicates items that must be confirmed when handling US320f or its software.
Tip	Indicates information that is helpful to keep in mind when using US320f.

Abbreviations of Operation Systems

In this document, Windows operating systems are referred to as follows.

Notations in this document	Official names of Windows
Windows 10	Windows 10 Enterprise 64-bit (x64) Edition
	Windows 10 Enterprise 32-bit (x86) Edition
Windows 8.1	Windows 8.1 Enterprise 64-bit (x64) Edition
	Windows 8.1 Enterprise 32-bit (x86) Edition
Windows 8	Windows 8 Enterprise 64-bit (x64) Edition
	Windows 8 Enterprise 32-bit (x86) Edition
Windows 7	Windows 7 Enterprise 64-bit (x64) Edition
	Windows 7 Enterprise 32-bit (x86) Edition
Windows 2016	Windows Server 2016 DataCenter Edition Windows Server 2016 Standard Edition
Windows 2012	Windows Server 2012 R2 Datacenter Edition Windows Server 2012 R2 Standard Edition Windows Server 2012 Datacenter Edition Windows Server 2012 Standard Edition
Windows 2008	Windows Server 2008 R2 Standard Edition Windows Server 2008 R2 Enterprise Edition Windows Server 2008 32-bit Standard Edition Windows Server 2008 32-bit Enterprise Edition Windows Server 2008 64-bit Standard Edition Windows Server 2008 64-bit Enterprise Edition

Trademarks

Adobe, Adobe logo, Adobe Flash Player, Adobe Reader are registered trademarks or trademarks of Adobe Systems Incorporated (Adobe Systems) in the United States and other countries.
Atrust is a registered trademark of Atrust Computer Corporation.
Citrix and Citrix product names are trademarks or registered trademarks of Citrix Systems, Inc. in the United States and other countries.
Intel and Celeron are trademarks of Intel Corporation or its subsidiaries in the United States and / or other countries.
Kensington is a US registered and pending trademark of ACCO Brands Corporation worldwide.
Microsoft, Windows, Windows Server, Windows Media, Windows PowerShell, Active Directory, Internet Explorer, SmartScreen are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
VMware and VMware product names are trademarks or registered trademarks of VMware, Inc. in the United States and other countries.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

Warnings and Additions to This Document

- **No part of this manual may be reproduced in any form without the prior written permission of NEC Corporation.**
- **The contents of this manual may be revised without prior notice.**
- **The contents of this manual should not be copied or altered without the prior written permission of NEC Corporation.**
- **Every effort has been made to ensure the completeness of this document. However, if you have any concerns, or discover errors or omissions, please contact your retailer.**
- **Notwithstanding item 4 above, NEC Corporation is not liable for any damage resulting from the use of this product.**
- **The sample values used in this document are not the actual values.**

Keep this document nearby so that you may refer to it as necessary.

This document was created based on the information available at the time of its creation. The screen images, messages, and procedures may differ from the actual screens, messages, and procedures. Substitute as appropriate when content has been modified. The most recent version of User's Guide, as well as other related documents, is also available for download from the following website.

http://www.58support.nec.co.jp/global/download/

To find the necessary information

To find the necessary information in the digital manuals, open the relevant document and enter a word or a phrase, or a part of phrase, in the **Search** window or on the **Find** toolbar. Refer to the help of your PDF reader for more details.

Confirmation of Accessories

Refer to the attached startup guide to confirm the accessories in the US320f packing box.

If you find any missing or damaged accessories, contact your service representative for a replacement.

Transfer to Third Parties

When transferring or reselling this product to a third party, make sure to provide this guide, the attached license agreement, and all the accessories along with US320f.

Disposal

Dispose of US320f, the battery, and all the optional devices according to national laws and regulations. Also dispose of the power cord provided with US320f to prevent it being used for other devices.

Shipping

A lithium metal battery or a lithium ion battery is used for US320f and its optional devices.

Aviation and marine transportation regulations apply when transporting lithium batteries, so confirm these regulations with your service representative before arranging shipment of US320f.

License, Rights, and Regulatory Compliance

Rights

Restricted Rights Legend

You acknowledge that the Software is of U.S. origin. You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments. For additional information about exporting the Software, see http://www.microsoft.com/exporting.

Regulatory Compliance for Thin Clients

AC Adapter

Use ADP-36JH included in the packing box of US320f as the external power supply unit.

Important **Use only the AC adapter that comes with US320f. Using an AC adapter that does not meet the required electrical specifications may cause a fire, malfunction, or fault to occur.**

FCC Statement

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.

This Class B digital apparatus complies with CAN ICES-3(B)/NMB-3(B)

Note: 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 or more 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.

Industry Canada Class B Emission Compliance Statement/ Avis de conformité à la réglementation d'Industrie Canada

CAN ICES-3(B)/NMB-3(B)

WEEE Directive

Disposing of your used product

In the European Union

EU-wide legislation as implemented in each Member State requires that used electrical and electronic products carrying the mark (left) must be disposed of separately from normal household waste. This includes Information and Communication Technology (ICT) equipment or electrical accessories, such as cables.

When disposing of used products, you should comply with applicable legislation or agreements you may have. The mark on the electrical and electronic products may only apply to the current European Union Member States.

Outside the European Union

If you wish to dispose of used electrical and electronic products outside the European Union, please contact your local authority and ask for the correct method of disposal.

Turkish RoHS information relevant for Turkish market

EEE Yönetmeliğine Uygundur

Vietnam RoHS information relevant for Vietnam market

Complying with “CIRCULAR, No.30/2011/TT-BCT (Hanoi, August 10 2011), Temporary regulations on content limit for certain hazardous substances in electrical products”

台灣電池規制 (廢棄物清理法)

廢電池請回收

限用物質含有情況標示聲明書 (Declaration of the Presence Condition of the Restricted Substances Marking)

設備名稱：精簡型電腦 型號（型式）：Atrust t180						
單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr+6)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板	-	○	○	○	○	○
配件 (電源線、排線等)	-	○	○	○	○	○
外殼	○	○	○	○	○	○
電源供應器	-	○	○	○	○	○
鈕扣電池	○	○	○	○	○	○
螺絲	-	○	○	○	○	○
備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。 備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。 備考3.〝−〞係指該項限用物質為排除項目。						

Precautions for Use (Be Sure to Read)

The following provides information required to use your product safely and properly. For definitions of the names in this section, refer to *Names and Functions of Components* in this document.

Safety Precautions

Follow the instructions in this document for the safe use of US320f.

This User's Guide describes hazardous parts of US320f, possible hazards, and how to avoid them.

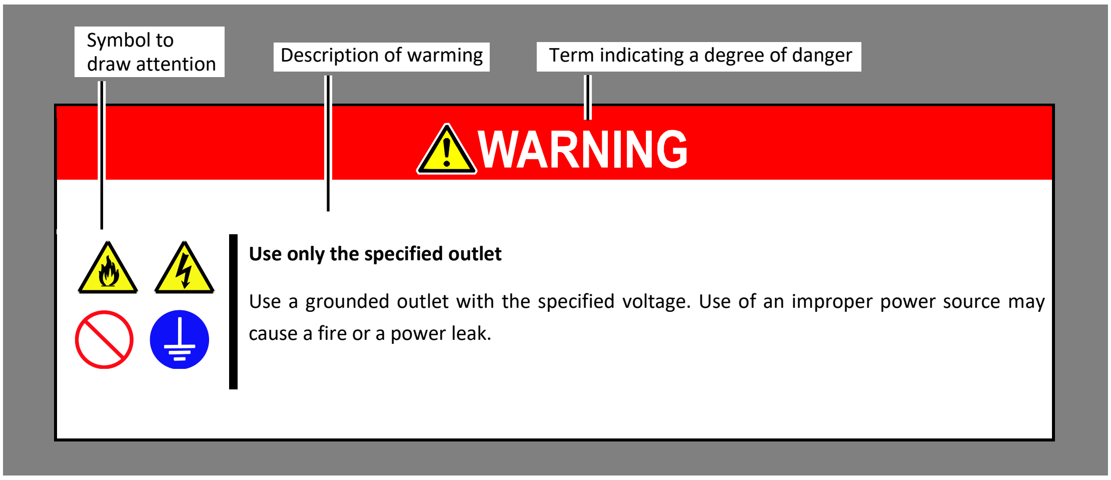
In User's Guide or on warning labels, WARNING or CAUTION is used to indicate a degree of danger. These terms are defined as follows:

⚠WARNING	Indicates there is a risk of death or serious personal injury.
⚠CAUTION	Indicates there is a risk of burns, other personal injury, or property damage

Precautions and notices against hazards are presented with one of the following three symbols. The individual symbols are defined as follows:

△	Attention	This symbol indicates the presence of a hazard if the instruction is ignored. An image in the symbol illustrates the hazard type.	Example Electric shock risk ⚠
⃠	Prohibited action	This symbol indicates prohibited actions. An image in the symbol illustrates a particular prohibited action.	Example Do not disassemble ⃠
●	Mandatory action	This symbol indicates mandatory actions. An image in the symbol illustrates a mandatory action to avoid a particular hazard.	Example Disconnect a plug ●

An indication example of user's guide



Use only the specified outlet

Use a grounded outlet with the specified voltage. Use of an improper power source may cause a fire or a power leak.

Symbols Used in This document and on Warning Labels

Attention

⚠	Indicates the presence of electric shock hazards	⚠	Indicates there is a risk of smoke emission or fire.
⚠	Indicates there is a risk of explosion	⚠	Indicates the presence of mechanical parts that can result in pinching or other bodily injury.
⚠	Indicates a general notice or warning that cannot be specifically identified.	⚠	Indicates the presence of a hot surface or component. Touching this surface can result in a burn.

Prohibited actions

🛇	Indicates the presence of a hot surface or component. Touching this surface can result in a burn.	🛇	Do not use US320f in the place where water or liquid may pour. This can result in an electric shock or fire.
🛇	Do not touch the component specified by this symbol. This can result in an electric shock or burn.	🛇	Do not place US320f near the fire. This can result in a fire.
🛇	Do not touch US320f with wet hands. This can result in an electric shock.	🛇	Indicates a general prohibited action that cannot be specifically identified.

Mandatory actions

●	Unplug the power cord of US320f. If the cord is not unplugged it can result in an electric shock or fire.	❗	Indicates a mandatory action that cannot be specifically identified. Make sure to follow the instruction.
⏚	Make sure equipment is properly grounded. If the equipment is not properly grounded, it can result in an electric shock or fire.		

Safety notes

This section provides notes on using US320f safely. Read this section carefully to ensure proper and safe use of US320f. For symbols, refer to *Safety Precautions*.

General

⚠WARNING

Do not use US320f for services which may directly affect human lives and for which critically high reliability is required.

US320f is not intended to be used with or control facilities or devices impacting human lives, including medical devices, nuclear facilities and devices, aeronautics and space devices, transportation facilities and devices, and facilities and devices requiring high reliability. NEC assumes no liability for any accident resulting in personal injury, death, or property damage if US320f has been used for the above applications.

Do not use US320f if any smoke, odor, or noise is present.

If smoke, odor, or noise is present, immediately turn off US320f and disconnect the power plug from the outlet. Then contact the store where you purchased the product or your maintenance service company. Using US320f under such conditions may cause a fire.

Do not insert wires or metal objects.

Do not insert wires or metal objects into ventilation holes or USB connectors. Doing so may cause an electric shock.

⚠CAUTION

Keep water or foreign matter away from US320f.

Do not let any liquid such as water or foreign materials including pins or paper clips enter US320f. Failure to follow this warning may cause an electric shock, a fire, or failure of US320f. If liquid or foreign matter accidentally enters US320f, immediately turn off the power and disconnect the power plug from the outlet. Do not disassemble US320f. Contact the store where you purchased the product or your maintenance service company.

Power supply and power cord

⚠WARNING

Do not hold the power plug with wet hands.

Do not disconnect or connect the plug while your hands are wet. Failure to follow this warning may cause an electric shock.

Do not connect the ground wire to a gas pipe.

Never connect the ground wire to a gas pipe. Failure to follow this warning may cause a gas explosion.

Do not connect or disconnect the ground wire while the power cord is connected.

Connect or disconnect the ground wire after disconnecting the power cord from the outlet.
Even if the power supply is turned off, if you touch the ground wire while the power cord is connected to the outlet, you might receive an electric shock, or cause shorting, which could lead to fire.

⚠CAUTION

Plug in to a proper power source.

Use a grounded outlet with the specified voltage. Use of an outlet with a voltage other than that specified can cause fire or electrical leakage. Do not install US320f in any environment that requires an extension cord. Connecting to a cord that does not conform to the power supply specifications of US320f can cause overheating, resulting in a fire.

If you want to use an AC cord set with a ground wire of class 0I, be sure to connect the ground wire before inserting the power plug into the outlet. Before disconnecting the ground wire, be sure to disconnect the power plug from the outlet.

Do not connect many cords into a single outlet by using extension cords.

This can cause the electric current to exceed the rated flow and overheat the outlet, which may cause a fire.

Insert the power plug into the outlet as far as it goes.

Heat generation resulting from a halfway inserted power plug (imperfect contact) may cause a fire. Heat will also be generated if condensation is formed on dusty blades of the halfway inserted plug, increasing the possibility of fire.

Do not unplug the power cord by holding the cable part.

Pull the power cord straight out by holding the plug. Pulling the power cord by holding the cable part or applying extra pressure to the connector may damage the cable part, which may cause a fire or electric shock.

⚠ CAUTION

Use the authorized power cord only.

Use only the power cord that comes with US320f. If an electric current exceeding the rated current flows, it could cause a fire. Also, observe the following precautions to prevent electrical shock or fire caused by a damaged power cord.

- Do not stretch the cord harness.
- Do not bend the power cord.
- Do not twist the power cord.
- Do not step on the power cord.
- Uncoil the power cord before use.
- Do not secure the power cord with staples or equivalent objects.
- Do not pinch the power cord.
- Keep chemicals away from the power cord.
- Do not place any object on the power cord.
- Do not alter, modify, or repair the power cord.
- Do not use a damaged power cord. (Replace the damaged power cord with a power cord of the same standard. For information about replacing the power cord, contact the store where you purchased the product or your maintenance service company.)

Do not use the attached power cord for any other device or usage.

The power cord that comes with US320f is designed to connect with US320f and to be used with US320f, and its safety has been tested. Do not use the attached power cord for any other purpose. Doing so may cause a fire or an electric shock.

Installation, relocation, storage, and connection

⚠ CAUTION

Do not install US320f in other than the specified location.

Do not install US320f in the following places or any place other than one specified in this User's Guide. Failure to follow this instruction may cause a fire.

- A dusty place
- A humid place such as near a boiler
- A place exposed to direct sunlight
- An unstable place

Do not use US320f in an environment where corrosive gases exist

Do not install US320f in a place subject to corrosive gases including sodium chloride, sulfur dioxide, hydrogen sulfide, nitrogen dioxide, chlorine, ammonia, or ozone. Do not install US320f in an environment that contains dust, chemicals that accelerate corrosion such as sodium chloride or sulfur, or conductive materials. Failure to follow this warning may cause the wiring on the printed wiring board to short-circuit, leading to fire. If you have any questions, contact the store where you purchased the product or your maintenance service company.

Battery unit

⚠WARNING

Do not put the battery in fire

Putting the battery in fire or heating the battery may cause an explosion.

Do not disassemble or alter the battery unit.

Do not disassemble or alter the battery unit. Doing so may cause an explosion or liquid leakage. The quality, performance, and/or safety of the battery unit will not be guaranteed if it is disassembled or altered.

⚠CAUTION

Keep the battery out of the reach of children and babies.

The toxic substance contained in the battery is harmful if it is taken into the body by mistake. Consult your doctor immediately if it is swallowed.

During Operation

⚠CAUTION

Avoid contact with US320f during thunderstorms.

Disconnect the power plug from the outlet when a thunderstorm is approaching. If it lightening occurs before you disconnect the power plug, do not touch any part of US320f including the cables. Failure to follow this warning may cause a fire or an electric shock.

Keep animals away from US320f.

Keep animals such as pets away from US320f. Pet hair or other waste can enter US320f, which may cause a fire or electric shock.

Do not block the ventilation opening.

This can cause the internal temperature to rise, which may cause fumes and/or fire.

Remove headphones before connection.

Do not connect headphones to the line-out connector of US320f while you are wearing them. Doing so may damage your ears.

Turn down the volume before connecting headphones.

Pay attention to the ventilation opening.

The temperature of the ventilation opening and its periphery is higher than room temperature. Exposing yourself to exhaust from the ventilation opening may cause a low temperature burn. Special care must be taken if you have sensitive skin.

Cleaning and working with internal devices

⚠ **CAUTION**

Do not disassemble, repair, or alter US320f.

Never attempt to disassemble, repair, or alter US320f under any circumstances. Failure to follow this instruction may cause an electric shock or fire as well as malfunction of US320f.

Disconnect the power plug before opening US320f.

Make sure to power off US320f and disconnect the power plug from the power outlet before cleaning the unit or attaching and detaching cables. Touching the inside of US320f with its power cord connected to a power source may cause an electric shock even if US320f is powered off.
Disconnect the power plug from the outlet occasionally and clean the plug with a dry cloth. Heat will be generated if water droplets are formed on a dusty plug, which may cause a fire.

For Proper Operation

Observe the following notes for successful operation of US320f. Ignoring these notes can cause malfunction or failure of US320f.

- When you have just turned off US320f, wait at least 10 seconds before turning it back on. If US320f is connected to an uninterruptible power supply (UPS), set a delay of at least 10 seconds in the power-on schedule.
- Turn off the power of US320f and unplug the power cord from the outlet before relocating US320f.
- Clean US320f on a regular basis. Regular cleaning proactively prevents various failures.
- Lightning may cause a momentary voltage drop. To prevent this problem, it is recommended to use an uninterruptible power supply (UPS) unit.
- It is recommended that US320f should be stored in a place where a stable room temperature is able to be maintained. It is preferable to store US320f under conditions of temperature: –10°C to 55°C (14°F to 131°F), humidity: 10% to 95% (non-condensing).
- Turn off cellular phones or pagers around US320f. Radio interference may cause malfunction of US320f.
- Observe the following notes on using and connecting an interface cable.
  - Do not use a damaged cable.
  - Do not step on the cable.
  - Do not place any object on the cable.
  - Do not use US320f with loose cable connections.
- If US320f or the option devices (add-ons) connected inside US320f are moved suddenly from a cold environment to a warm environment, condensation might form inside US320f or its add-ons, causing malfunction or damage if US320f is used in this state. To protect your important data and assets, be sure to consider the environment carefully before using US320f.
- Make sure that all add-ons and peripherals are able to be attached or connected to US320f. Note, however, that even if add-ons or peripherals can be physically attached or connected, they might damage US320f if they do not work properly.
- We recommend only using official NEC add-ons. Add-ons such memory sticks or hard disk drives from other companies might be able to be used with US320f, but if these add-ons cause US320f to fail or become damaged, NEC will not cover the cost of repair, even if the damage occurs within the warranty period.

Advice for Health

The longer you keep using computer equipment, the more tired you become, which may affect your health and wellbeing. When you use a computer, observe the following to keep yourself from getting tired:

Good Working Posture
You will have good posture if you observe the following when using a computer:

You sit on your chair with your back straight.

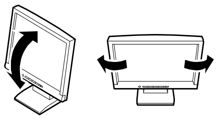
Your hands are parallel with the floor when you put them on the keyboard.

You look at the screen slightly lower than your eye height.

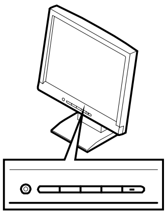
You have "good working posture" as described above when no part of your body is under excess strain, in other words when your muscles are most relaxed.

You have "bad posture" when you sit with your back hunched up or you operate a display unit with your face close to the screen. Bad working posture may cause eye strain or poor eyesight.

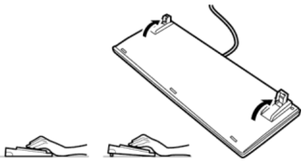
Adjustment of Display Unit Angles
Most display units are designed for adjustment of the horizontal and vertical angles. This adjustment is important to prevent the screen from reflecting bright lights and to make the display contents easy to see. You will not be able to maintain your good working posture and you will feel more tired than you should if you operate a display unit without adjusting horizontal and vertical angles.



Adjustment of Screen Brightness and Contrast
The display unit has brightness and contrast adjustment functions. The most suitable brightness and contrast depend on the individual and the working environment (well-lit room versus insufficient light). Adjust brightness and contrast so that the screen will be easy to see. An extremely bright or dark screen will have a bad effect on your eyes.



Adjustment of Keyboard Angle
The angle of the keyboard provided with the server can be adjusted. Adjust the keyboard to an angle at which it is easy to operate. Adjustment assists in reducing strain on your shoulders, arms, and fingers.



Cleaning of Equipment
Clean equipment regularly. It is difficult to see contents on a dusty screen. Keeping equipment clean is also important for your eyesight.

Fatigue and Rest
If you feel tired, you should stop working and do light exercises.

NEC Express5800 Series
US320f

1

Chapter 1 About US320f

This chapter describes the features of US320f and the names of the components.

1. **Introduction**
   provides an overview of US320f

2. **Names and Functions of Components**
   Describes the names and functions of US320f components.

3. **Installation and Connection**
   Describes how to install and connect US320f.

4. **Setting up the System BIOS**
   Describes how to set up the Basic Input Output System (BIOS).

1. Introduction

Thank you for purchasing NEC Express5800 Series thin client US320f.

US320f is a desktop thin client terminal that is designed to configure a virtual PC thin client system.

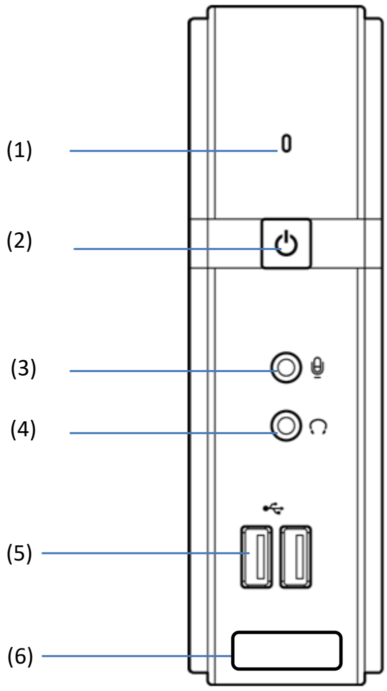
US320f incorporates a dedicated operating system and has a hardware configuration suitable for thin client purposes, thereby providing secure business system.

Read this document thoroughly before using US320f to fully understand the handling of US320f, and appreciate its functions to the maximum extent.

2. Names and Functions of Components

This section describes the names and functions of US320f components.

2.1 Front View



(1) Status LED (Blue: normal state, Orange: standby state) (*1)

(2) Power switch

(3) Microphone connector

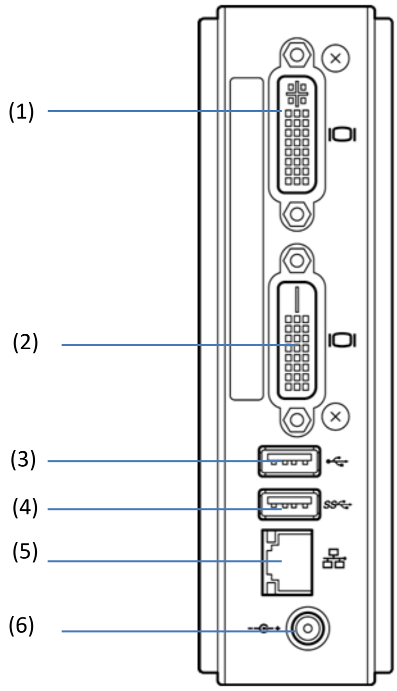
(4) Headphone connector

(5) USB 2.0 ports (2 ports)

(6) COA label (*2)

*1. US320f does not support standby operations.
*2. Do not remove this label.

2.2 Rear View



(1) DVI-I port	(4) USB 3.0 port (*1)
(2) DVI-D port	(5) LAN connector
(3) USB 2.0 port	(6) Power connector

*1. The USB 3.0 port on US320f operates in USB 2.0 mode.

2.2.1 DVI-I port

A monitor conforming to the DVI standard can be connected to the DVI-I port.

An analog monitor can be connected to the DVI-I port by using the supplied DVI-VGA adapter.

Important **Do not connect any device other than US320f to the DVI-VGA adapter.**

2.2.2 DVI-D port

A monitor conforming to the DVI standard can be connected to the DVI-D port.

Note The DVI-VGA adapter cannot be connected to the DVI-D port.

2.2.3 USB 2.0 port

Three USB ports are located on US320f to connect peripherals conforming to the USB 2.0 standard (such as keyboard, mouse, and HDDs) to US320f.

Note US320f cannot be woken up from a USB 2.0 port.

2.2.4 USB 3.0 port

One USB port is located on US320f to connect peripherals conforming to the USB 2.0 standard (such as keyboard, mouse, USB flash drives and HDDs) to US320f.

Note

- US320f cannot be woken up from a USB 3.0 port.
- The USB 3.0 port on US320f operates in USB 2.0 mode.

2.2.5 LAN connector

Use this connector to connect to the LAN by using a network cable.

Note The Wake-on-LAN feature operates only after Windows is started.

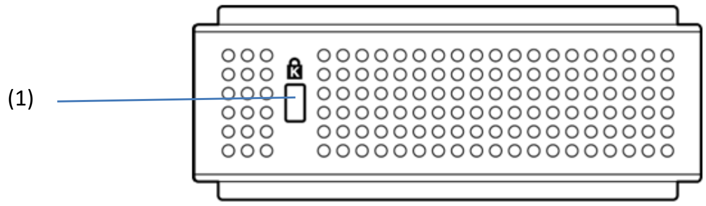
If the DC plug is disconnected from the power connector or the power cord is disconnected from the outlet, you need to start the OS again.

2.2.6 Power connector

Use the AC adapter that comes with US320f.

Important **Be sure to use the AC adapter and power cord that comes with US320f. Using another adapter or power cord may cause the system to be damaged even if they seem to be the same as the ones that come with US320f.**

2.3 Top View



(1) Security slot

3. Installation and Connection

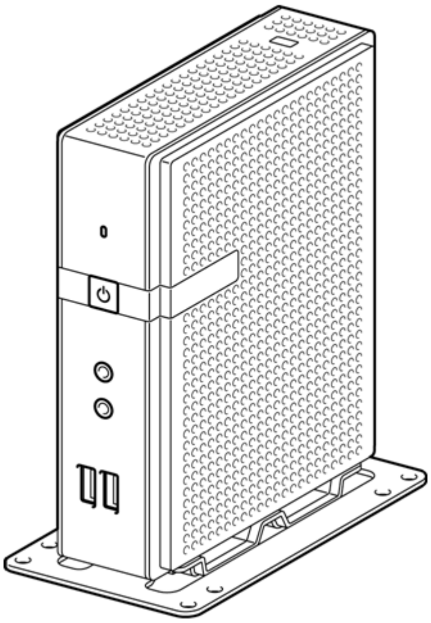
This section describes how to install and connect US320f.

3.1 Installation

Install US320f by using the stand that comes with US320f.

3.1.1 Placing on a desk

Place US320f (with its stand) on a desk or similar place in an upright position.

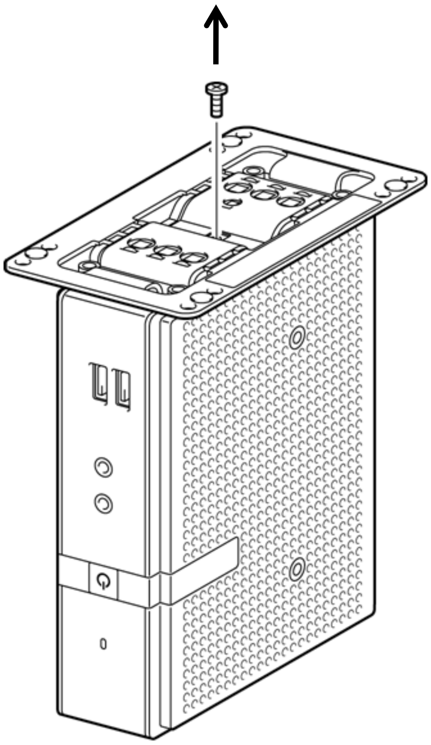


3.1.2 Mounting on the back of a monitor

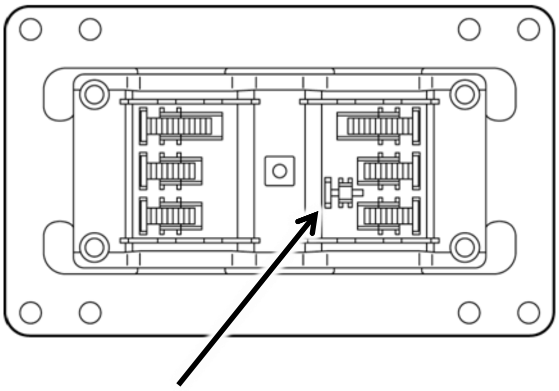
Mount US320f on the back of a monitor by using the stand.

You can mount your US320f on a monitor conforming to VESA.

1. Place your US320f with its bottom facing up, and remove the screw located in the center.



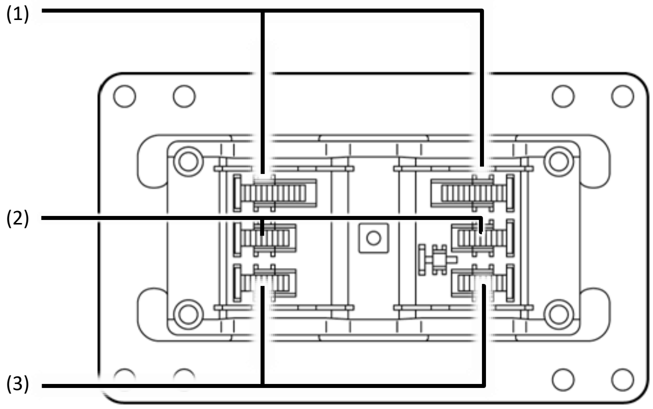
Store the removed screw inside the stand.



The screw head must face inside.

Important **It is highly recommended to store screws inside the stand when not needed to prevent them getting lost.**

2. Remove the four screws from the stand.



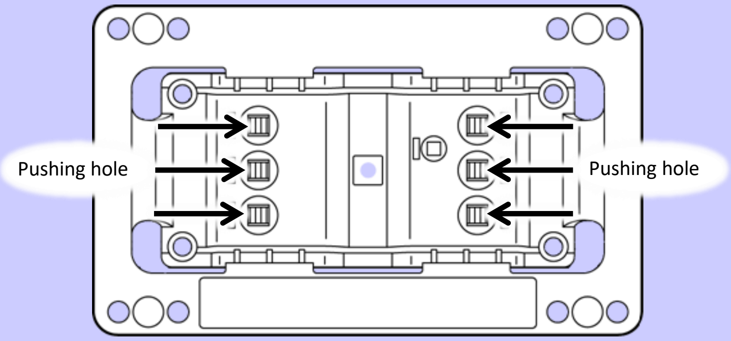
(1) Fixing screw for monitor (long) (Approx. 13 mm)

(2) Fixing screw for monitor (short) (Approx. 10 mm)

(3) Fixing screw for body

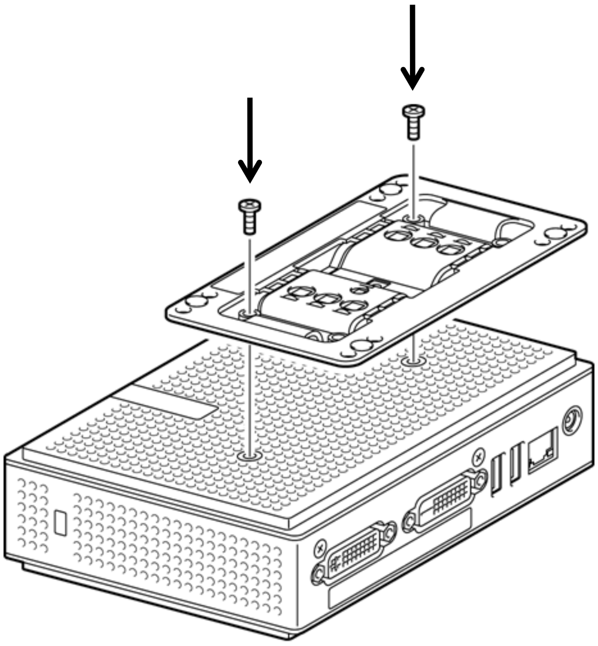
Tips

- Use only one type of screw (long or short).
- Select screws having a length appropriate to your monitor according to the instruction manual that comes with your monitor.
- If it is hard to remove the screw, push the screw up from the hole underneath by using a thin screwdriver.

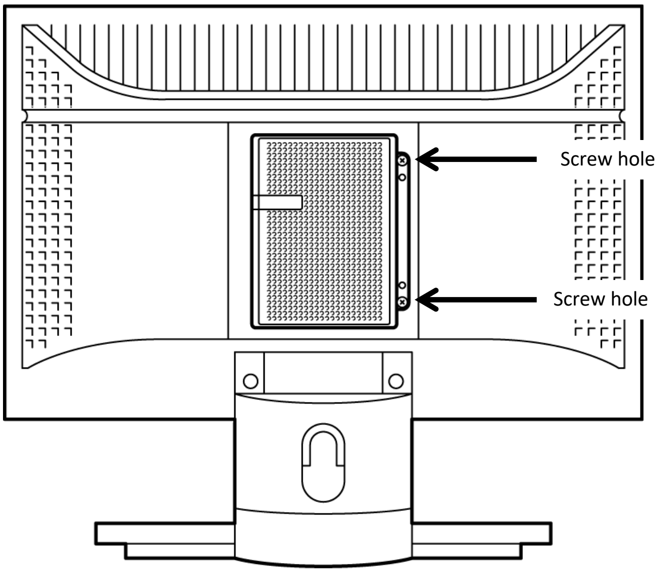


- If the screwdriver is too thin (or too thick) for the screw, the screw thread may be damaged. Use the proper screwdriver.

3. Mount the stand on US320f by using the screws for the body.



4. Use the screws for the monitor to mount US320f on the mounting holes on the monitor so that the front of US320f faces left. See the figure below.



Tips

- Use two screws to mount US320f on the monitor.
- The location of the mounting holes depends on the monitor size.
  Refer to the manual that comes with your monitor.
- To remove US320f from the monitor, reverse the steps (1) through (4) in "3.1.2 Mounting on the back of a monitor" to remove US320f and mount the stand.

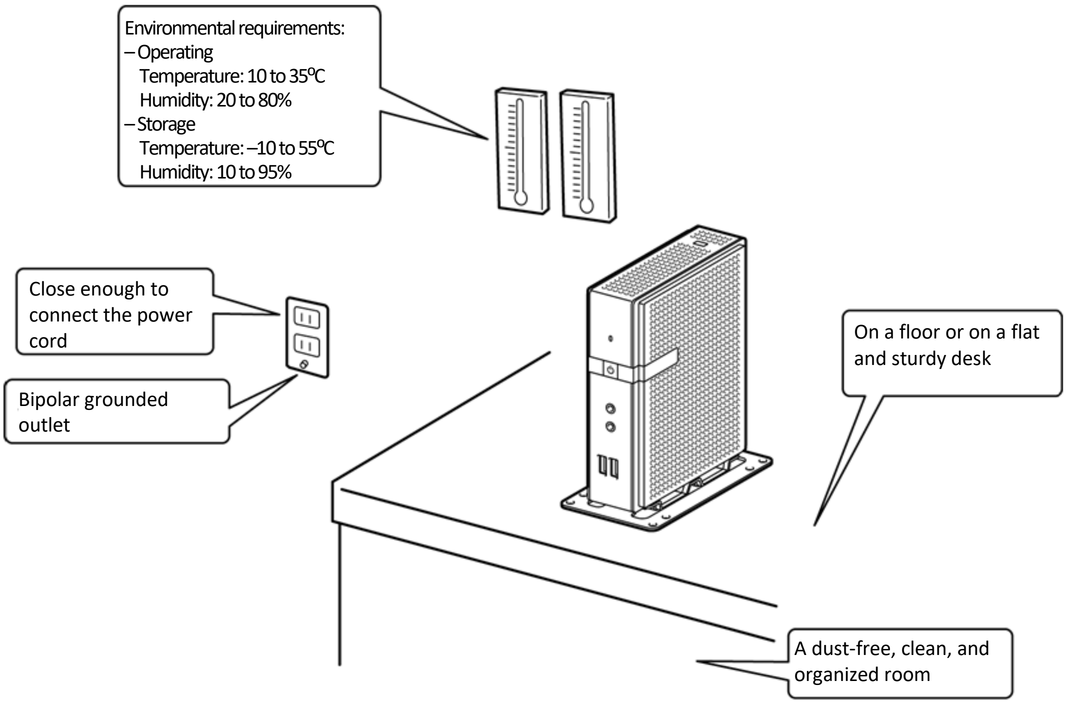
Important

- **Do not use US320f with the stand being removed.**
- **Do not change combination of US320f and the stand.**

⚠ CAUTION

Observe the following instructions to use US320f safely. Failure to follow these instructions may cause a fire, personal injury, or property damage. For details, see *Precautions for Use*.

- **Do not install US320f in other than the specified locations.**


Environmental requirements:
– Operating
Temperature: 10 to 35ºC
Humidity: 20 to 80%
– Storage
Temperature: –10 to 55ºC
Humidity: 10 to 95%
Close enough to connect the power cord
Bipolar grounded outlet
On a floor or on a flat and sturdy desk
A dust-free, clean, and organized room

Do not place US320f in the following places. Otherwise, US320f might malfunction.

- Places with drastic changes in temperature (such as near a heater, air conditioner, or refrigerator)
- Places with strong vibration
- Places subject to corrosive gases (an environment where sulfur vapor may be dispersed in the air)
- Places where chemicals are nearby or chemicals may be sprayed accidentally.
- On a non-antistatic carpet
- Places where objects might fall down easily
- Places where the power cord or interface cable may be stepped or tripped on
- Places near a device generating an intense magnetic field (such as a TV, radio, broadcast/communication antenna, power transmission wire, and electromagnetic crane) (If unavoidable, contact your service representative to request proper shield construction.)
- Places where a power outlet that shares the ground line with another device (especially one with a large power consumption) must be used for US320f
- Places near equipment that generates power noise (for example, contact sparks when powering-on or powering-off a commercial power supply via a relay). (To install US320f near equipment that generates power noise, ask your service representative to separate the power wiring or install a noise filter.)

3.2 Connection

Connect US320f to your network.

After connecting the network cable and other cables, connect the AC adapter that comes with US320f to US320f and plug the power cord into the wall socket.

⚠WARNING

Observe the following instructions to use US320f safely. Failure to follow these instructions may result in death or serious personal injury. For details, see *Precautions for Use*.

- Do not hold the power plug with a wet hand.

⚠CAUTION

Observe the following instructions to use US320f safely. Failure to follow these instructions may cause a fire, personal injury, or property damage. For details, see *Precautions for Use*.

- Plug into a proper power source of the specified voltage.
- Do not connect exceeding number of power cords to a power outlet to prevent excessive electrical load.
- Do not use US320f with any loose interface connection.
- Use the authorized power cord only.
- Do not connect any interface cable with the power cord of US320f being connected to a power source.
- Do not use any unauthorized interface cable.

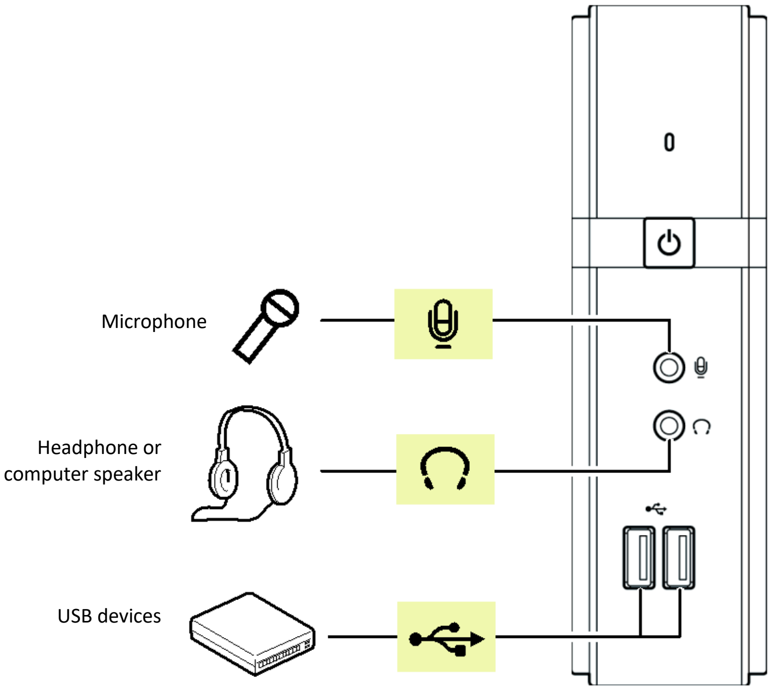
Important

- **Before connecting US320f, turn off US320f and peripherals to be connected. Failure to follow this may cause malfunction or failure.**
- **Before connecting a third-party peripheral or interface cable to US320f, ask the dealer whether the device or cable can be used for US320f. Some third-party devices cannot be used for US320f. NEC does not bear any responsibility for faults caused by using third-party peripherals or interface cables not authorized by NEC.**

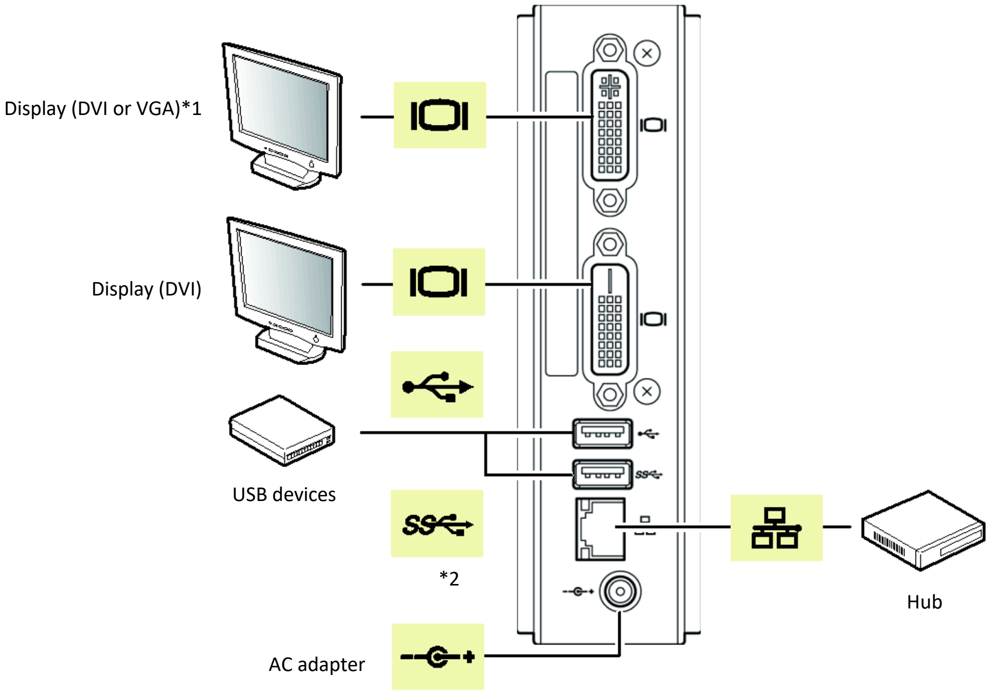
Note

To connect a display via a VGA interface, use the DVI-VGA adapter that comes with US320f.

Front view



Rear view



*1. Use the supplied DVI-VGA adapter to connect a display that uses a VGA interface.
*2. The USB 3.0 port is disabled by the factory default settings.

4. Setting up the System BIOS

This section describes how to set up the Basic Input Output System (BIOS).

Read this section before installing US320f or adding or removing optional devices.

4.1 Overview

SETUP is a utility intended for basic hardware setup. The SETUP utility can run without any exclusive utilities because it is installed in the flash memory incorporated in US320f.

Because the SETUP settings specified at shipment are the most standard and optimal settings, SETUP is not required in most cases. Use SETUP in the cases described below as necessary.

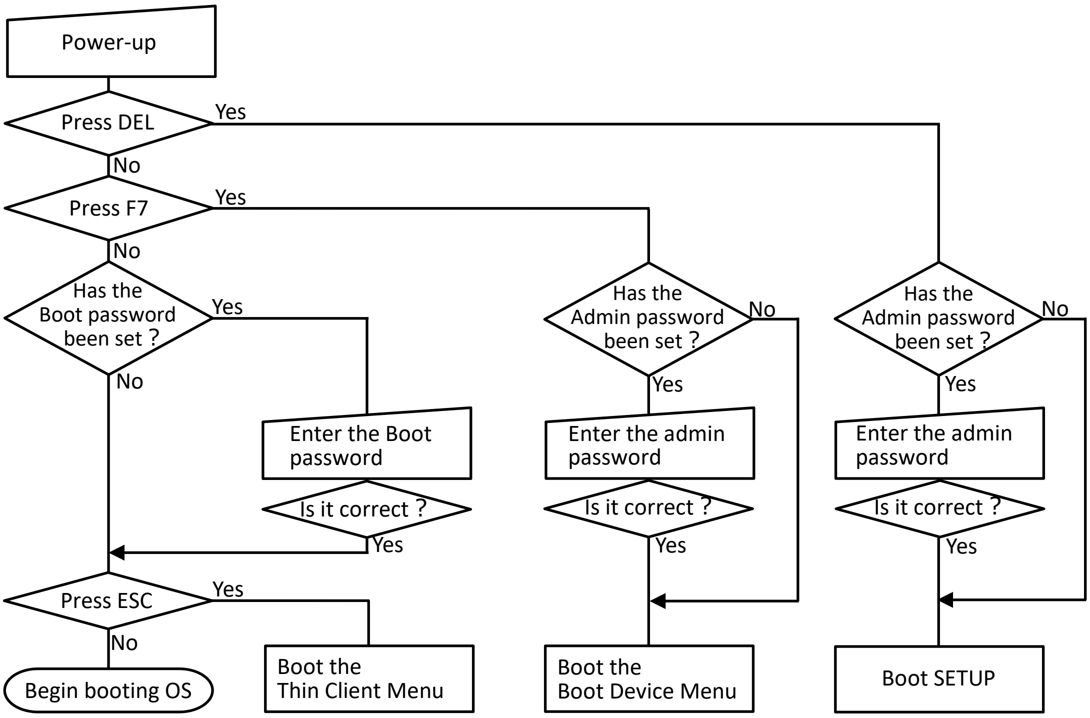
Important

- **Ask the system administrator to operate SETUP.**
- **SETUP allows you to set passwords.**
- **The latest version SETUP is installed in US320f. Accordingly, the actual setting screens may differ from those described in this guide. For the actual setting items, see the online help or contact your service representative.**
- **Be sure to close SETUP by selecting the Save & Exit menu or pressing <ESC> key or < F4> key.**
- **Turning off the power of US320f or resetting US320f with SETUP activated may cause the settings of SETUP to be updated incorrectly.**

4.2 Starting SETUP

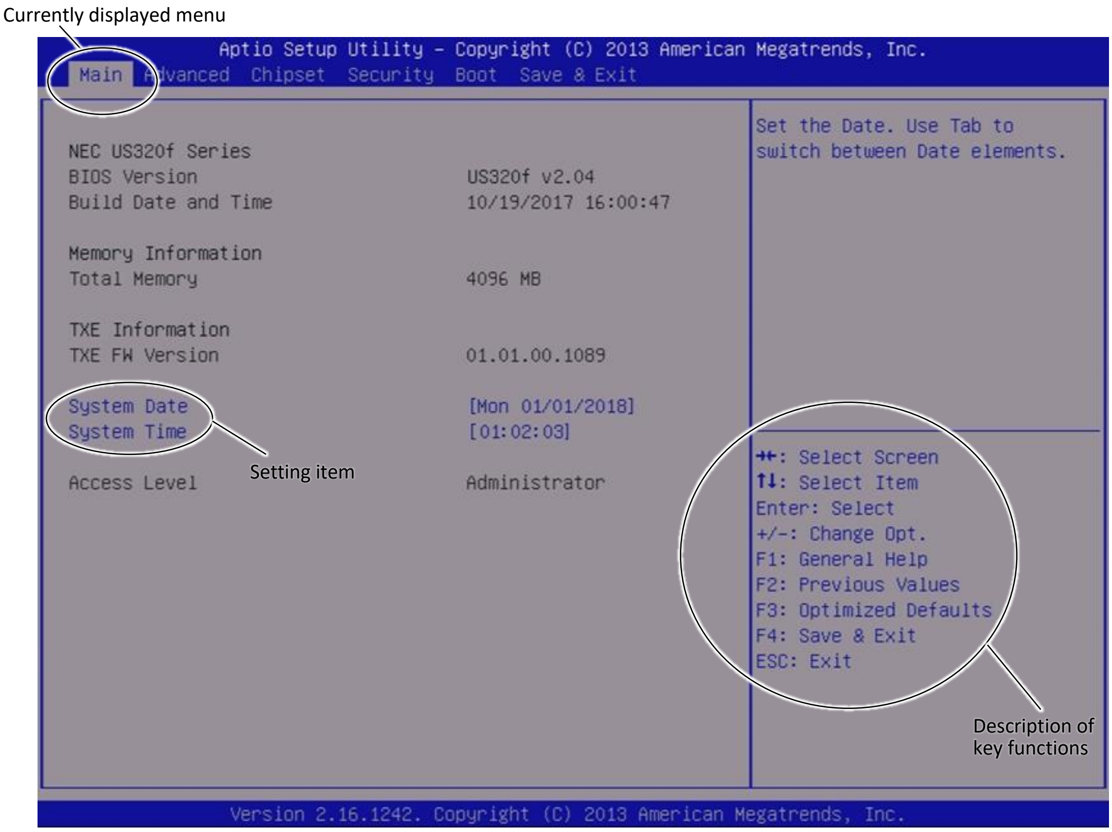
When power is turned on, the BIOS diagnostic screen appears briefly. Press the <DEL> key while this screen is displayed to start SETUP. The Main menu is then displayed.

Following the flowchart, you can load the Boot Device Menu and Thin Client menu by pressing the <F7> and <ESC> keys.



4.3 Keys and Screens

You can use the following keys to operate SETUP. (The functions of keys appear at the bottom right of the screen.)



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.

NEC US320f Series
BIOS Version                          US320f v2.04
Build Date and Time                   10/19/2017 16:00:47

Memory Information
Total Memory                          4096 MB

TXE Information
TXE FW Version                        01.01.00.1089

System Date                           [Mon 01/01/2018]
System Time                           [01:02:03]

Access Level                          Administrator

Set the Date. Use Tab to
switch between Date elements.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

Cursor keys (<←>, <→>)	Used to select the **Main**, **Advanced**, **Chipset**, **Security**, **Boot**, or **Save & Exit** menu.
Cursor keys (<↑>, <↓>)	Used to select an item appearing on the screen. The highlighted item is the currently selected item.
<+> key /<–> key	Used to change the value (parameter) of the selected item.
<+> key	Changes the current value of the selected item to the next value (increment).
<–> key	Changes the current value of the selected item to the previous value (decrement).
<F1> key	Displays the help of the key operations on the SETUP screen.
<F2> key	Returns all the settings to the values before the change. *1
<F3> key	Returns all the settings to their default values. *1
<F4> key	Used to save the set parameters and exit from SETUP.
<Esc> key	Used to return to the previous screen. If you press this key continuously, the cursor advances to the **Save & Exit** menu.
<Enter> key	Used to select a submenu.

*1. **Boot option Priorities** and **Hard Drive BBS Priorities** on the **Boot** tab and **Administrator Password** and **User Password** on the **Security** tab are excluded.

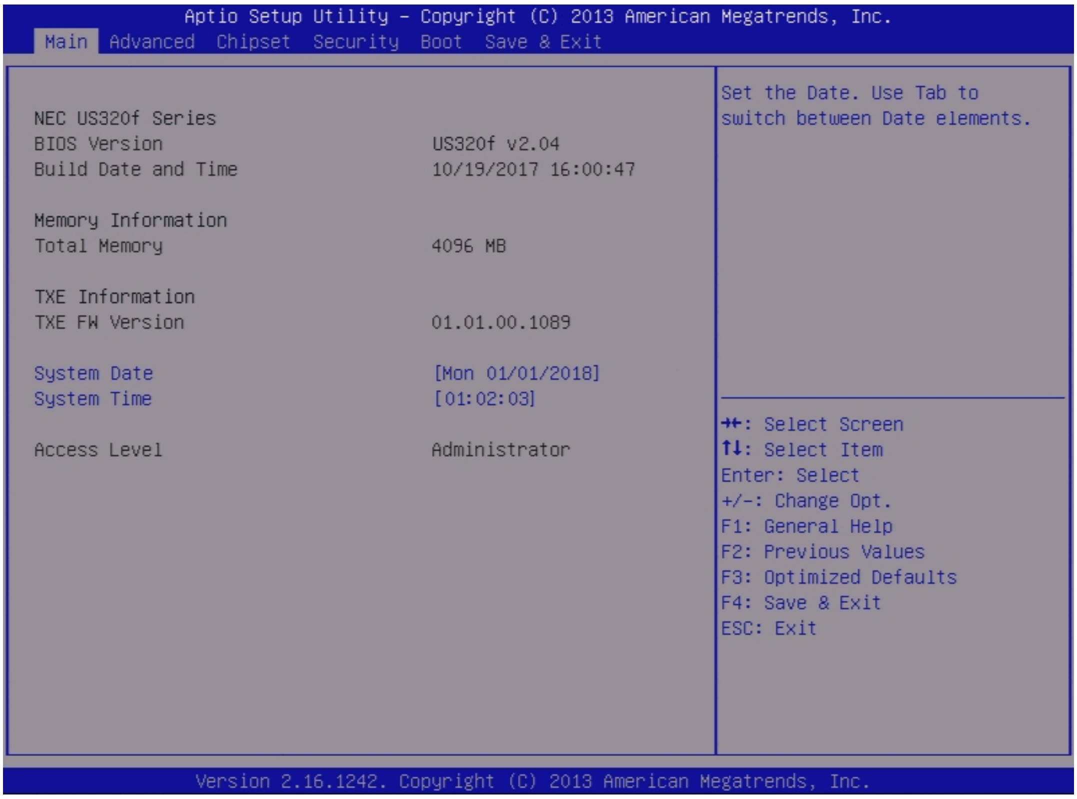
4.4 Parameters

4.4.1 Main

The SETUP screen includes the following six main menus:

- Main
- Advanced
- Chipset
- Security
- Boot
- Save&Exit

You can select a submenu that belongs to a main menu to see detailed functions.
The following describes the functions and parameters available in the menus displayed on the screen and the values of the parameters at shipment.



```
        Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
  Main  Advanced  Chipset  Security  Boot  Save & Exit

  NEC US320f Series                                      Set the Date. Use Tab to
  BIOS Version                   US320f v2.04            switch between Date elements.
  Build Date and Time            10/19/2017 16:00:47

  Memory Information
  Total Memory                   4096 MB

  TXE Information
  TXE FW Version                 01.01.00.1089

  System Date                    [Mon 01/01/2018]
  System Time                    [01:02:03]
                                                         →←: Select Screen
  Access Level                   Administrator           ↑↓: Select Item
                                                         Enter: Select
                                                         +/-: Change Opt.
                                                         F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The items that can be set on the **Main** menu screen and their functions are described below.

Item	Parameter	Description
System Date	[Weekday] MM/DD/YYYY	Set the date.
System Time	HH:MM:SS	Set the time.

Important

Be sure to confirm that the date and time are set appropriately by using the relevant BIOS parameters. Check and adjust the system clock before using US320f in any of the following circumstances:

- **After transportation of US320f**
- **After storage of US320f**

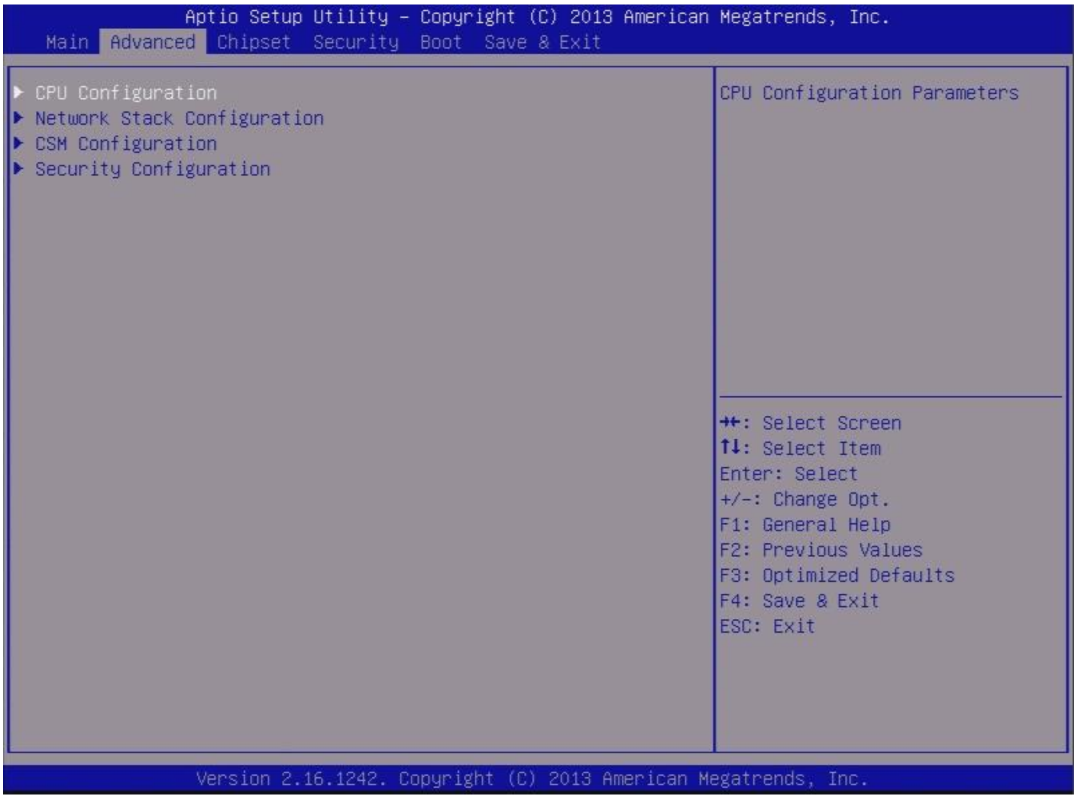
Check the system clock about once a month.

- **If the system clock gains or loses a significant amount of time as time passes even if you adjust the time, contact your service representative and request maintenance.**

4.4.2 Advanced menu

If you move the cursor to **Advanced**, the **Advanced** menu appears.

If you select a menu item preceded by "►" and press <**Enter> key**, the submenu of the menu item appears.



```
Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

► CPU Configuration                          CPU Configuration Parameters
► Network Stack Configuration
► CSM Configuration
► Security Configuration

                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

       Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

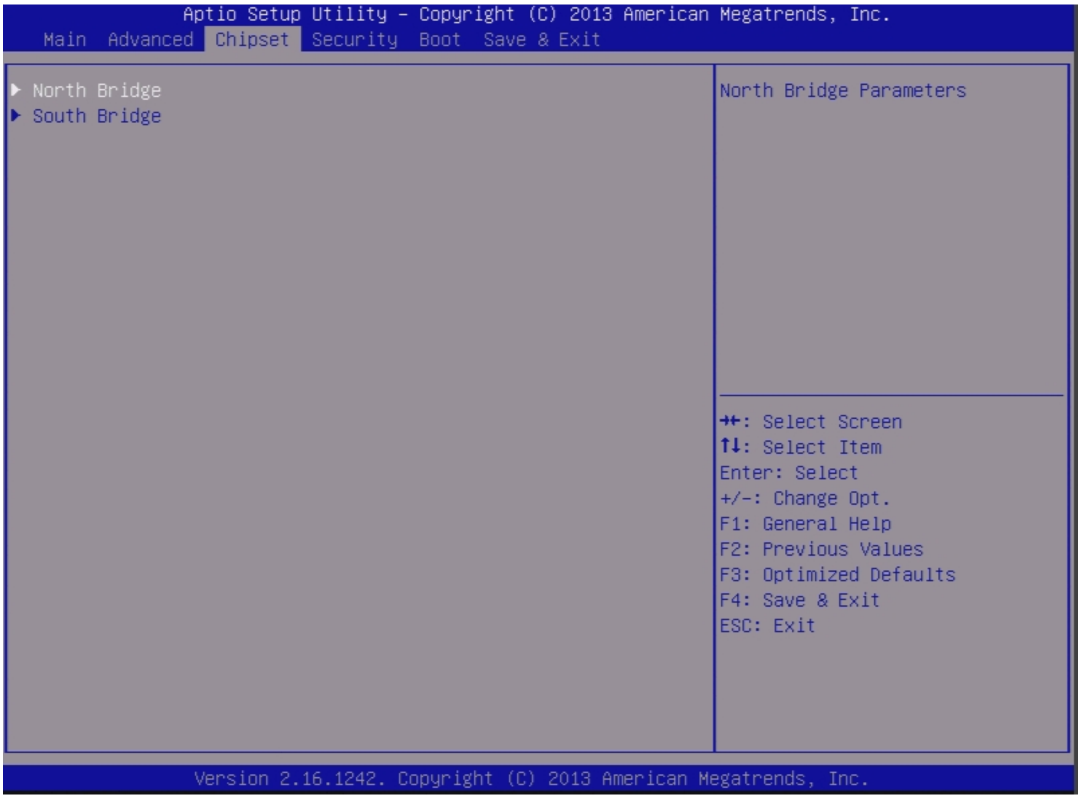
The items that can be set on the **Advanced** menu screen and their functions are described below.

Item	Parameter	Description
CPU Configuration / Power Technology	Disable [Energy Efficient]	Do not change this setting.
Network Stack Configuration / Network Stack	[Disable] Enable	Do not change this setting.
CSM Configuration / Boot option filter	[UEFI and Legacy] Legacy only UEFI only	Do not change this setting.
/ Network	Do not launch UEFI only [Legacy only] Legacy first UEFI first	Do not change this setting.
/ Video	Do not launch UEFI only [Legacy only] Legacy first UEFI first	Do not change this setting.
/ Other PCI Device	[UEFI first] Legacy only	Do not change this setting.
Security Configuration / TXE	[Enable] Disable	Do not change this setting.
/ TXE HMRFPO	Enable [Disable]	Do not change this setting.

[ ]: Factory setting

4.4.3 Chipset menu

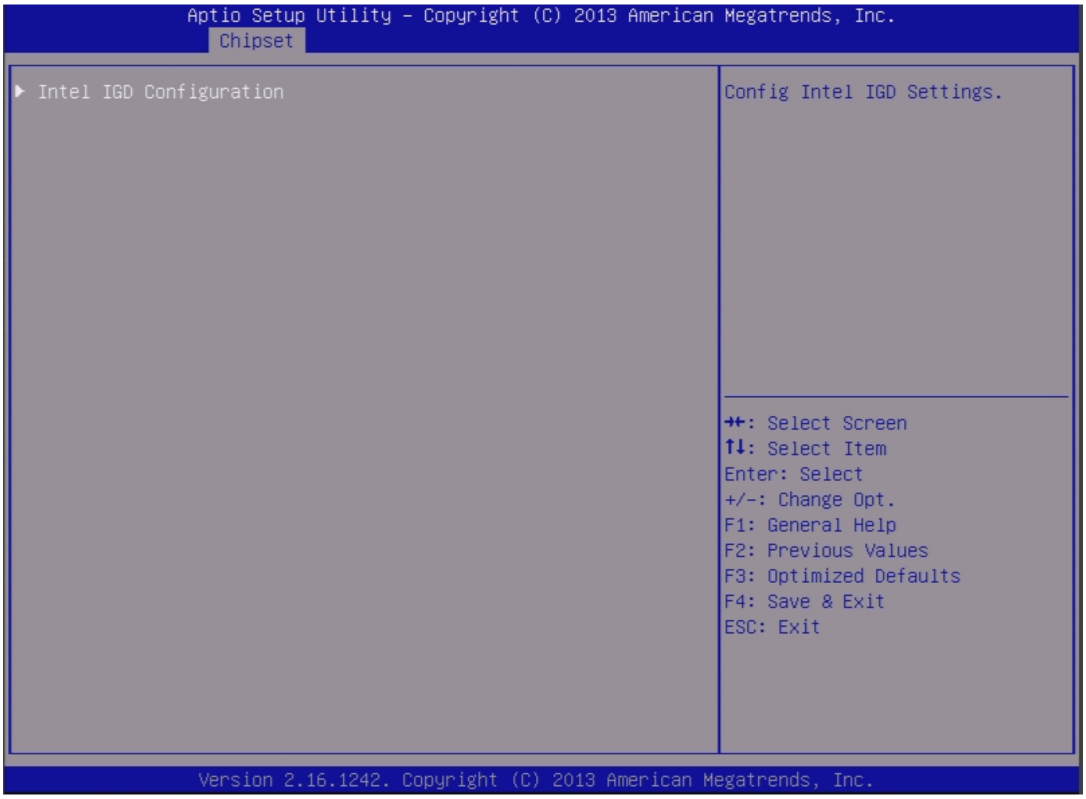
If you move the cursor to **Chipset**, the **Chipset** menu appears.



```
Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
  Main  Advanced  Chipset  Security  Boot  Save & Exit

▶ North Bridge                                   North Bridge Parameters
▶ South Bridge

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

4.4.4 Intel IGD Configuration

If you select **North Bridge** on the **Chipset** menu, you can check the Intel IGD Configuration setting.



```
Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
Chipset

▶ Intel IGD Configuration                Config Intel IGD Settings.

                                         →←: Select Screen
                                         ↑↓: Select Item
                                         Enter: Select
                                         +/-: Change Opt.
                                         F1: General Help
                                         F2: Previous Values
                                         F3: Optimized Defaults
                                         F4: Save & Exit
                                         ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

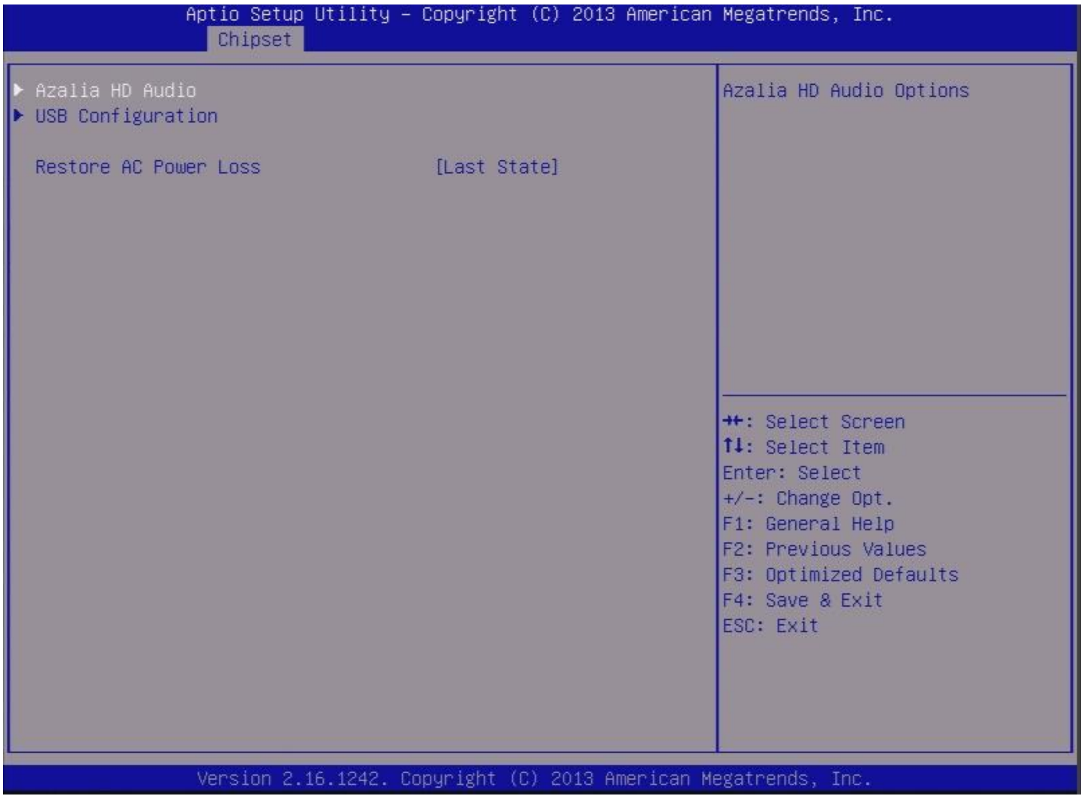
See the table below for each item.

Item	Parameter	Description
Intel IGD Configuration / DVMT Total Gfx Mem	[128MB] 256MB Max	Do not change this setting.
/ Aperture Size	[128MB] 256MB 512MB	Do not change this setting.

[ ]: Factory setting

4.4.5 South Bridge

If you select **South Bridge** on the **Chipset** menu, you can check the **South Bridge** menu.



```
Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
Chipset

▶ Azalia HD Audio                                   Azalia HD Audio Options
▶ USB Configuration

  Restore AC Power Loss          [Last State]

                                                    →←: Select Screen
                                                    ↑↓: Select Item
                                                    Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
                                                    F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

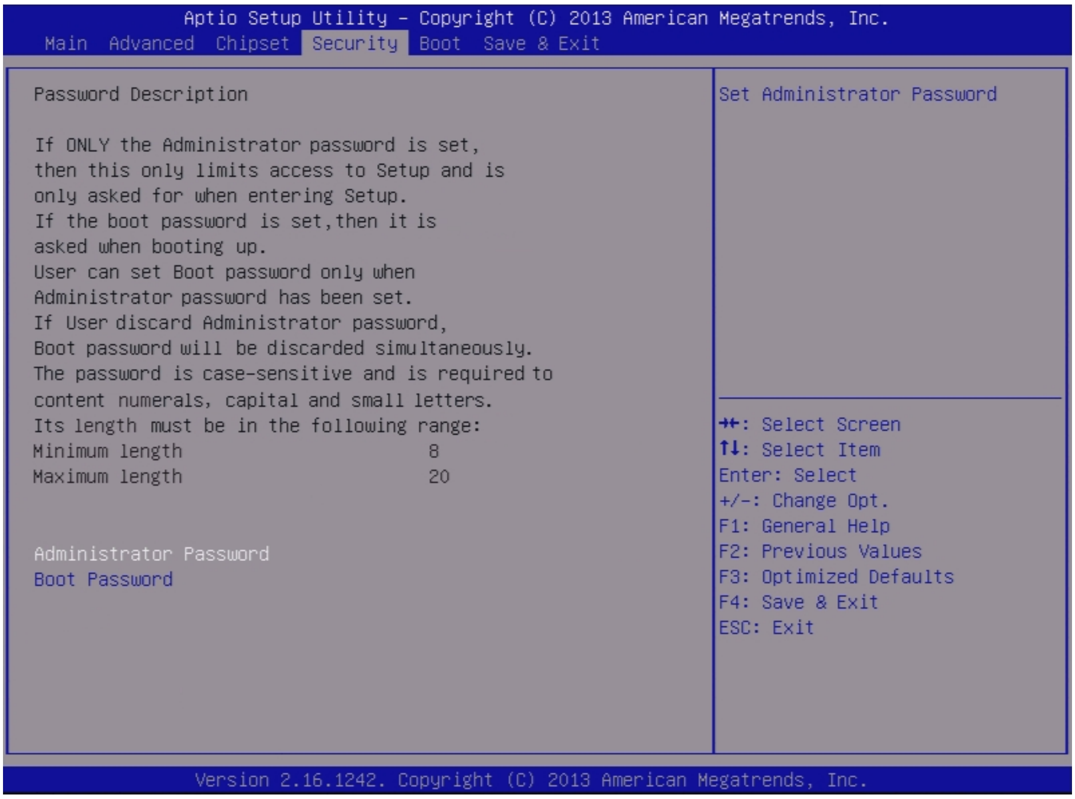
See the table below for each item.

Item	Parameter	Description
Azalia HD Audio / Audio Controller	Disable [Enable]	Specify whether to enable or disable Audio feature.
USB Configuration / USB Mode	XHCI [EHCI]	Do not change this setting.
/ USB2 Link Power Management	[Enable] Disable	Displayed when **XHCI** is selected for **USB Configuration** or **USB Mode**. Do not change this setting.
Restore AC Power Loss	Power Off Power On [Last State]	Specify the option for recovery from a power failure.

[ ]: Factory setting

4.4.6 Security menu

If you move the cursor to **Security**, the **Security** menu appears.



```
           Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

  Password Description                                     Set Administrator Password

  If ONLY the Administrator password is set,
  then this only limits access to Setup and is
  only asked for when entering Setup.
  If the boot password is set,then it is
  asked when booting up.
  User can set Boot password only when
  Administrator password has been set.
  If User discard Administrator password,
  Boot password will be discarded simultaneously.
  The password is case-sensitive and is required to
  content numerals, capital and small letters.
  Its length must be in the following range:              →←: Select Screen
  Minimum length                        8                 ↑↓: Select Item
  Maximum length                        20                Enter: Select
                                                          +/-: Change Opt.
                                                          F1: General Help
  Administrator Password                                  F2: Previous Values
  Boot Password                                           F3: Optimized Defaults
                                                          F4: Save & Exit
                                                          ESC: Exit

             Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The items that can be set on the **Security** menu screen and their functions are described below.

Item	Parameter	Description
Administrator Password	–	Set the Administrator password.
Boot Password	–	Set the password to start Windows.

Important

Control the Administrator password strictly.

Regardless of the warranty period, extra charge is required to recover the Administrator password.

4.4.7 Boot

If you move the cursor to **Boot**, the **Boot** menu appears.

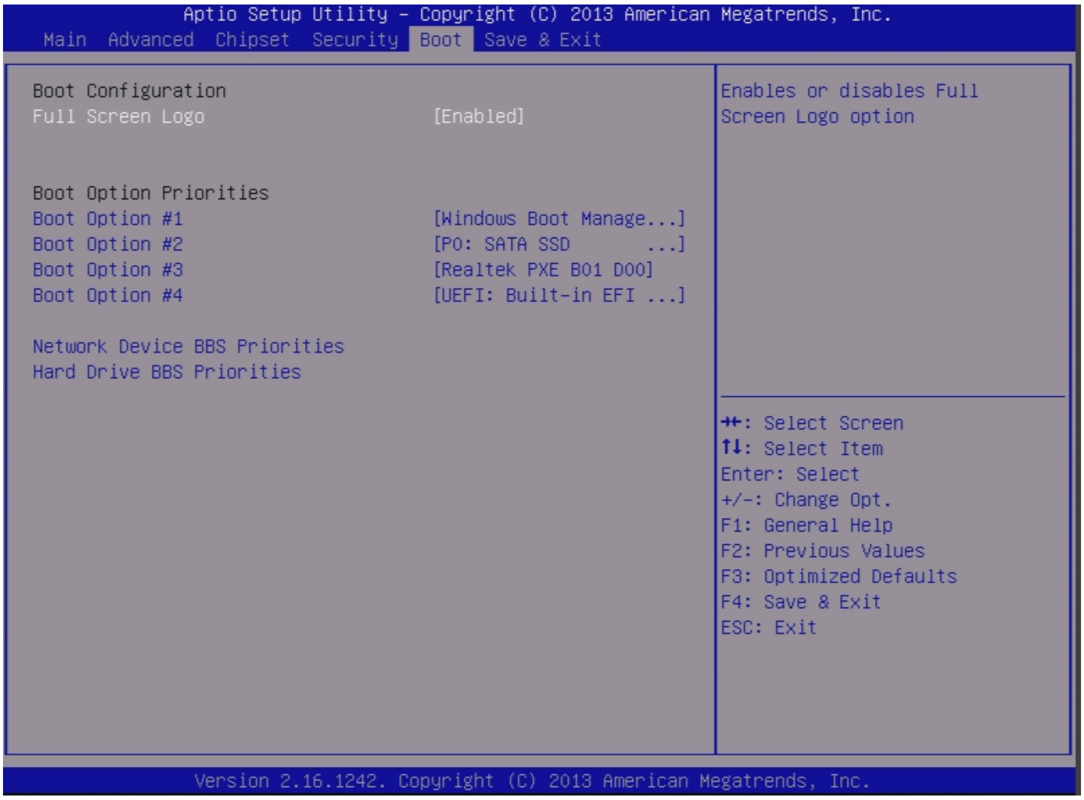
This menu contains a list showing the sequence in which devices are booted. The operating system is booted from the first device on this list. If booting fails for some reason, such as because that device does not contain the operating system, the OS will be booted from the next device on the list.

To change the device from which the OS is booted, move the cursor to the corresponding device by using the up and down arrow keys (↑ and ↓) and press the plus key (+) to move the device to the top of the list, or the minus key (–) to move the device to the bottom of the list.

The factory-set boot sequence is shown below.

1. Windows Boot Manager
2. Storage device
3. Network device
4. UEFI device

The actual screen is as follows:



```
            Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

  Boot Configuration                                  Enables or disables Full
  Full Screen Logo                [Enabled]           Screen Logo option

  Boot Option Priorities
  Boot Option #1                  [Windows Boot Manage...]
  Boot Option #2                  [P0: SATA SSD      ...]
  Boot Option #3                  [Realtek PXE B01 D00]
  Boot Option #4                  [UEFI: Built-in EFI ...]

  Network Device BBS Priorities
  Hard Drive BBS Priorities
                                                      →←: Select Screen
                                                      ↑↓: Select Item
                                                      Enter: Select
                                                      +/-: Change Opt.
                                                      F1: General Help
                                                      F2: Previous Values
                                                      F3: Optimized Defaults
                                                      F4: Save & Exit
                                                      ESC: Exit

            Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The items that can be set on the **Boot** menu screen and their functions are described below.

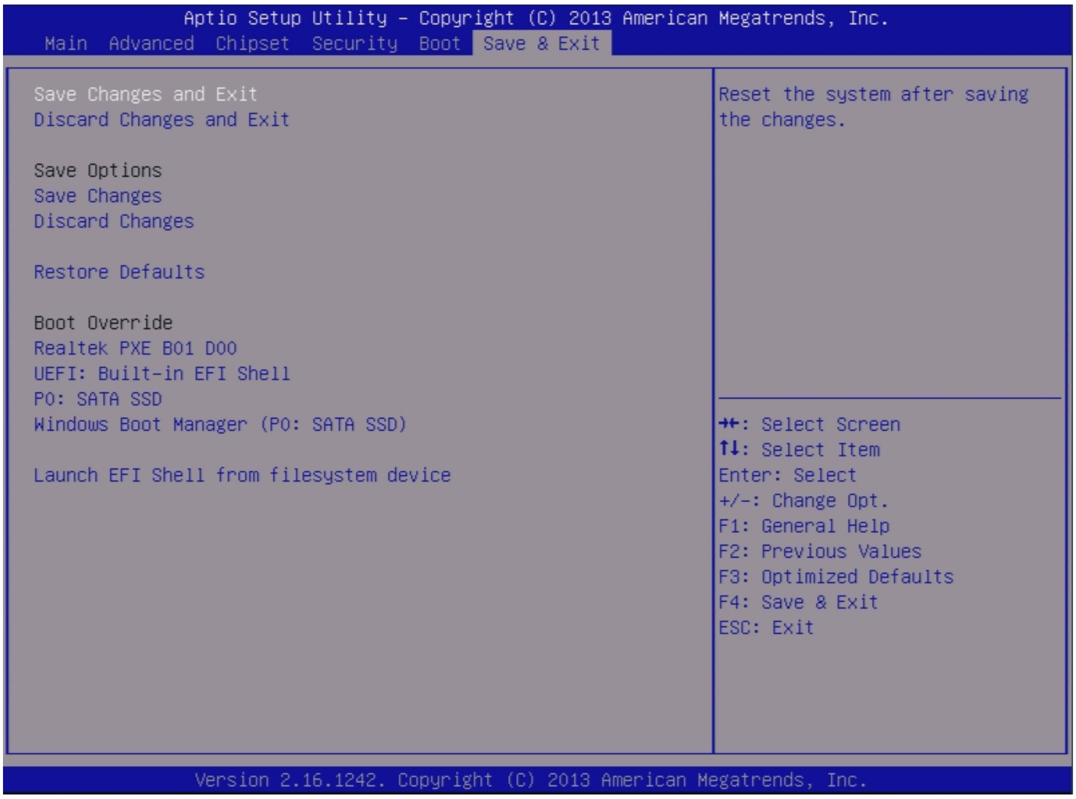
Item	Parameter	Description
Full Screen Logo	[Enable] Disable	Do not change this setting.
Network Device BBS Priorities / Boot Option #1 / Other devices	[Realtek …] Other devices	Do not change this setting.
Hard Drive BBS Priorities / Boot Option #1 / Other devices	[P0: SATA …] Other devices	Do not change this setting.

[ ]: Factory setting

Realtek PXE Boot is not supported.

4.4.8 Save & Exit

If you move the cursor to **Save & Exit**, the **Save & Exit** menu appears.



```
        Aptio Setup Utility – Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

  Save Changes and Exit                                Reset the system after saving
  Discard Changes and Exit                             the changes.

  Save Options
  Save Changes
  Discard Changes

  Restore Defaults

  Boot Override
  Realtek PXE B01 D00
  UEFI: Built-in EFI Shell
  P0: SATA SSD
  Windows Boot Manager (P0: SATA SSD)                  →←: Select Screen
                                                       ↑↓: Select Item
  Launch EFI Shell from filesystem device              Enter: Select
                                                       +/-: Change Opt.
                                                       F1: General Help
                                                       F2: Previous Values
                                                       F3: Optimized Defaults
                                                       F4: Save & Exit
                                                       ESC: Exit

          Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

The items that can be set on the **Save & Exit** menu screen and their functions are described below.

Item	Description
Save Changes and Exit	Saves the changes and closes the BIOS setup menu. (The same thing happens when you press the <**F4**> key.)
Discard Changes and Exit	Closes the BIOS setup menu without saving the changes. (The current values are discarded.)
Save Changes	Saves the changes. (The BIOS setup menu does not close.)
Discard Changes	Returns the items to their values before change. (The BIOS setup menu does not close.) (The same thing happens when you press the <**F2**> key.)
Restore Defaults	Returns all items to their default values. Note that the default values might not be the factory-set values. (The same thing happens when you press the <**F3**> key.)
Boot Override	Do not select this item.

NEC Express5800 Series
US320f

2

Chapter 2 Before Getting Started

Read this section before starting work on US320f.

1. **UWF (Unified Write Filter)**
   Describes UWF (Unified Writer Filter).

2. **Default User Accounts**
   Describes the default user accounts.

3. **The Behavior of System Startup**
   Describes the behavior of system startup.

4. **Standard / Customized Desktop Shortcuts**
   Describes the standard and customized desktop shortcuts.

5. **Connecting to a Printer**
   Describes how to connect US320f to a printer.

6. **Connecting to a Monitor**
   Describes how to connect US320f to a monitor.

1. UWF (Unified Write Filter)

Before getting started on client configuration through the Atrust Client Setup console or through the Windows 10 IoT operating system, 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 10 IoT system.

By default, your US320f 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. See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)" for more information.

Important

Read Chapter 5, "3. Using the Unified Write Filter (UWF)" first before making any changes to your system.

Note

- As a thin client device, your US320f is mainly for access to remote or virtual desktops on servers. With the limited and protected (UWF-enabled) hard disk drive space, it is *not* recommended to save data on your US320f. 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.

2. Default User Accounts

There are two default user accounts for your US320f: one is the standard, the other administrative.

The default credentials are shown as follows:

Type	Account name	Password
Administrator	Administrator	Administrator
Standard user	User	User

Important **Please be sure to change the user password for the administrator (Administrator) when starting operation.**

Note The passwords are case sensitive.

<<< IMPORTANT NOTICE >>>

In a device that can be controlled via the network, if the control password is kept at the initial value, risk of allowing unauthorized access by a malicious third party will occur. If the equipment is compromised by unauthorized access, there is a possibility that not only information leakage but also availability and integrity are hindered and the system is damaged or it can be exploited as a scaffold for cyber attack by botnet.

The initial password of this product is provided only for initial setting in maintenance operation. Be sure to change the password at initial setting. If damage caused by unauthorized access due to the operation with the initial password unchanged, we can not assume any responsibility.

Even if you change your password, it is difficult to prevent unauthorized access with low intensity (passwords with fewer digits) or easily thinkable passwords (such as "123456789", "abcdefg", "password", "Administrator").

Please change to strong password (8 letters or more and mixed case letters / small letters / numbers are recommended).

Each user account belongs to the groups shown below.

Type	Account name	Group to belong
Administrator	Administrator	Administrators
Standard user	User	Users

US320f allows a standard user (User account) to change the date and time. A standard user can change the date and time without being subject to UAC (User Account Control) access restrictions. However, a standard user cannot change time synchronization with the Internet.

Tips

- A standard user (User account) cannot access items that require administrative privileges due to UAC (User Account Control) restrictions. To access these items, type in the credentials of the administrator user (Administrator account) in the Administrator Privilege Elevation dialog box.
- A standard user (User account) cannot access Local Area Connection properties due to UAC (User Account Control) restrictions.

Based on a Windows 10 IoT Enterprise LTSB OS, US320f imposes the following access restrictions on the default accounts to provide a more secure environment.

Control Panel (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
BitLocker drive encryption	○	×
Flash Player (32 bit)	○	○
RemoteApp and Desktop Connections	○	○
Windows Defender	○	○
Windows To Go	○	×
Windows Firewall	○	×
Internet Option	○	○
Index Option	○	×
Intel® HD Graphics	○	○
Explorer Option	○	×
Keyboard	○	○
Ease of Access Center	○	○
Sound	○	○
System	○	×
Security and Maintenance	○	×
Taskbar and Navigation	○	×
Display	○	○
Device Manager	○	×
Devices and Printers	○	○
Troubleshooting	○	×
Network and Sharing center	○	○
Backup and Restore (Windows 7)	○	×
File History	○	×
Fonts	○	○
Programs and Features	○	×
Home Group	○	×
Mouse	○	○
User Account	○	×
Work Folder	×	×
Speech Recognition	○	○
Restore	○	×
Administrative Tools	○	×
Default Programs	○	×
Storage Spaces	○	×
Language	○	○
Personalization	○	○

Control Panel (○: Not restricted, ×: Restricted)		
Credential Manager	○	×
Autorun	○	×
Color Management	○	○
Infrared	○	×
Region	○	○
Power Options	○	○
Phone and Modem	○	○
Sync Center	○	×
Date and Time	○	○

Start Menu (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Citrix Receiver	○	○
VMware Horizon Client	○	○
Internet Explorer	○	○
Windows Media Player	○	○
Calculator	○	○
Remote Desktop Connection	○	○
Windows Ease of Access	○	○
Windows Defender	○	○
Default Programs	○	○
Control Panel	○	○
Devices	○	○
Intel ® HD Graphics Control Panel	○	○
Character Map	○	×
Task Manager	○	×
Windows Administrative Tool	○	×
Snipping Tool	○	×
Windows FAX and Scan	○	×
XPS Viewer	○	×
Steps Recorder	○	×
Paint	○	×
WordPad	○	×
Math Input Panel	○	×
Atrust Client Setup	○	×
Windows PowerShell	○	×
Notepad	○	×

Start Menu (○: Not restricted, ×: Restricted)		
This PC	○	×
File Explorer	○	×
Command Prompt	○	×
Run	○	×
Search (* disable search by clicking)	○	×
Settings	○	○
Show More Tiles	○	×
Show Most Used Apps	○	×

Windows Defender (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Change of Real Time Protection Settings	○	×
Change of Cloud Based Protection Settings	○	×
Change of Automatic Sample Submission Settings	○	×
Adding Exclusions	○	×
Change of Enhanced Notifications Settings	○	×
Windows Defender Offline Scan	×	×

Task Manager (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Use of Task Manager	○	×

Security Option (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Lock Computer	○	×
Change Password	○	×
Block Microsoft Account	×	×

Taskbar (○: Not restricted, ×: Restricted)

Item	Administrator	User
Lock Taskbar	○	×
Access to Shortcut Menu on Taskbar	○	×
Search Box on Taskbar	○	×

Quick Access (○: Not restricted, ×: Restricted)

Item	Administrator	User
Frequent folders	○	×
Recent Files	○	×

Recycle Bin (○: Not restricted, ×: Restricted)

Item	Administrator	User
Recycle Bin icon on desktop	○	×
Move deleted files to Recycle Bin	○	×

Explorer (○: Not restricted, ×: Restricted)

Item	Administrator	User
Display C Drive	○	×
File Menu on Explorer	○	×
Folder Options (Options button on View tab on ribbon)	○	×
Manage item on the file Explorer context menu	○	×
Map Network Drive and Disconnect Network Drive	○	×
Windows+X hotkey	○	×
File Explorer's default contex menu	○	×
Access to C Drive from My Computer	○	×
Autoplay on Removable media drives	×	×

Internet Explore (○: Not restricted, ×: Restricted)

Item	Administrator	User
FTP Folder View	○	×
Programs Tab	○	×
Install new versions automatically	×	×
Browsing history	×	×

Start Button Right Click Menu (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Programs and Features	○	×
Power Options	○	×
Event Viewer	○	×
System	○	×
Device Manager	○	×
Network Connection	○	×
Disk Management	○	×
Computer Management	○	×
Command Prompt	○	×
Command Prompt (Admin)	○	×
Task Manager	○	×
Control Panel	○	○
File Explorer	○	×
Search	○	×
Run	○	×
Shutdown or Sign out	○	○
Desktop	○	○

Developer Features (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Access to Developer Features	○	×

Connection to Office or School (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Domain Participation	○	×

Adobe Flash Player Settings Manager(○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
Access to Update Settings	○	×

Virtual Desktop Session (○: Not restricted, ×: Restricted)		
Item	**Administrator**	**User**
C Drive Mapping of Microsoft RDP	○	×
C Drive Mapping of Citrix ICA Session	○	×

Virtual Desktop Session (○: Not restricted, ×: Restricted)

C Drive Mapping of VMware Horizon Session	○	×

File Sharing (○: Not restricted, ×: Restricted)

Item	Administrator	User
SMB 1.0/CIFS File Sharing Support	×	×

Program Access (○: Not restricted, ×: Restricted)

Item	Administrator	User
Command Prompt	○	×
Registory Editor	○	×
Windows PowerShell	○	×
Windows PowerShell ISE	○	×
Disk Cleanup Utility	○	×
CScript	○	×
MMC Snap-in	○	×
Paint	○	×
Netsh	○	×
Netstat	○	×
Notepad	○	×
Wordpad	○	×

Notification Area and Action Center (○: Not restricted, ×: Restricted)

Item	Administrator	User
Notification Area and Action Center	○	×

Windows Update (○: Not restricted, ×: Restricted)

Item	Administrator	User
Windows Update	×	×
Installing Drivers by Windows Update	×	×
Automatic Driver Update	×	×

3. The Behavior of System Startup

Every time US320f is started up, you will automatically log in to the Windows Embedded operating system using the default standard user account.

3.1 Switching the Sign-In User

Sign in to the system using other than default user account as follows:

1. Sign in automatically by default user account.
2. Sign out from the start menu.
3. Click a mouse or input at a keyboard to release the lock screen.
4. Enter the user name and password to sign in and click the → **(OK)** button.

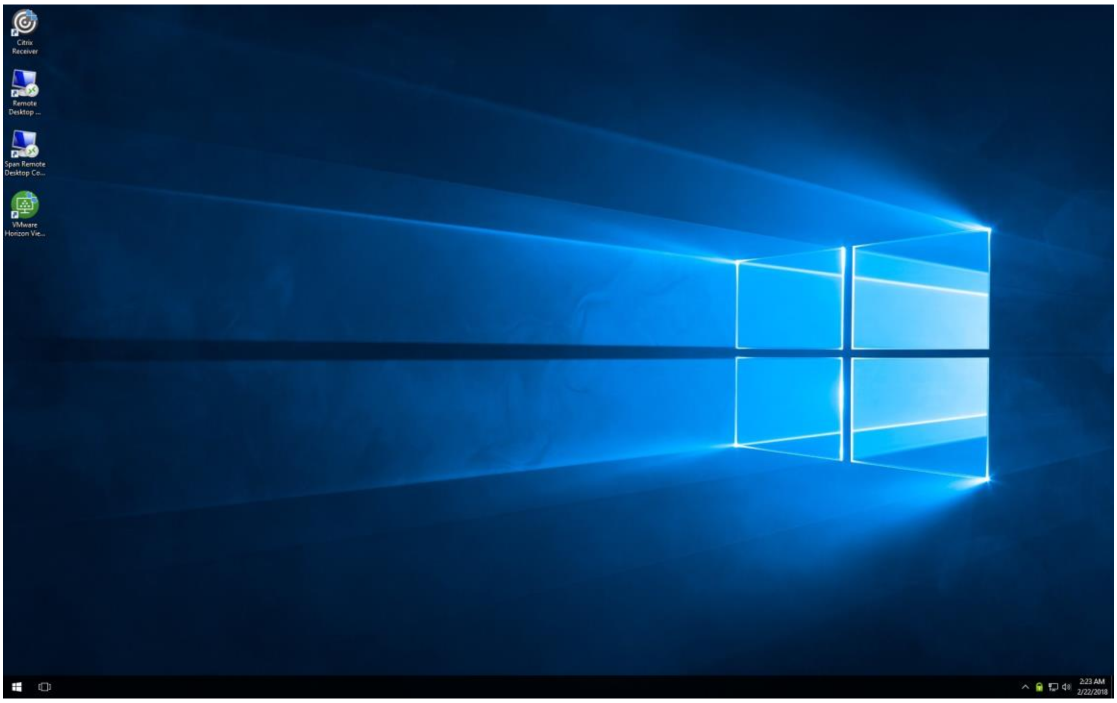
4. Standard / Customized Desktop Shortcuts

With US320f, 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 by default; the latter can be created and customized through the Atrust Client Setup console.

- Standard Desktop Shortcuts

  You can find out how to use standard desktop shortcuts to access desktop virtualization solutions in chapter 3, "Using US320f".



- Customized Desktop Shortcuts

  You can find out how to create and customize access shortcuts in chapter 4, "Configuring Client Settings with Atrust Client Setup".

5. Connecting to a Printer

When using a local or virtual desktop, to use the printer by using the device mapping feature, you need to install the proper printer driver on US320f.

Note

- When using a virtual desktop, if you use a printer by using the USB Redirect feature (such as Citrix HDX USB redirection), you do not need to install a printer driver on US320f.
- If you want to connect a parallel printer to US320f, you need to prepare a USB-parallel printer cable (not supplied with US320f).

6. Connecting to a Monitor

US320f can be connected to a monitor by using the DVI-I port, DVI-D port, or DVI-VGA adapter.

For information about configuring dual display settings, see Chapter 5, "11 Configuring Dual Monitor Display".

6.1 Supported Monitor Configurations

Monitor Configuration	DVI-I port	DVI-D port
Single	DVI-D	–
	VGA (*1)	–
	–	DVI-D
Dual	DVI-D	DVI-D
	VGA (*1)	DVI-D

*1. VGA output port to connect the DVI-VGA adapter that comes with US320f

Important **NEC only supports genuine optional monitors. When using another monitor in the actual operating environment, thoroughly evaluate the operation with the specified settings based on the actual operating environment and confirm that there is no problem.**

NEC Express5800 Series
US320f

3

Chapter 3 Using US320f

This chapter provides the basics of how to use your US320f.

1. **Standard Shortcuts**

   Describes default shortcuts on the desktop

2. **Accessing Citrix Services**

   Describes how to access Citrix services

3. **Accessing Microsoft Remote Desktop Services**

   Describes how to access Microsoft Remote Desktop services

4. **Accessing VMware View and Horizon Services**

   Describes how to access VMware View and Horizon services

5. **Accessing NEC Client Management Option (CMO) Services**

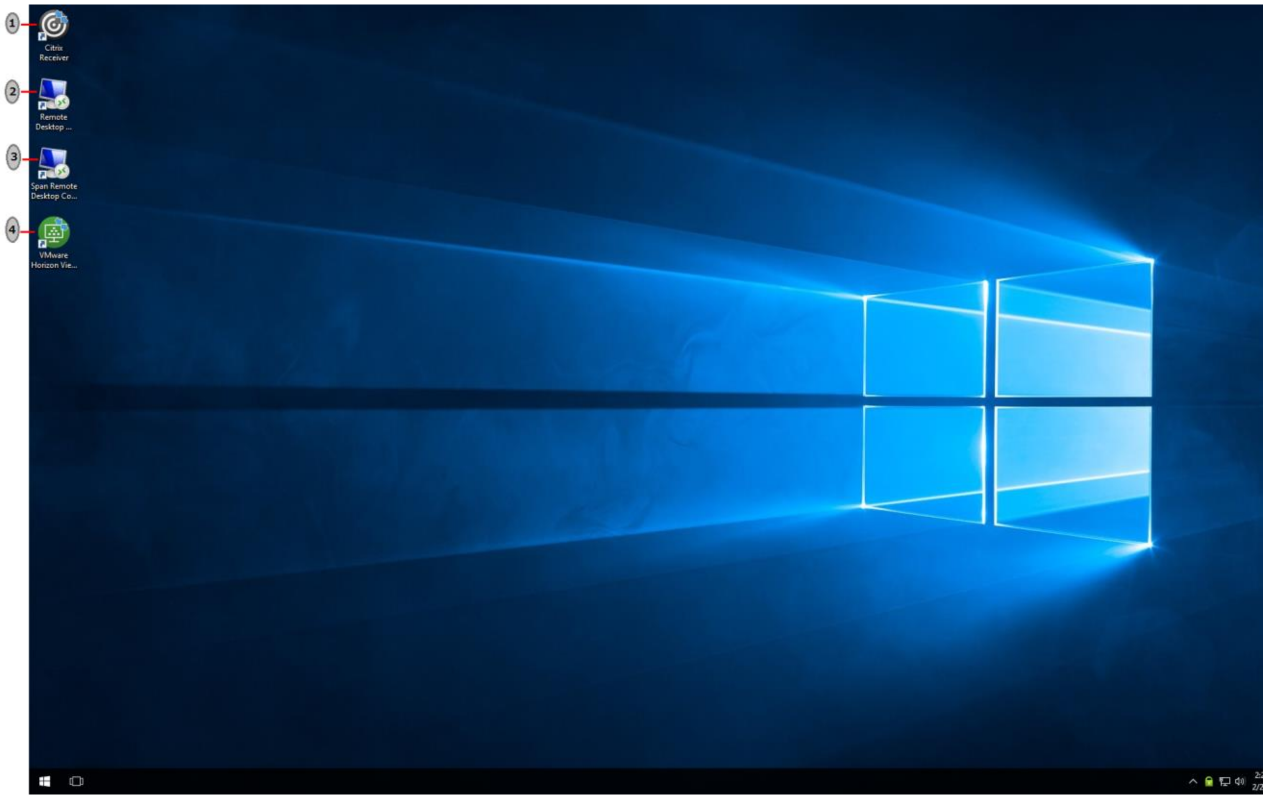
   Describes how to access NEC Client Management Option (CMO) services.

6. **Browsing the Internet by Using Internet Explorer**

   Describes how to browse the Internet by using the browser.

1. Standard Shortcuts

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



No.	Shortcuts	Description
1	Citrix Receiver	Double click to access Citrix services.
2	Remote Desktop Connection	Double click to access Microsoft Remote Desktop services.
3	Remote Desktop Connection (Span mode)	Double click to access Microsoft Remote Desktop services in the span mode.
4	VMware Horizon Client	Double click to access VMware View and VMware Horizon services.

Note

If the secure network connection (HTTPS) is not implemented in your Citrix environment, you might not be able to access Citrix services through Citrix Receiver. Alternatively, Citrix allows service access simply through the Internet Explorer. Try to use the Internet Explorer if you have problems with Citrix Receiver.

2. Accessing Citrix Services

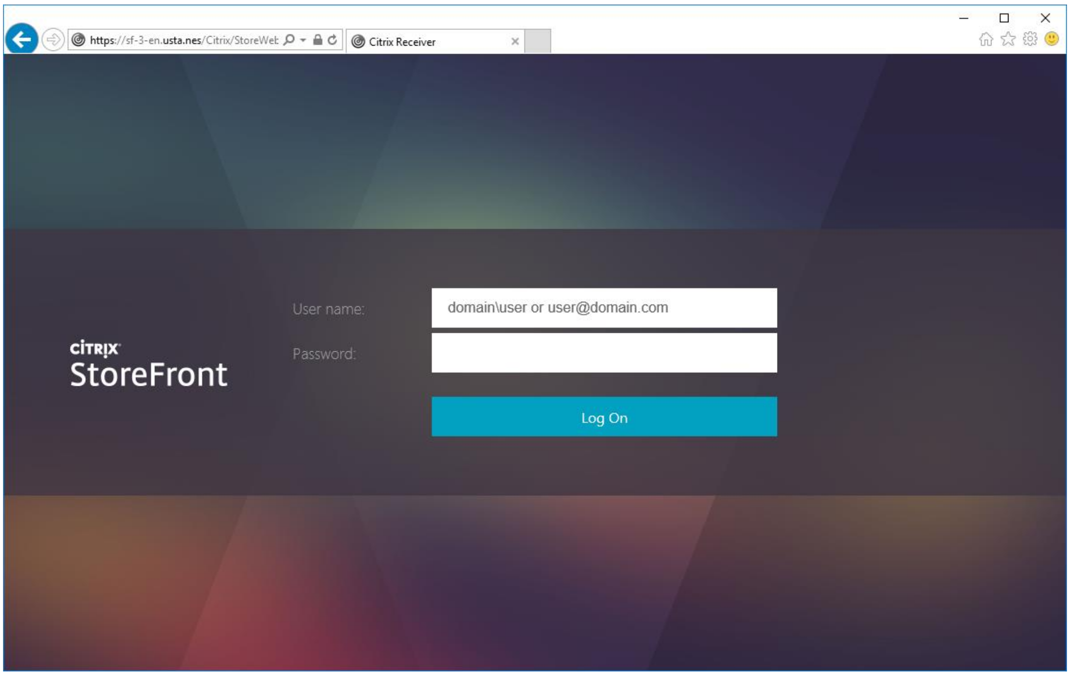
You can access Citrix services:

- From your Web browser (Internet Explorer)
- By using the Citrix Receiver shortcut

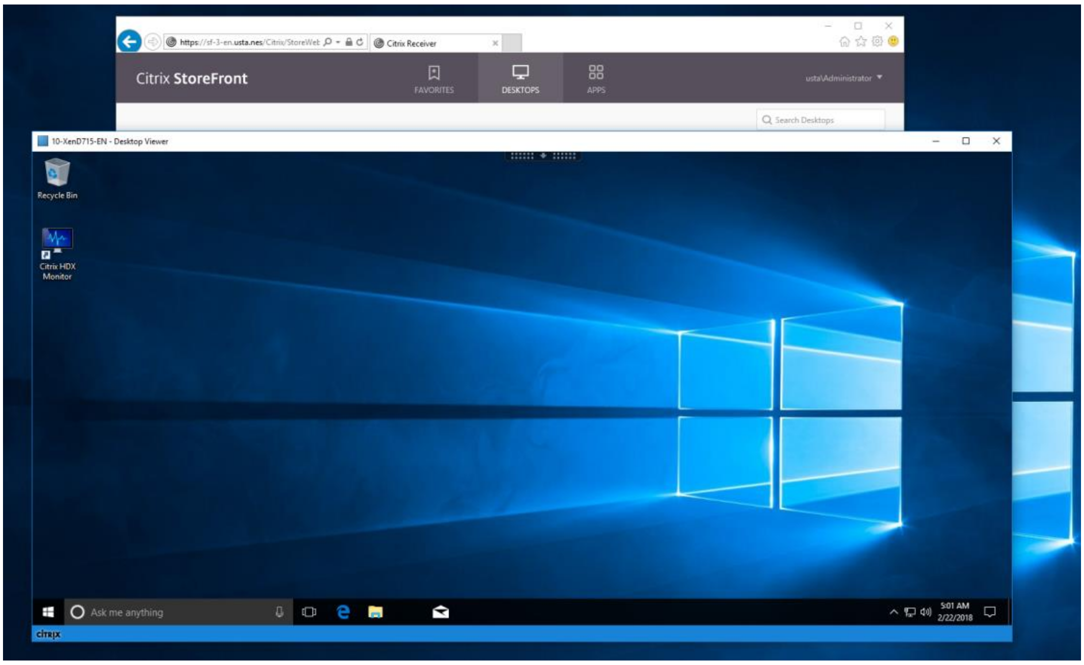
2.1 Accessing Citrix Service with Internet Explorer

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

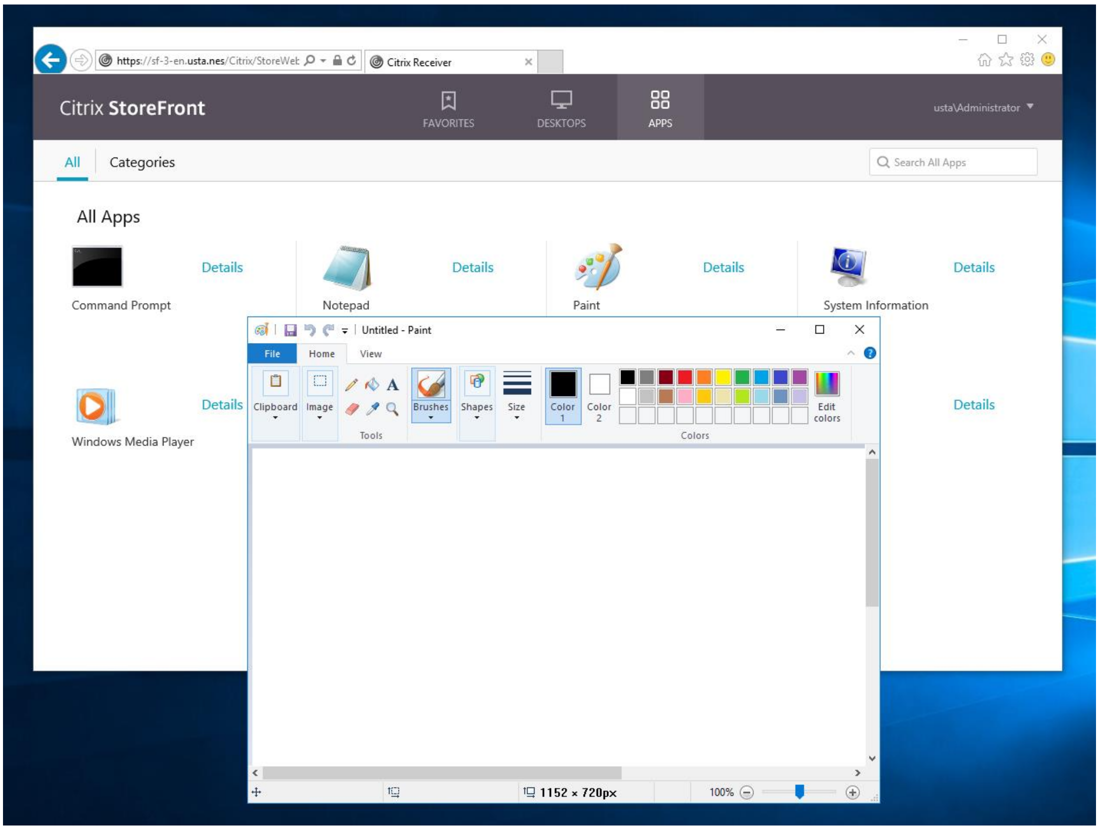
1. Open the Internet Explorer by clicking its icon on the Start menu.
2. Enter the IP address / URL / FQDN of the server through which Citrix services are accessible.
3. Follow the on-line instructions to provide the required data and access Citrix services.


https://sf-3-en.usta.nes/Citrix/StoreWeb
Citrix Receiver
CiTRIX
StoreFront
User name:
domain\user or user@domain.com
Password:
Log On

Logon Screen Example (XenDesktop 7.15 Platinum)



Virtual Desktop Example (Windows 10 Enterprise)



Virtual Application Examples

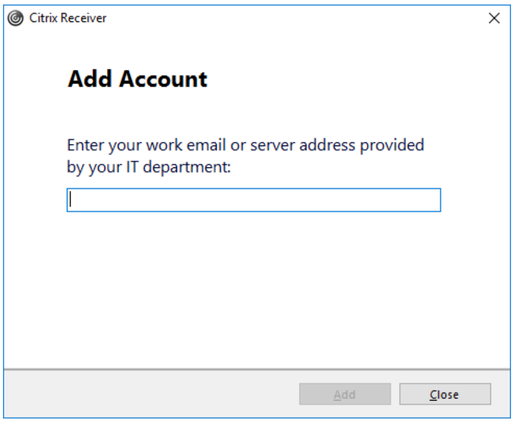
2.2 Accessing Citrix Service through the Citrix Receiver Shortcut

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

1. By default, a secure connection (HTTPS) is required to access Citrix services by using the Citrix Receiver shortcut. You therefore need to install a certificate.

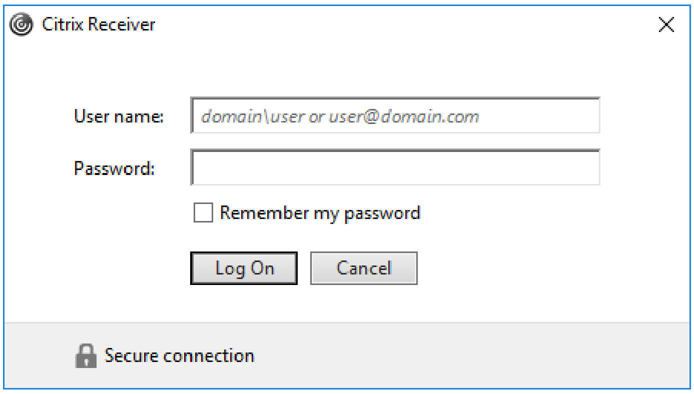
   Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

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



Enter your work email or server address provided by your IT department:

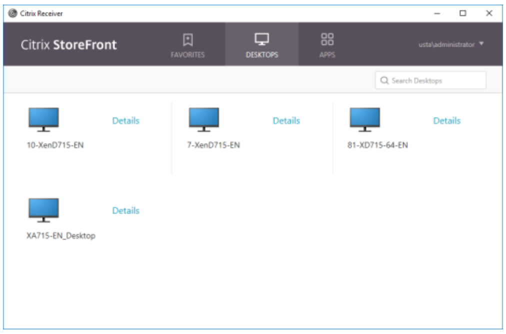
4. Log on with the credentials for your Citrix services.

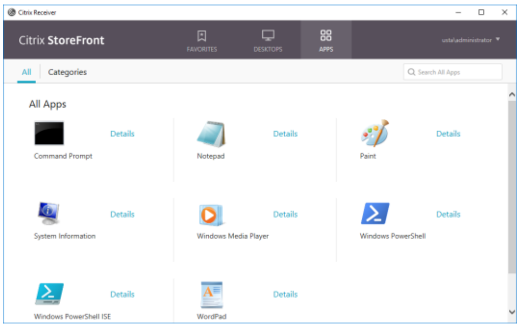


User name: domain\user or user@domain.com

□ Remember my password

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





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

3. Accessing Microsoft Remote Desktop Services

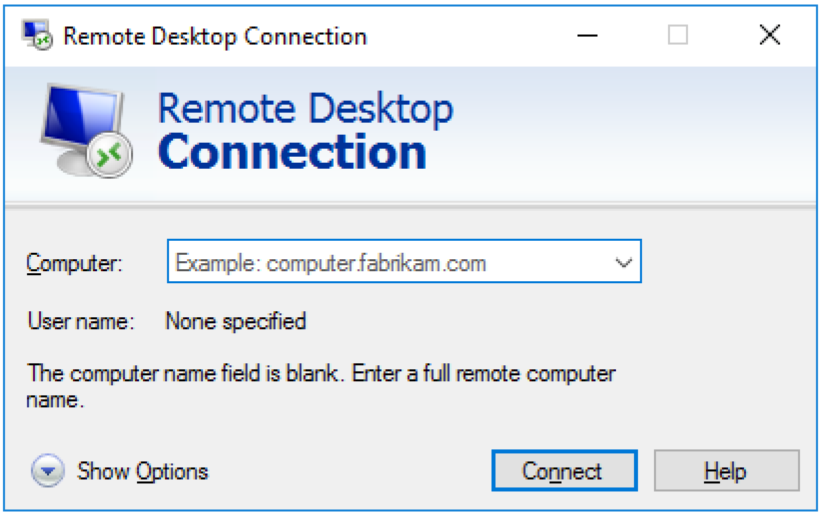
You can access Microsoft Remote Desktop Services:

- By using Remote Desktop Connection
- By accessing a Remote Desktop Service by using Remote Desktop Connection (Span mode)
- By using RemoteApp and Desktop Connection
- From your Web browser (Internet Explorer)

3.1 Accessing Microsoft Remote Desktop Services by Using Remote Desktop Connection

To access Remote Desktop services, 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 Remote Desktop Connection window, and then click **Connect**.



Remote Desktop Connection

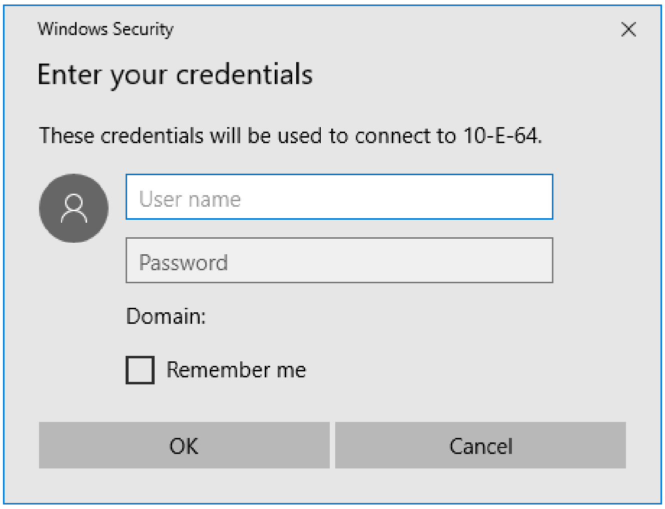
Remote Desktop Connection

Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

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



Windows Security

Enter your credentials

These credentials will be used to connect to 10-E-64.

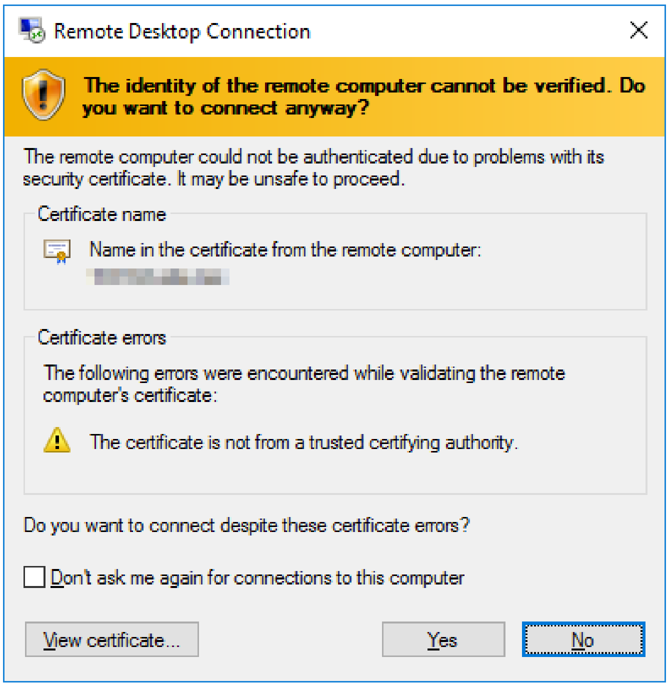
User name

Password

Domain:

□ Remember me

4. A window may appear with a certificate message about the remote computer. Consult your system administrator for details. To bypass, click **Yes** to continue.



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
[redacted]

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

⚠ The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

5. US320f is connected to the remote desktop, and the virtual desktop will be displayed on the screen.

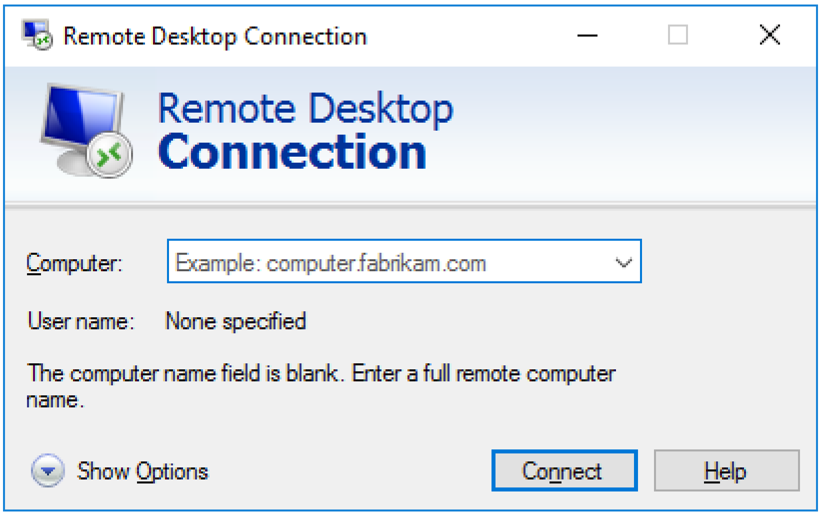
3.2 Accessing Microsoft Remote Desktop Services by Using Remote Desktop Connection (Span Mode)

To access Remote Desktop Services by using Remote Desktop Connection (span mode), do the following:

Note To establish a connection in the span mode, connect the primary and secondary monitors to US320f. In addition, open Control Panel and click **Display** -> **Change display settings** -> **Display** to properly configure your display settings. (For details, see documentation available from Microsoft at http://www. microsoft.com.)

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

Note If you select **Show Options** -> **Display** tab -> **Display configuration** and select the **Use all my monitors for the remote session** check box, you will be connected to the virtual PC in multiple monitors mode (that is, the primary and secondary monitors will be connected to the virtual PC independently).

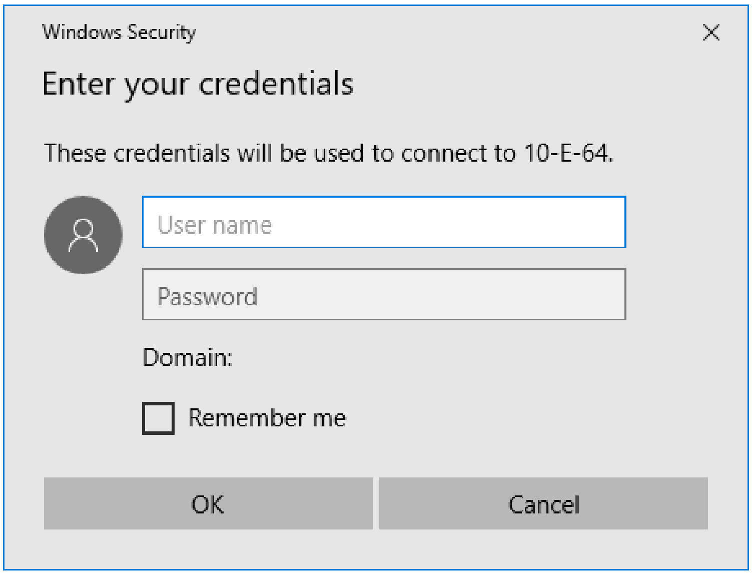


Computer: Example: computer.fabrikam.com

User name: None specified

The computer name field is blank. Enter a full remote computer name.

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



Enter your credentials

These credentials will be used to connect to 10-E-64.

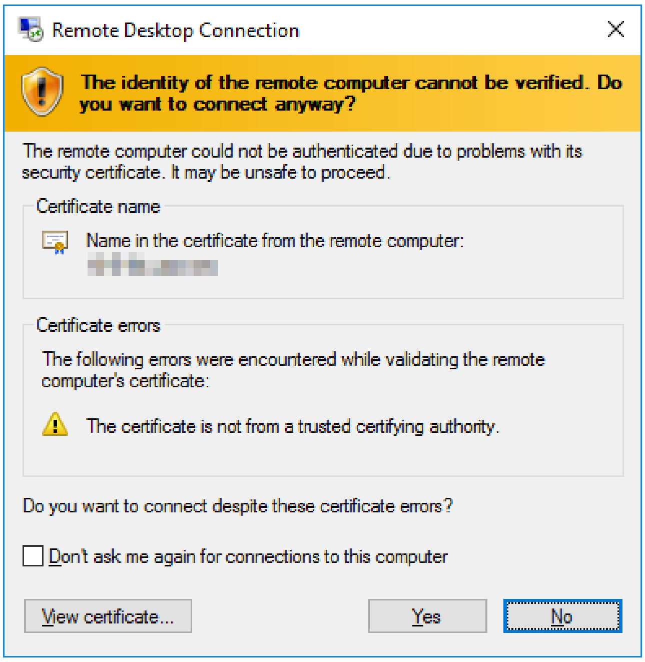
User name

Password

Domain:

□ Remember me

4. A window may appear with a message about the remote computer certificate. Consult your system administrator for details. To bypass, click **Yes**.



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
[redacted]

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

5. US320f is connected to the remote desktop, and the virtual desktop will be displayed on the screen.

6. After logging on to the virtual desktop, check that US320f is connected in the span mode.

* When US320f is connected to the remote desktop in the span mode, applications such as NotePad are displayed across two screens when maximized.

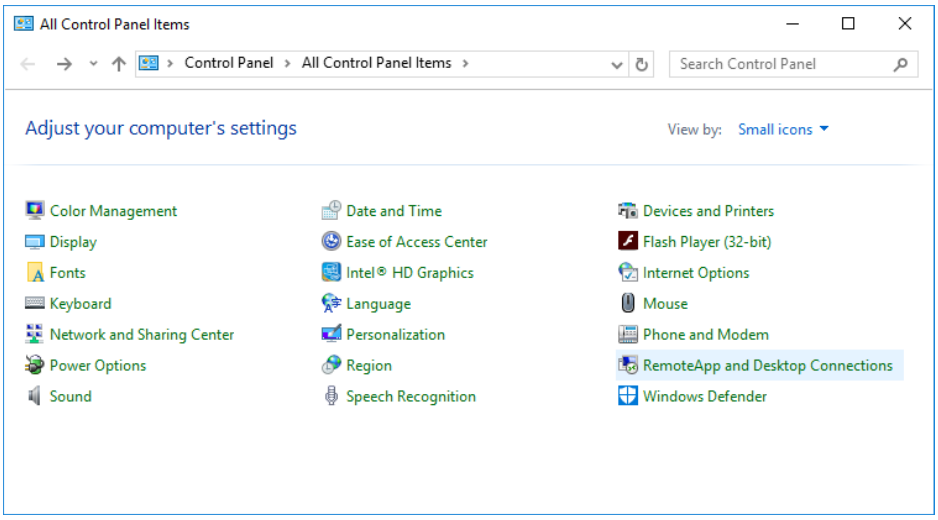
3.3 Accessing Remote Desktop Services by Using RemoteApp and Desktop Connection

Access Remote Desktop services by using RemoteApp and Desktop Connection as follows:

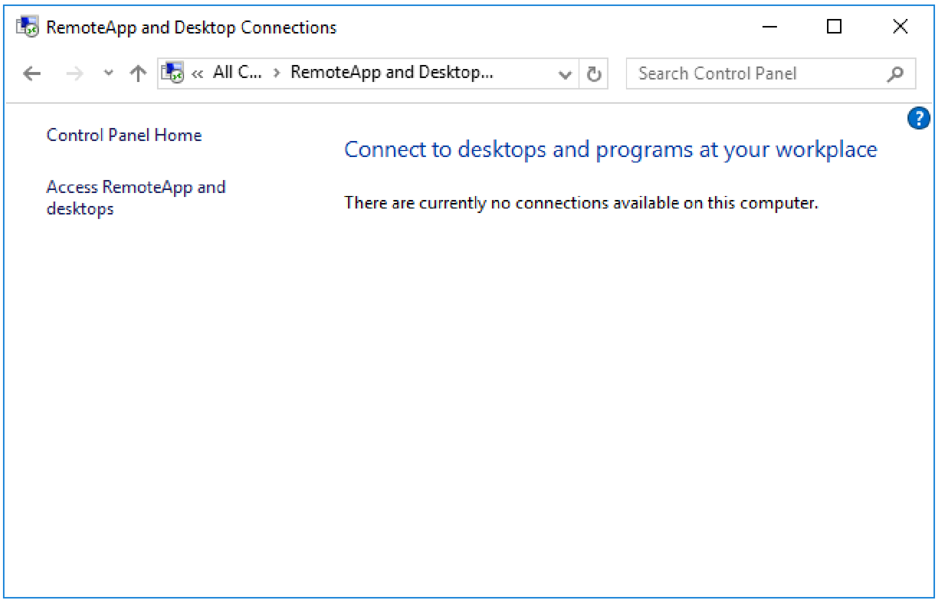
1. By default, a secure connection (HTTPS) is required to connect to Remote Desktop Services by using RemoteApp and Desktop Connection. You therefore need to install a certificate.

   Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

2. On your desktop, move the mouse pointer to the bottom-left corner, and right-click **Start** to open the popup menu.
3. Click **Control Panel**.
4. Select **RemoteApp and Desktop Connections**.



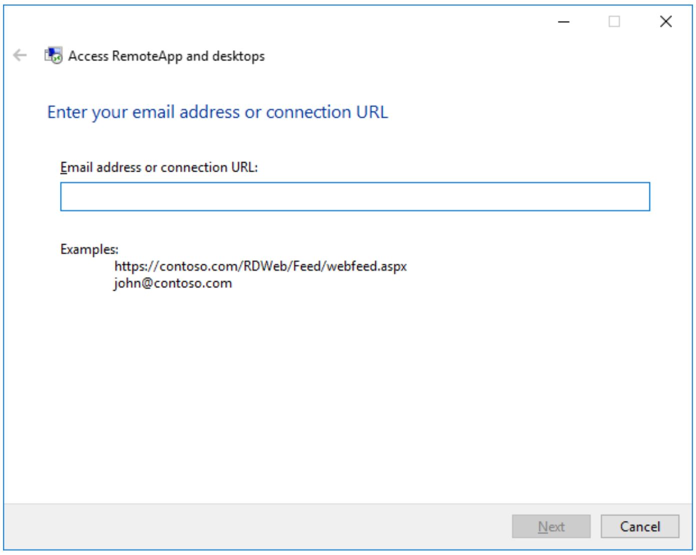
5. Click **Access RemoteApp and Desktops** on the left pane.


RemoteApp and Desktop Connections
« All C... > RemoteApp and Desktop...
Search Control Panel
Control Panel Home
Access RemoteApp and desktops

Connect to desktops and programs at your workplace

There are currently no connections available on this computer.

6. A window appears prompting your to enter your email address or connection URL. Consult your system administrator for the proper information to provide here, enter the required data, and then click **Next** to continue.



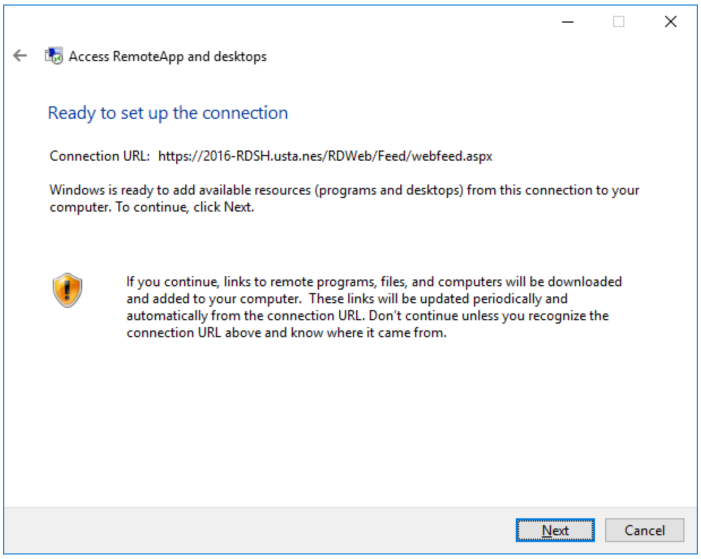
Access RemoteApp and desktops

Enter your email address or connection URL

Email address or connection URL:

Examples:
https://contoso.com/RDWeb/Feed/webfeed.aspx
john@contoso.com

7. A window indicating that you are ready to set up the connection appears. Click **Next**.



Access RemoteApp and desktops

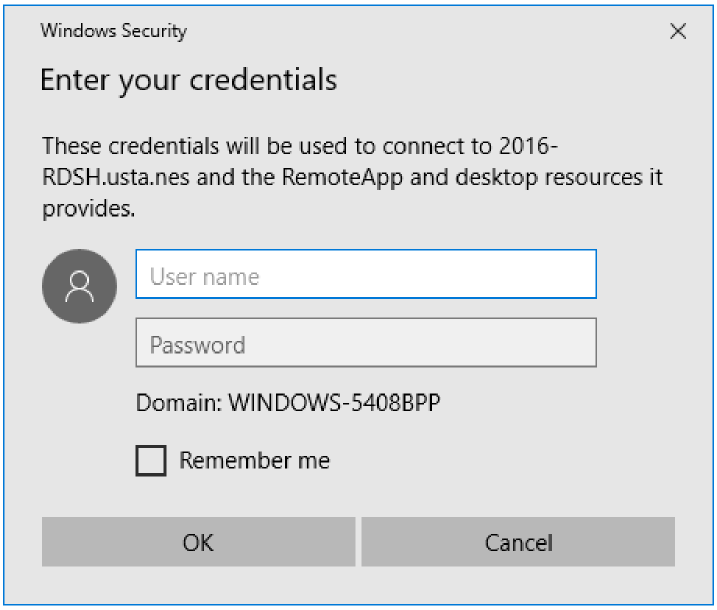
Ready to set up the connection

Connection URL: https://2016-RDSH.usta.nes/RDWeb/Feed/webfeed.aspx

Windows is ready to add available resources (programs and desktops) from this connection to your computer. To continue, click Next.

If you continue, links to remote programs, files, and computers will be downloaded and added to your computer. These links will be updated periodically and automatically from the connection URL. Don't continue unless you recognize the connection URL above and know where it came from.

8. Type in your credentials, and then click **OK**.



Windows Security

Enter your credentials

These credentials will be used to connect to 2016-RDSH.usta.nes and the RemoteApp and desktop resources it provides.

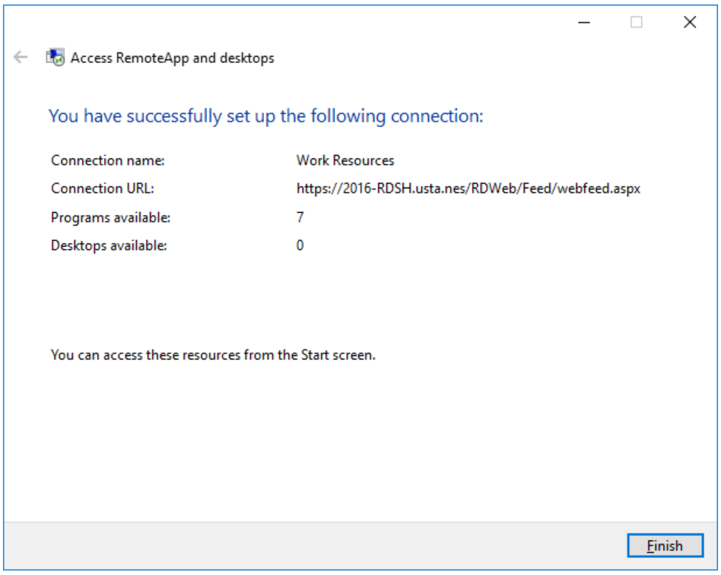
User name

Password

Domain: WINDOWS-5408BPP

□ Remember me

9. A window indicating that connection is properly set up appears. Click **Finish**.

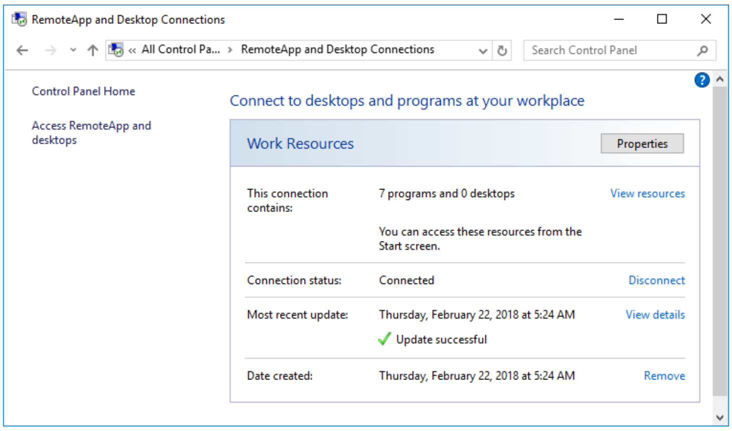


You have successfully set up the following connection:

Connection name:	Work Resources
Connection URL:	https://2016-RDSH.usta.nes/RDWeb/Feed/webfeed.aspx
Programs available:	7
Desktops available:	0

You can access these resources from the Start screen.

10. When the information you have specified in the steps above is displayed in **RemoteApp and Desktop Connections**, close the **RemoteApp and Desktop Connections** window.

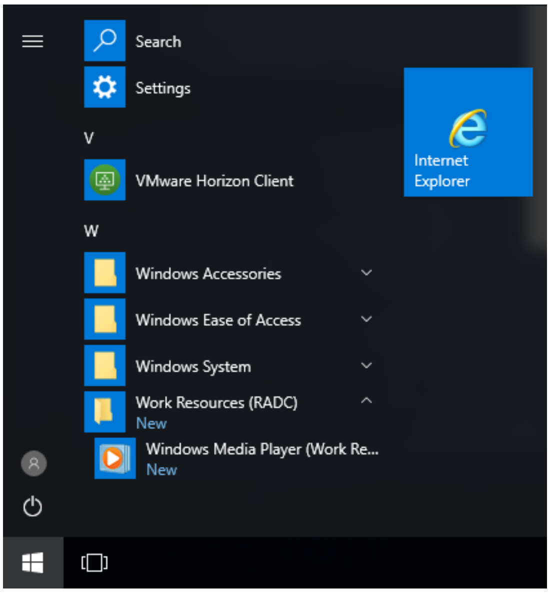

RemoteApp and Desktop Connections
« All Control Pa... › RemoteApp and Desktop Connections
Search Control Panel
Control Panel Home
Access RemoteApp and desktops
Properties
View resources
Disconnect
View details
Remove

Connect to desktops and programs at your workplace

Work Resources

This connection contains:	7 programs and 0 desktops You can access these resources from the Start screen.
Connection status:	Connected
Most recent update:	Thursday, February 22, 2018 at 5:24 AM ✓ Update successful
Date created:	Thursday, February 22, 2018 at 5:24 AM

11. Icons for published applications and desktops for remote desktop services are displayed on the **Start** menu.



12. Click an icon on the **Start** menu to connect to a desktop or application.

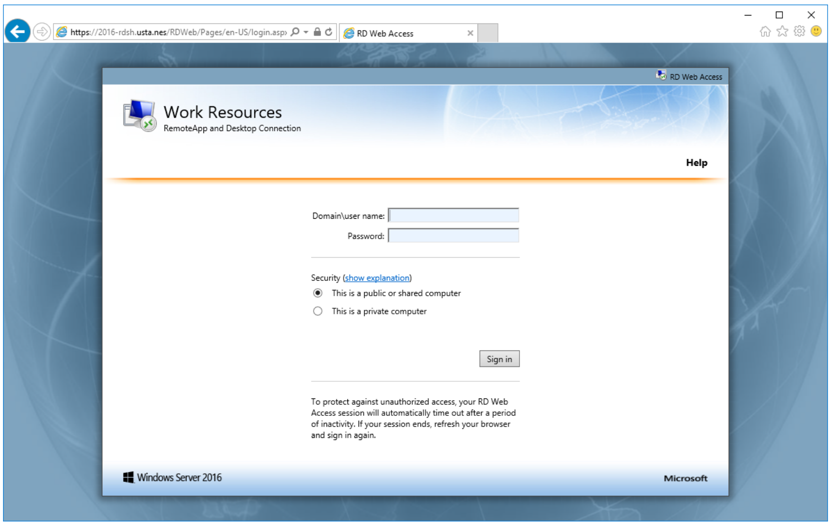
3.4 Accessing Remote Desktop Services by Using Internet Explorer

Access Remote Desktop services by using Internet Explorer as follows:

1. By default, a secure connection (HTTPS) is required to connect to Remote Desktop Services by using Internet Explorer. You therefore need to install a certificate.

Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

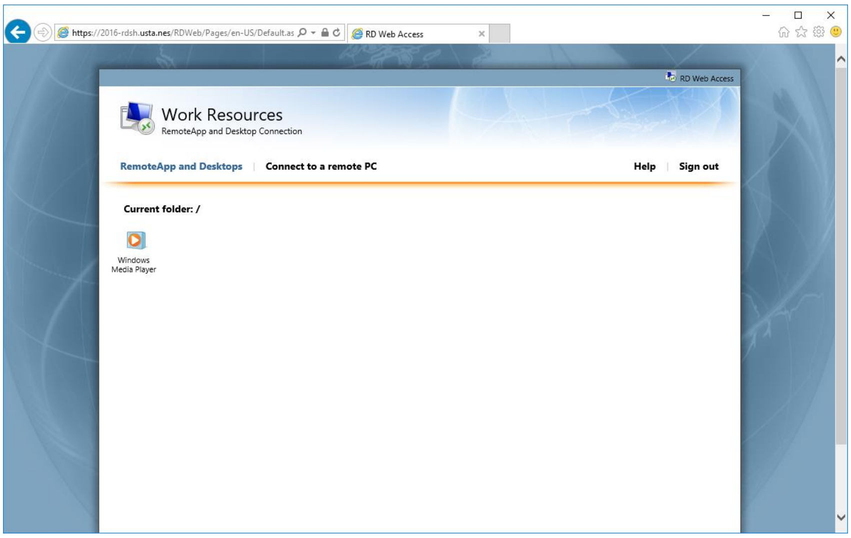
2. Click the Internet Explorer icon on the **Start** screen or taskbar on your desktop to launch Internet Explorer.
3. Enter the IP address, URL, or FQDN of the server through which Remote Desktop Services will be accessed.
4. Enter your credentials, and then click **Sign in**.


https://2016-rdsh.usta.nes/RDWeb/Pages/en-US/login.aspx
RD Web Access
RD Web Access
Work Resources
RemoteApp and Desktop Connection
Help
Domain\user name:
Password:
Security (show explanation)
● This is a public or shared computer
○ This is a private computer
Sign in
Windows Server 2016
Microsoft

To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

Note You may be prompted for permission to run the add-on for "Microsoft Remote Desktop Services Web Access Control". In this case, please select "allow" or add the website to the zone of the local intranet or trusted site.

5. Icons for connecting to desktops and applications published by Remote Desktop Services are displayed.



6. Select an icon to connect with a desktop or application.

4. Accessing VMware View and Horizon Services

You can access VMware View and Horizon Services:

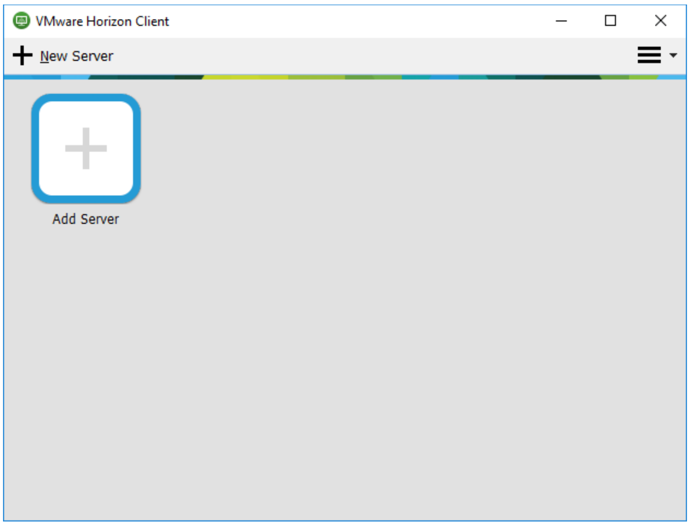
- By using VMware Horizon Client
- From your Web browser (Internet Explorer)

Note To access VMware View and Horizon Services from your Web browser, VMware Horizon HTML Access must be configured in VMware View and Horizon Services.

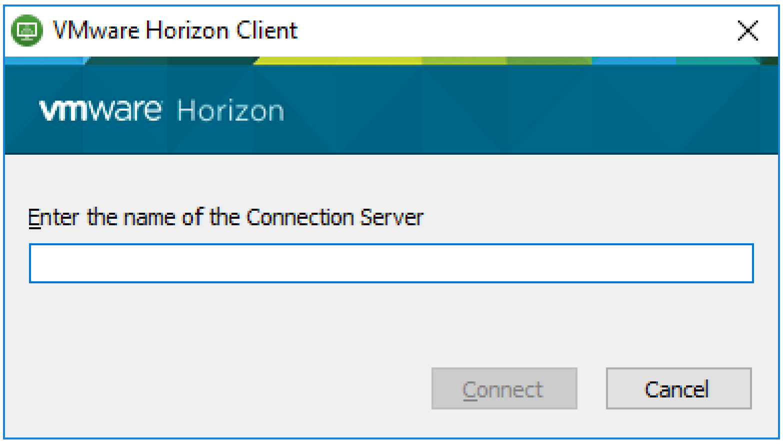
4.1 Accessing VMware View and Horizon Services by Using VMware Horizon Client

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

1. Double click **VMware Horizon 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**.

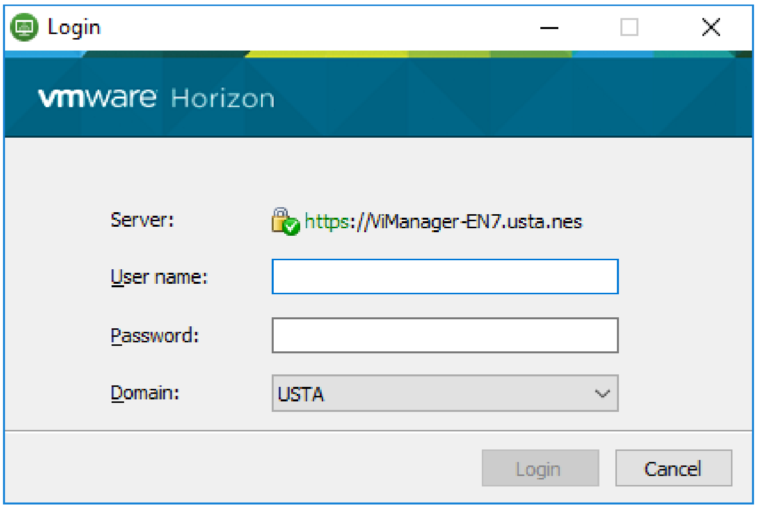


5. By default, a secure connection (HTTPS) is required to connect to the View Connection server. You therefore need to install a certificate.

Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

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**.



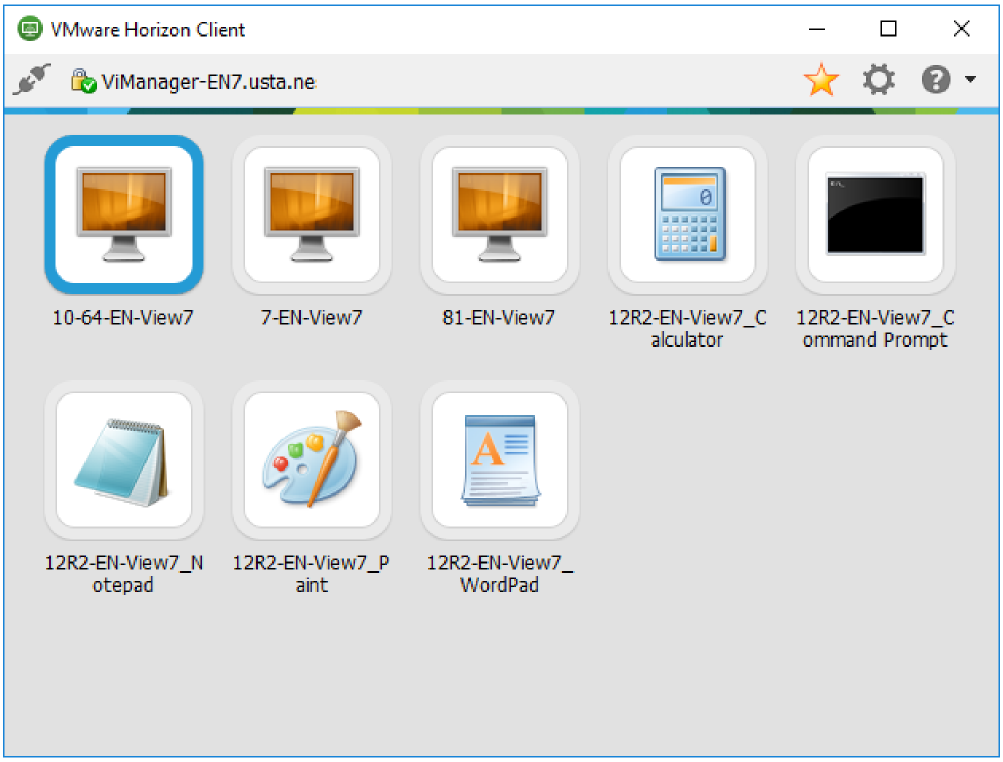
Server: https://ViManager-EN7.usta.nes

User name:

Password:

Domain: USTA

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



9. The desktop will be displayed on the screen.

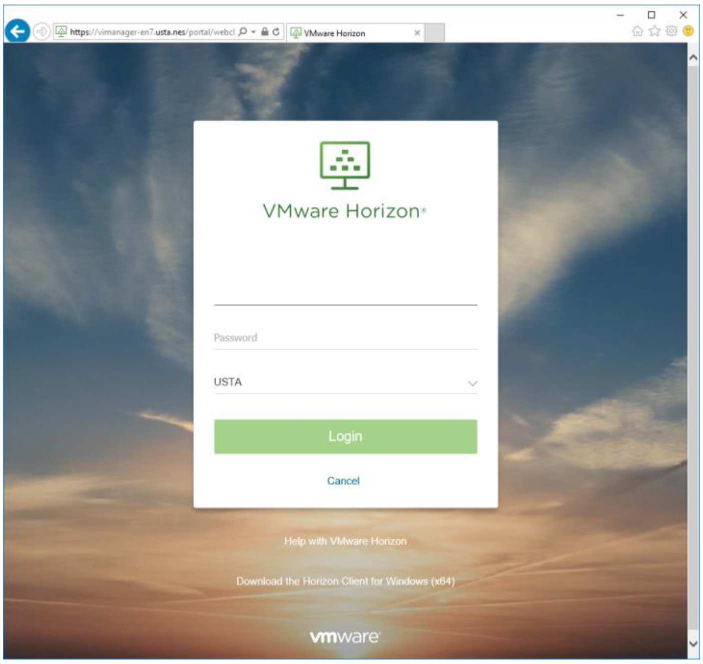
4.2 Accessing VMware View and Horizon Services by Using Internet Explorer

Access VMware View and Horizon Services by using Internet Explorer as follows:

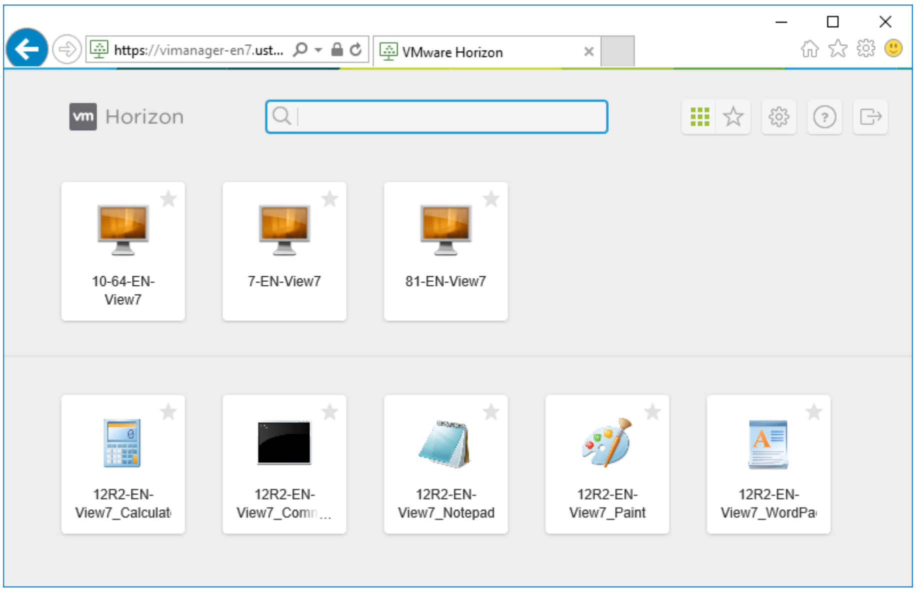
1. By default, a secure connection (HTTPS) is required to connect to VMware View and Horizon Services. You therefore need to install a certificate.

Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

2. Click the Internet Explorer icon on the **Start** screen or taskbar on your desktop to launch Internet Explorer.
3. Enter the IP address, URL, or FQDN of the server through which VMware View and Horizon Services will be accessed.
4. Enter your credentials, and then click **Login**.



5. Icons for connecting to virtual desktops registered in VMware View and Horizon Services are displayed.



6. Select an icon to connect with a virtual desktop.

5. Accessing NEC Client Management Option (CMO) Services

You can access NEC Client Management Option (CMO) Services:

- By using CMO Terminal Agent

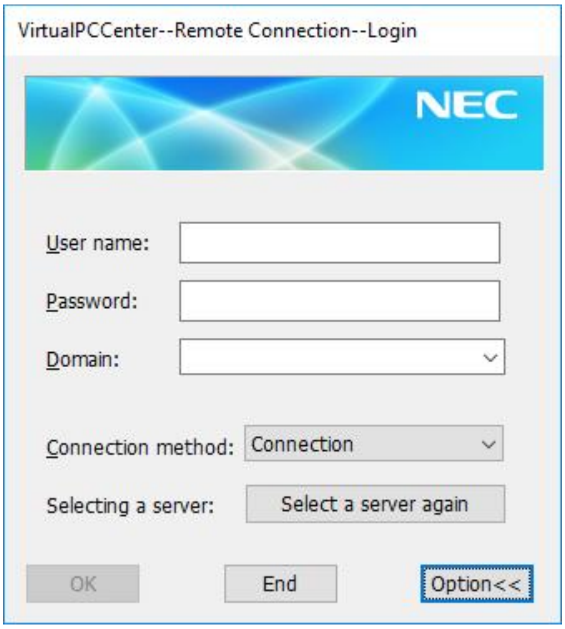
Important **To access NEC Client Management Option (CMO) Services, CMO Terminal Agent must be installed on your US320f (it is not installed by default).**

Your US320f contains a CMO Terminal Agent installer. See Chapter 5, "12. Installing CMO Terminal Agent" for how to install this software.

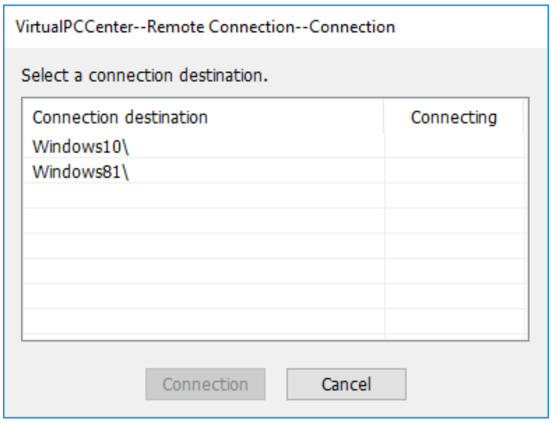
5.1 Accessing NEC Client Management Option (CMO) Services by Using CMO Terminal Agent

Access NEC Client Management Option (CMO) Services by using CMO Terminal Agent as follows:

1. On your desktop, double-click the **Remote Connection** icon.
2. Enter your credentials, and then click **OK**.


VirtualPCCenter--Remote Connection--Login

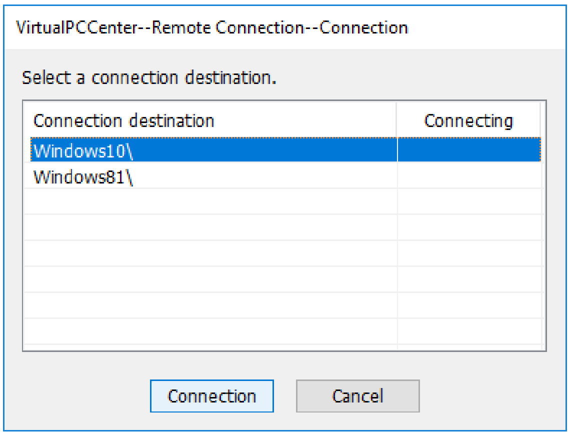
3. A list of virtual desktops registered in NEC Client Management Option (CMO) Services is displayed.


VirtualPCCenter--Remote Connection--Connection

Select a connection destination.

Connection destination	Connecting
Windows10\	
Windows81\	

4. Select the virtual desktop you want to connect to, and then click **Connection**.



VirtualPCCenter--Remote Connection--Connection

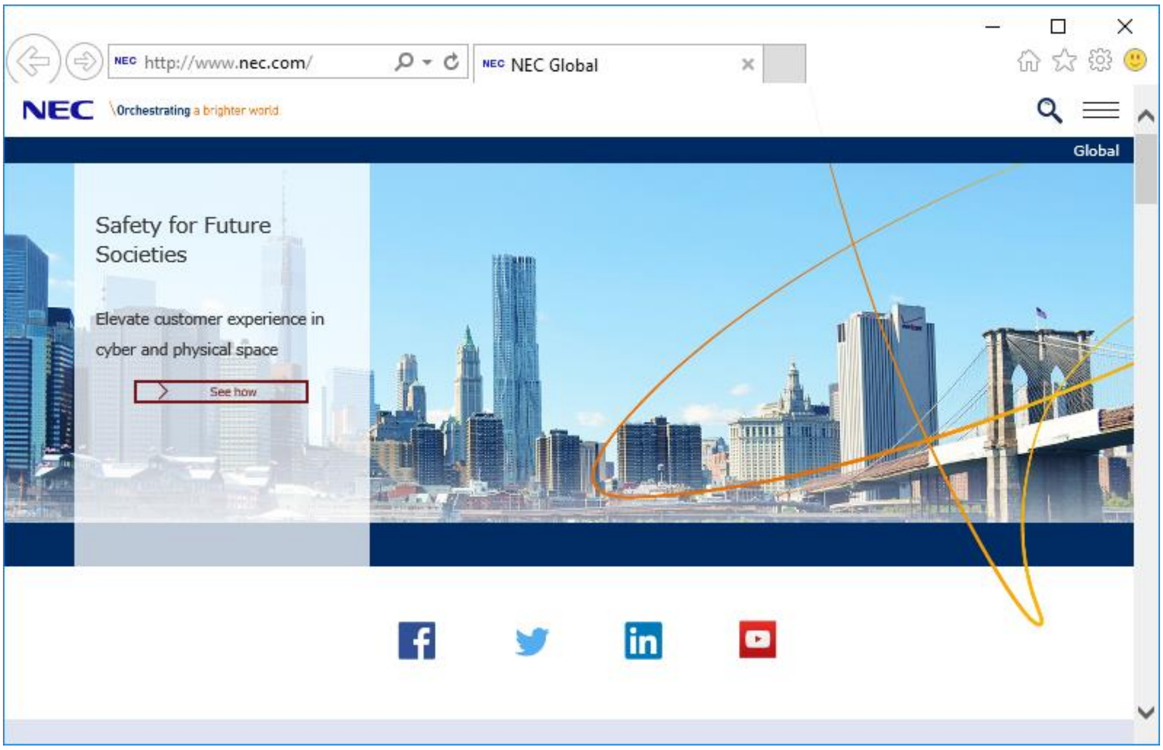
Select a connection destination.

Connection destination	Connecting
Windows10\	
Windows81\	

5. The client is connected to the selected virtual desktop.

6. Browsing the Internet by Using Internet Explorer

Use Microsoft Internet Explorer 11 to browse the Internet. To launch the browser, click **Start** > **Internet Explorer**.


http://www.nec.com/
NEC Global
NEC \Orchestrating a brighter world
Global
Safety for Future Societies
Elevate customer experience in cyber and physical space
See how

NEC Express5800 Series
US320f

4

Chapter 4 Configuring Client Settings with Atrust Client Setup

This chapter provides instructions on how to configure your US320f with Atrust Client Setup.

1. **Atrust Client Setup**

   Describes Atrust Client Setup overview.

2. **Configuring System Settings**

   Describes system settings of Atrust Client Setup.

3. **Configuring External Device Settings**

   Describes how to configure external devices using Atrust Client Setup.

4. **Configuring User Interface Settings**

   Describes how to configure user interface using Atrust Client Setup.

5. **Configuring Service Access Settings**

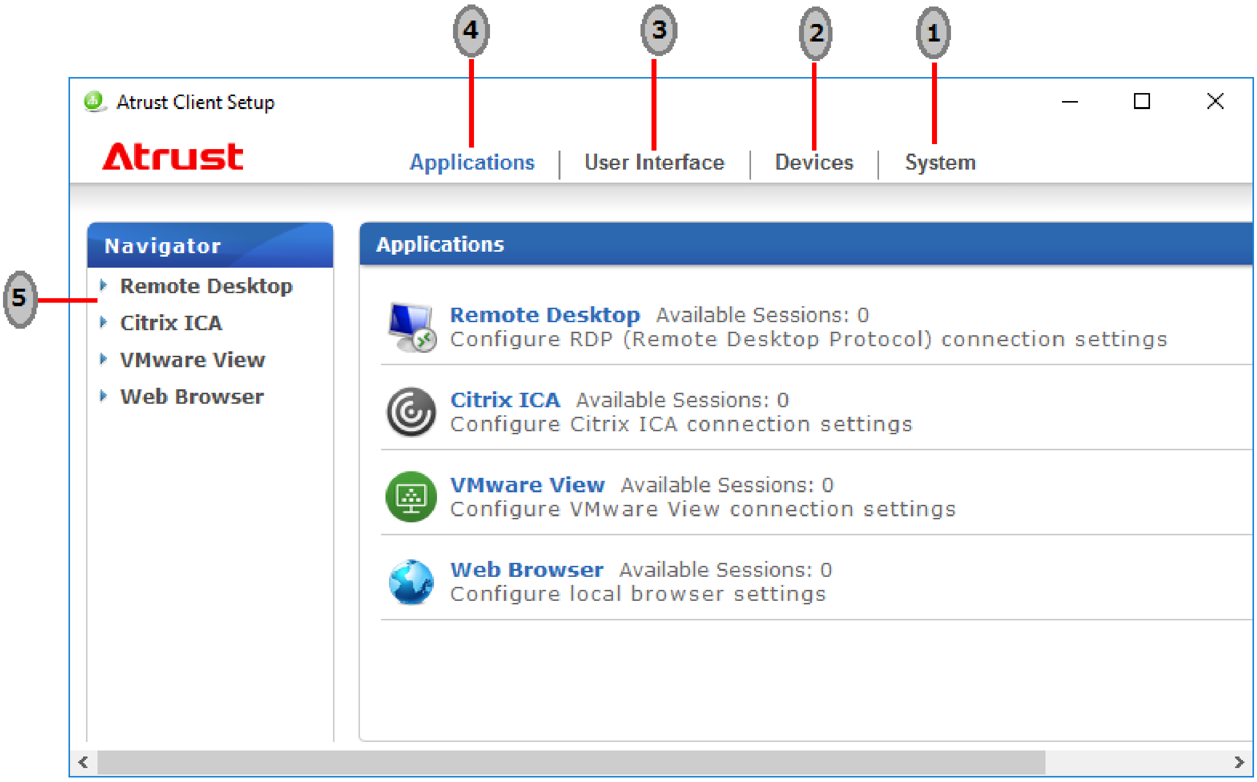
   Describes how to configure service access settings using Atrust Client Setup.

1. Atrust Client Setup (ACS)

1.1 Interface Overview

To access Atrust Client Setup on your US320f thin client, do the following:

1. Log in to your US320f with an administrator account (see Chapter 2 "2. Default User Accounts" for the default account).
2. Click **Atrust Client Setup** on the Start screen.
3. The Atrust Client Setup window appears.



Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

Web Browser Available Sessions: 0
Configure local browser settings

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.

1.2 Client Settings

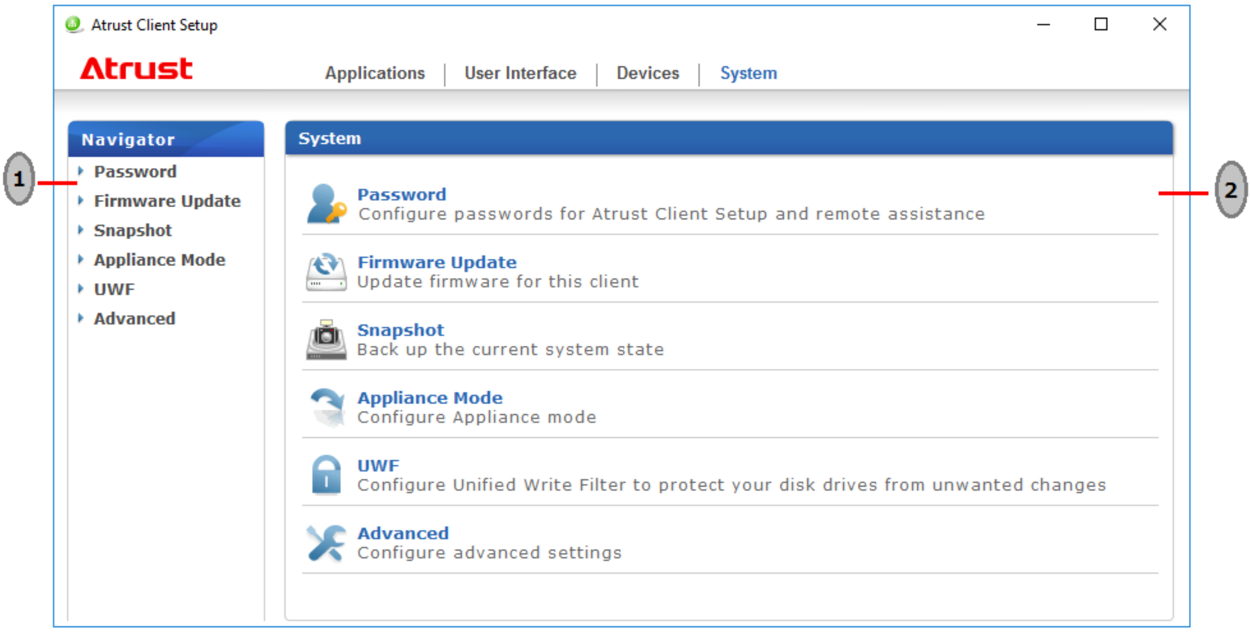
The following table provides a brief description of each setting item under four main setting categories.

Tab	Setting item	Section page
System	• Configuring whether a password is required to access Atrust Client Setup and setting a password • Enabling/disabling remote assistance and setting a password • Updating firmware • Taking snapshots • Enabling/disabling the Appliance mode • Configuring UWF (Unified Writer Filter) • Automatic registration, stealth mode setting	Chapter 4, "2. Configuring System Settings".
Devices	• Configuring settings for USB storage devices • Configuring settings for audio devices	Chapter 4, "3. Configuring External Device Settings".
User Interface	• Configuring whether to display or hide the service access shortcut	Chapter 4, "4. Configuring User Interface Settings".
Applications	• Configuring Microsoft RDP connection settings • Configuring Citrix ICA connection settings • Configuring VMware View connection settings • Configuring Web browser session settings	Chapter 4, "5. Configuring Service Access Settings".

2. Configuring System Settings

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.



Password
Configure passwords for Atrust Client Setup and remote assistance

Firmware Update
Update firmware for this client

Snapshot
Back up the current system state

Appliance Mode
Configure Appliance mode

UWF
Configure Unified Write Filter to protect your disk drives from unwanted changes

Advanced
Configure advanced settings

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.

2.2 Available Settings

Tab	Setting	Icon	Description	Section page
System	Password		Click to set a password to access Atrust Client Setup. You can enable or disable remote assistance and set a password here.	- Chapter 4 "2.3 Setting a Password to Access Atrust Client Setup" - Chapter 4 "2.4 Configuring Shadow Settings for Remote Assistance"
	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.	- Chapter 4, "2.5 Updating Firmware from the Management Computer".
	Snapshot		Click to take a snapshot (system image) of the client for mass deployment.	- Chapter 4, "2.6 Taking Snapshots for Mass Deployment".
	Appliance Mode		Click to enable/disable the Appliance mode to allow/disallow the automatic RDP / Citrix ICA / VMware View sessions. In Appliance mode, the client starts up with the desired RDP / Citrix ICA / VMware View session and shuts down when the user logs out.	- Chapter 4, "2.8 Enabling or Disabling the Appliance Mode"
	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. After restart, all changes will be discarded.	- Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".
	Advanced		You can automatically register US320f in Atrust Device Manager and set the stealth mode to disable manual detection of US320f by IP range from Atrust Device Manager.	- Chapter 4, "2.10 Enabling / Disabling Automatic Registration and Stealth Mode"

Note

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

2.3 Setting a Password to Access Atrust Client Setup

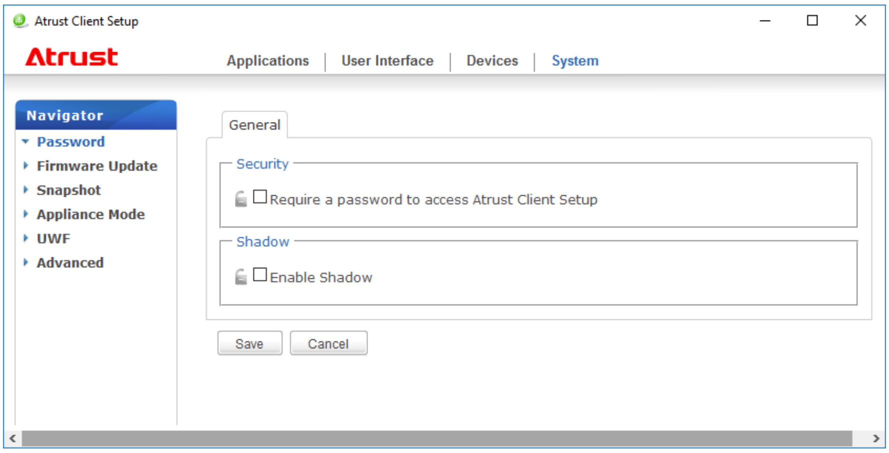
You can set a password to access Atrust Client Setup.

Note

- Only the system administrator and manager are allowed to access Atrust Client Setup by default. So, if you do not set a password, system administrator privileges are sufficient to access Atrust Client Setup. If you set a password, that password must be entered to launch Atrust Client Setup.
- If a password to access Atrust Client Setup is set, the standard US320f user needs the following two passwords to access Atrust Client Setup: the password for the administrator account in Windows 10 IoT Enterprise LTSB and the password to access Atrust Client Setup.

To set a password to access Atrust Client Setup, do the following:

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

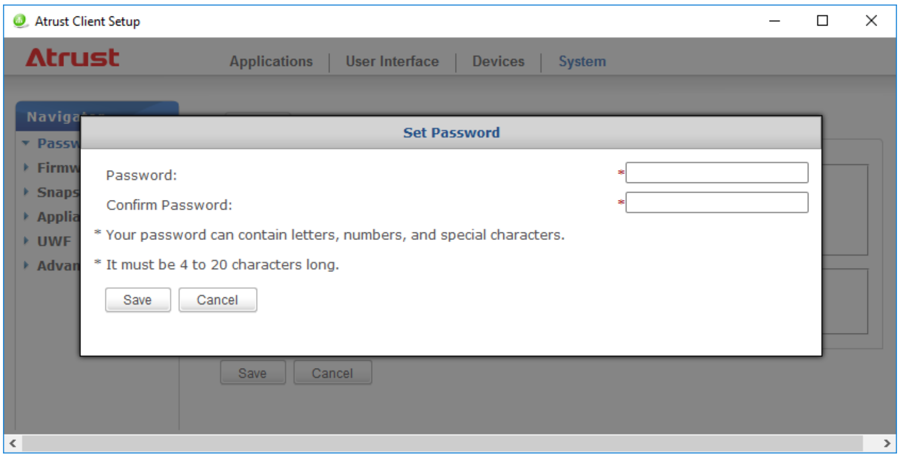


□ Require a password to access Atrust Client Setup

□ Enable Shadow

2. Check **Security** > **Require a password to access Atrust Client Setup**.

3. A window appears for you to set the password.



Password: *

Confirm Password: *

* Your password can contain letters, numbers, and special characters.

* It must be 4 to 20 characters long.

4. Enter an arbitrary password and click **Save** to apply it.

5. Click **Save** to save all the changes.

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.

Important **Although VNC (remote shadow) is convenient, security consideration is necessary. When enabling remote shadow of US320f, you can connect from other VNC client software as well as connection from ADM if you know even password.**

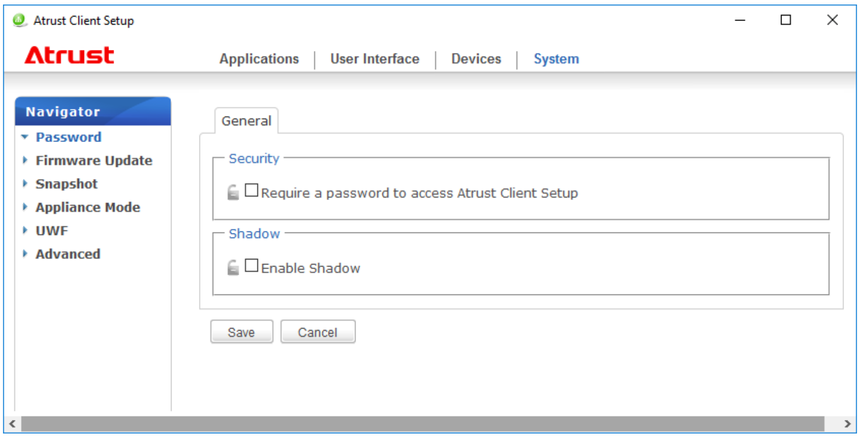
Therefore, it is necessary to take security measures such as using only inside the firewall or invalidating unnecessary VNC.

Note By enabling "Japanese keyboard" in the Remote Shadow Viewer option, it is possible to switch to Japanese input mode by using Kanji key of keyboard.

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, refer to the User's Guide of Atrust Device Manager.

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

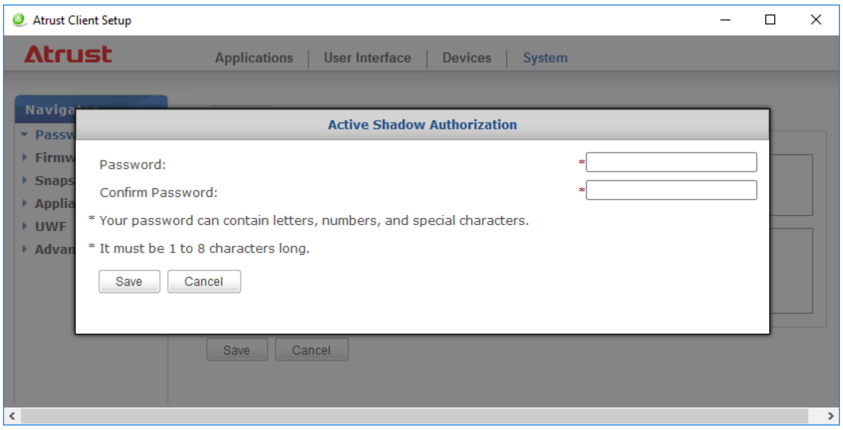
1. On Atrust Client Setup, click **System** > **Password**.



□Require a password to access Atrust Client Setup

□Enable Shadow

2. Check **Shadow** > **Enable Shadow**.
3. The Shadow feature is enabled and a window appears for you to set a password for remote assistance.


Atrust Client Setup
Atrust
Applications | User Interface | Devices | System
Active Shadow Authorization
Save
Cancel

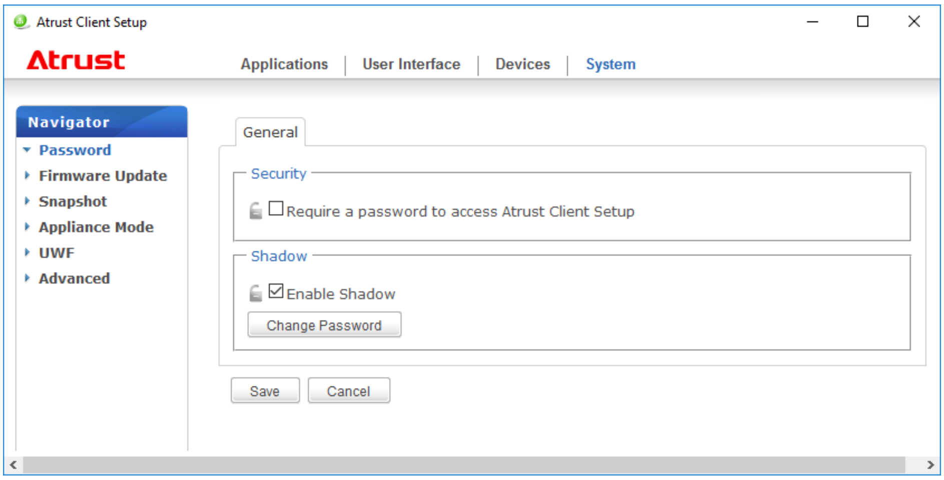
Password: *

Confirm Password: *

* Your password can contain letters, numbers, and special characters.

* It must be 1 to 8 characters long.

4. Set a password and click **Save**.
5. Click **Save** and confirm that "Your settings have been saved." appears.



☐ Require a password to access Atrust Client Setup

☑ Enable Shadow

Note

When the Shadow feature is enabled, the 👁 icon is displayed on the Notification area of the Taskbar in US320f. When this feature is being executed from the remote computer, the icon color changes to yellow 👁.

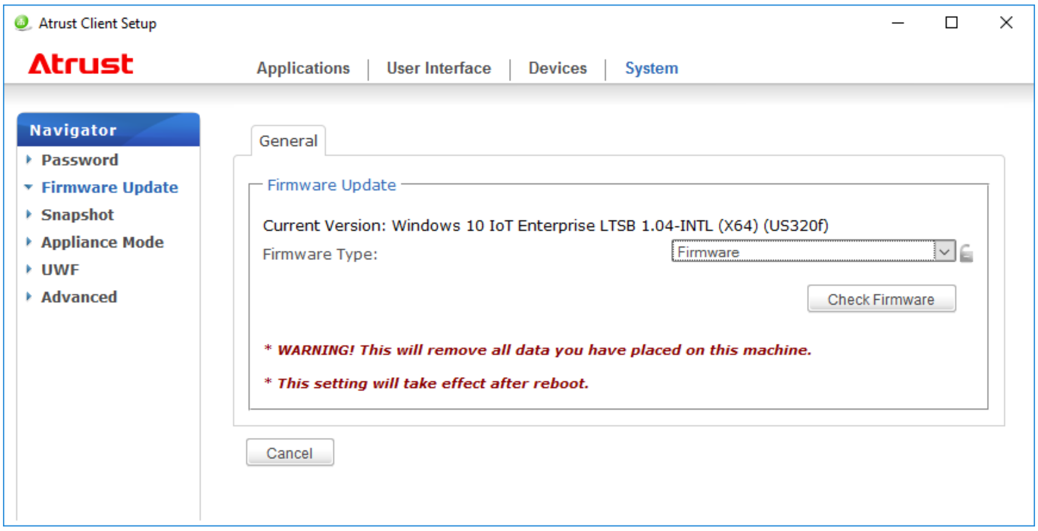
2.5 Updating Firmware from the Management Computer

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.

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

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



Current Version: Windows 10 IoT Enterprise LTSB 1.04-INTL (X64) (US320f)

Firmware Type: Firmware

* WARNING! This will remove all data you have placed on this machine.

* This setting will take effect after reboot.

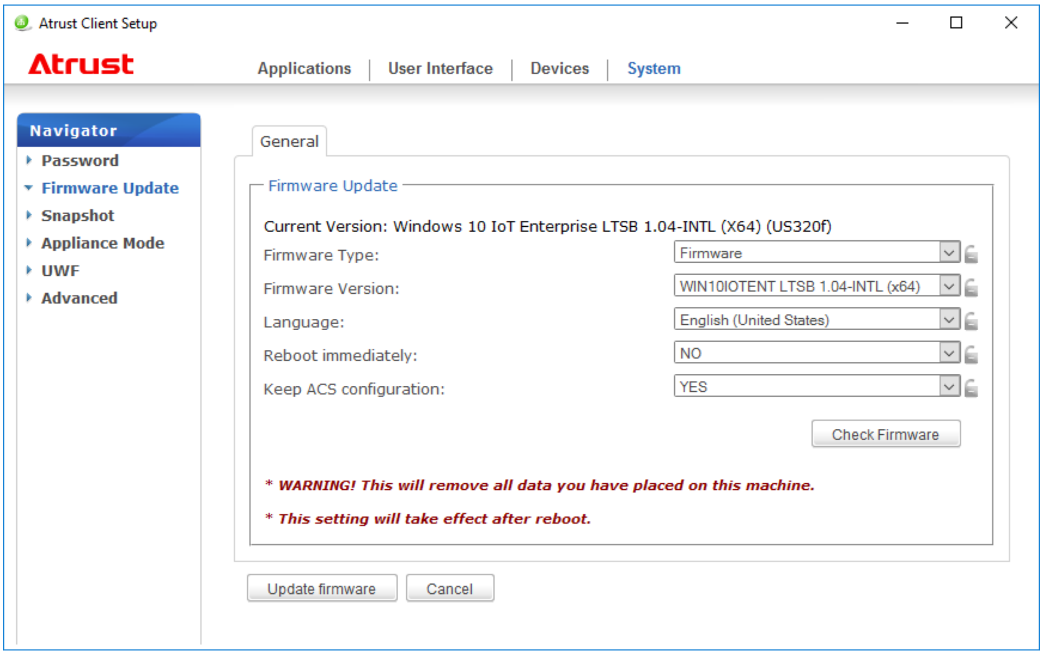
2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Firmware**. The system will then automatically download the Firmware list from the remote computer.

Note You can also update the firmware of a client with a snapshot (the system image of a client) which is coming from another client of the same model and is with a newer firmware version. For detailed information, see Chanter 4, "2.6 Taking Snapshots for Mass Deployment" about the snapshot.

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.



Current Version: Windows 10 IoT Enterprise LTSB 1.04-INTL (X64) (US320f)

Firmware Type: Firmware

Firmware Version: WIN10IOTENT LTSB 1.04-INTL (x64)

Language: English (United States)

Reboot immediately: NO

Keep ACS configuration: YES

* WARNING! This will remove all data you have placed on this machine.

* This setting will take effect after reboot.

Firmware Update Options

Item	Description
Firmware Type	Click to select the desired firmware type. <table><tr><th>Type</th><th>Description</th></tr><tr><td>**Firmware**</td><td>The system image of a client.</td></tr><tr><td>**Snapshot**</td><td>The system image of a client coming from another client of the same model.</td></tr></table>
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, refer to the User's Guide of Atrust Device Manager.

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

2.6 Taking Snapshots for Mass Deployment

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

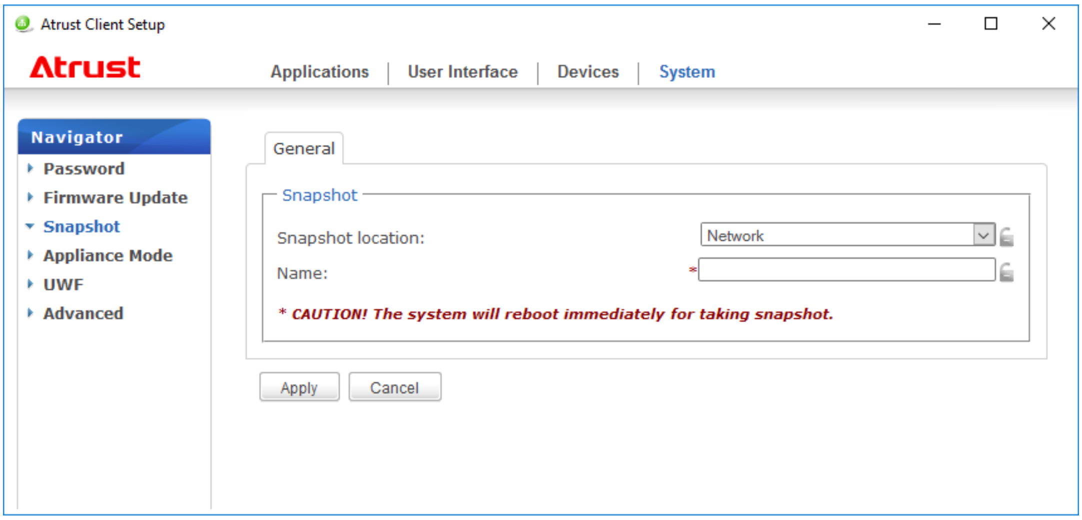
Note

- 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.
- When taking a snapshot, 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.
- Taking a snapshot will reset the startup behavior to the default (auto-sign-in with the default standard user account). For details, see Chapter 2, "3. The Behavior of System Startup".
- In case of taking a snapshot in an USB flash memory, you need at least 32 megabytes of flash memory that is not encrypted.
- When taking a snapshot in an USB flash memory, USB flash memory is formated.
- When taking a snapshot in a remote management computer, a remote management computer needs at least 8 gigabytes of free space.

2.6.1 Taking a snapshot in an USB flash memory

To create a snapshot stored in an USB flash memory from the thin client, do the following:

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

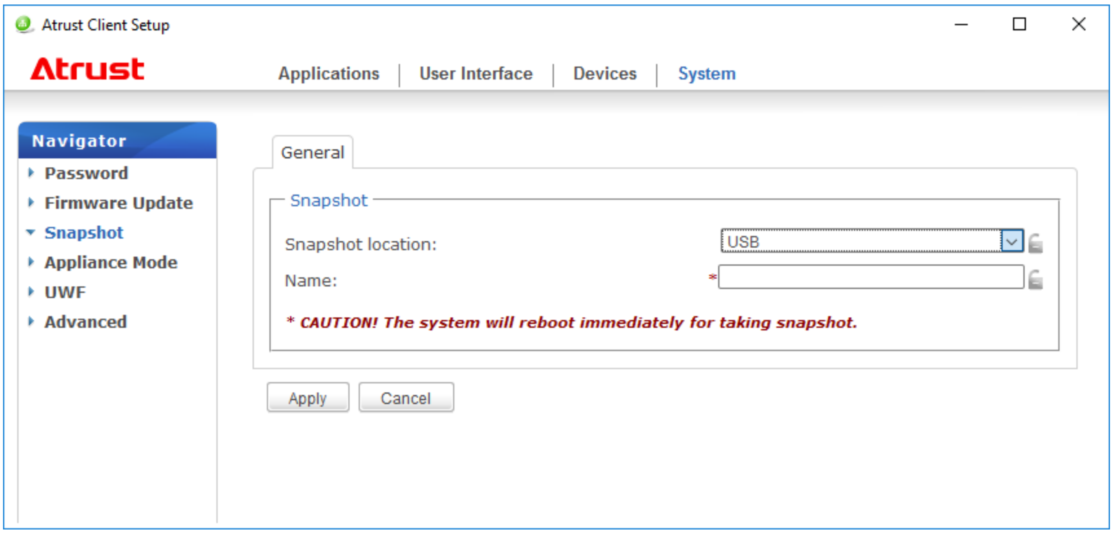


Snapshot location: Network

Name:

* CAUTION! The system will reboot immediately for taking snapshot.

2. Select the location to save the snapshot from **Snapshot location** in the **Snapshot** section. You can select **USB**.

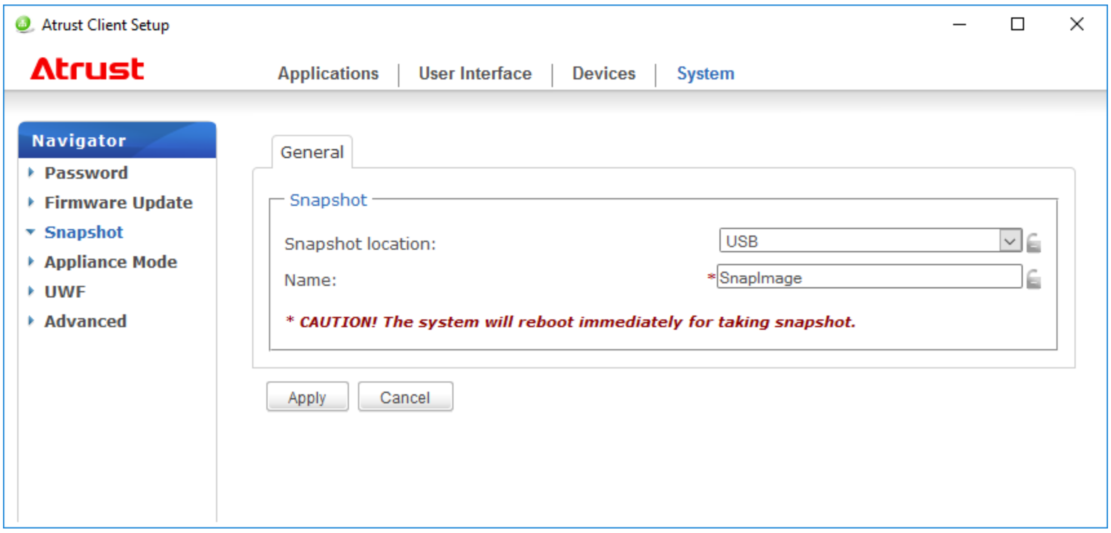


Snapshot location: USB

Name: *

* CAUTION! The system will reboot immediately for taking snapshot.

3. Fill in **Name.**

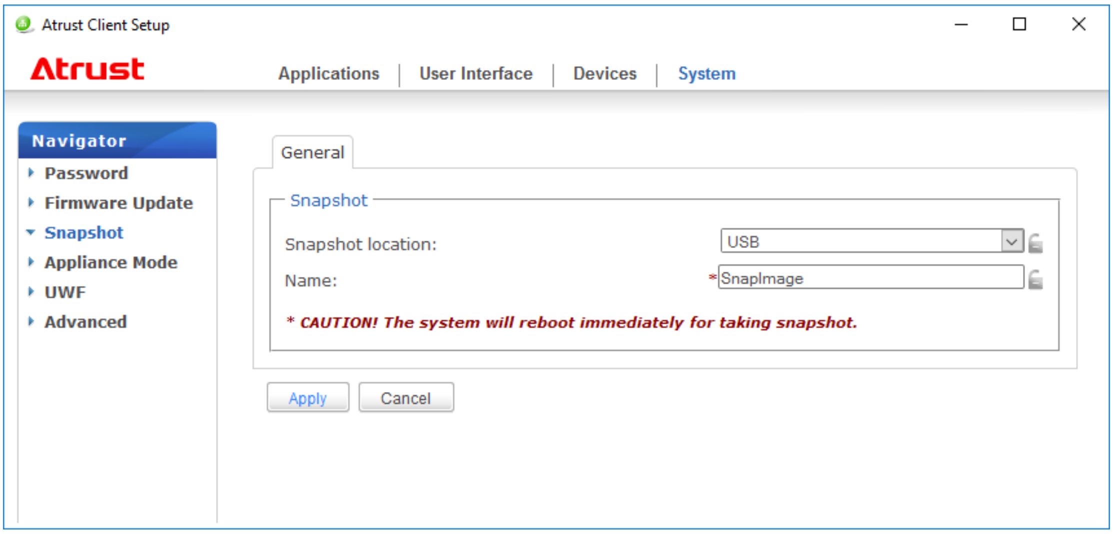


Snapshot location: USB

Name: *SnapImage

* CAUTION! The system will reboot immediately for taking snapshot.

4. Click **Apply**.

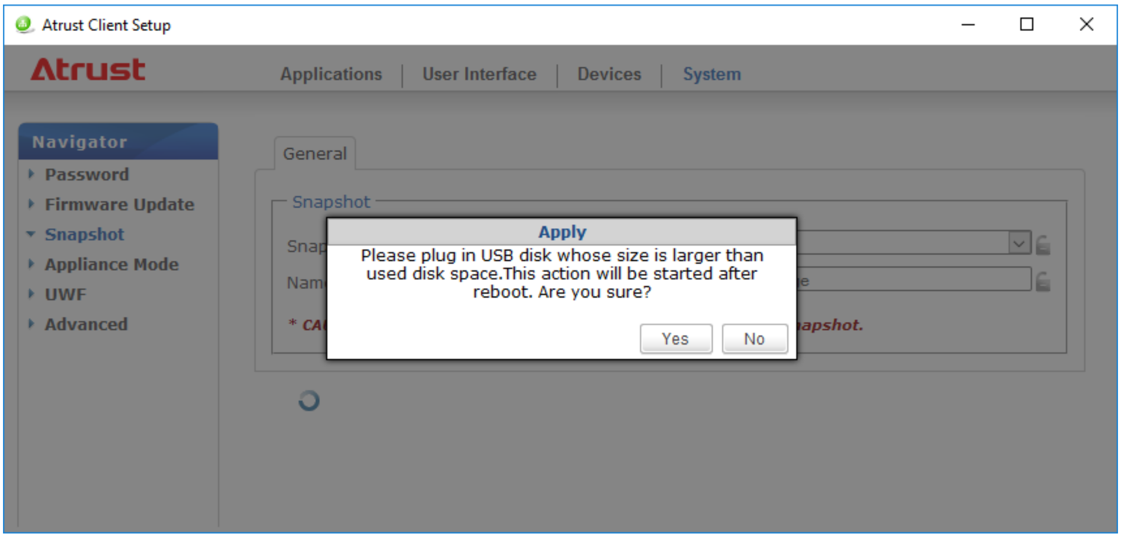


Snapshot location: USB

Name: *SnapImage

* CAUTION! The system will reboot immediately for taking snapshot.

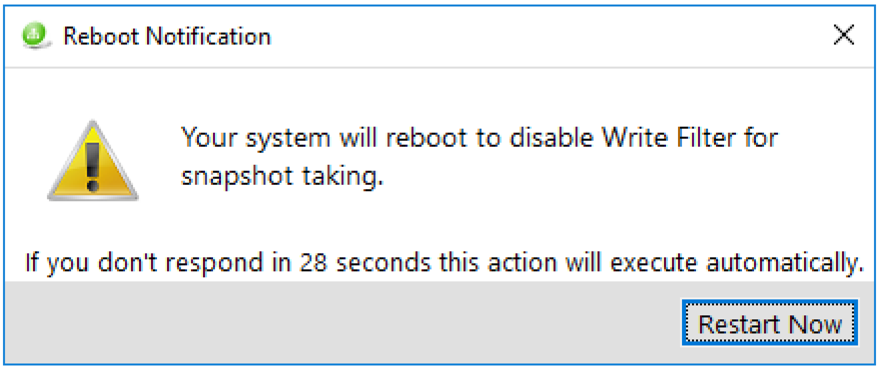
5. A message appears prompting you for confirmation. Click **Yes**.



Apply

Please plug in USB disk whose size is larger than used disk space.This action will be started after reboot. Are you sure?

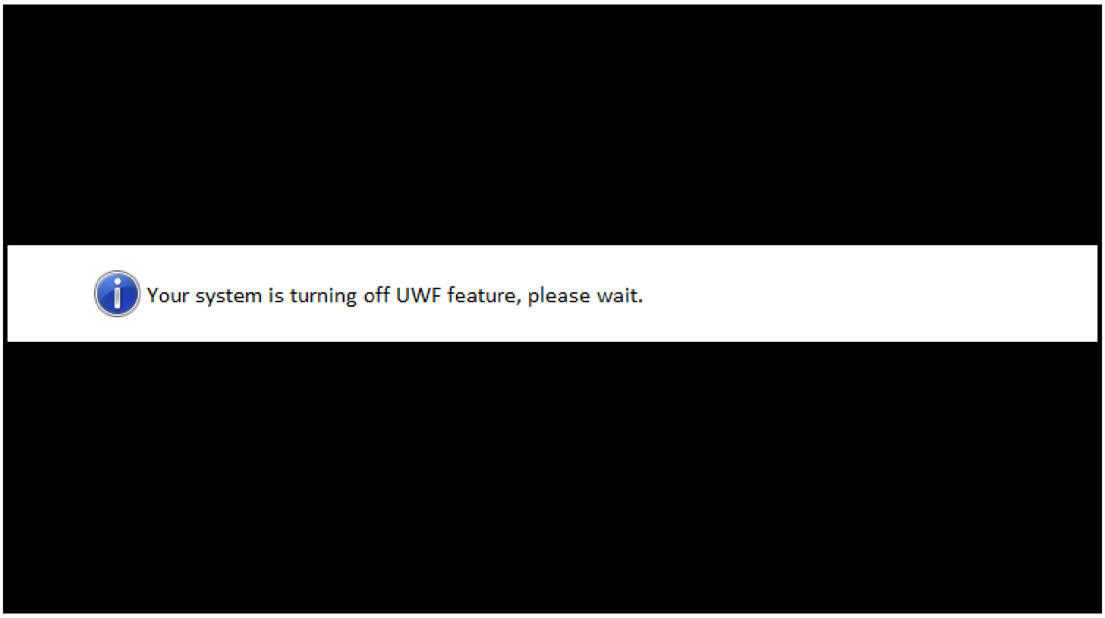
6. The Reboot Notification dialog appears. After inserting an USB flash memory in the thin client, click **Restart Now**.


Reboot Notification

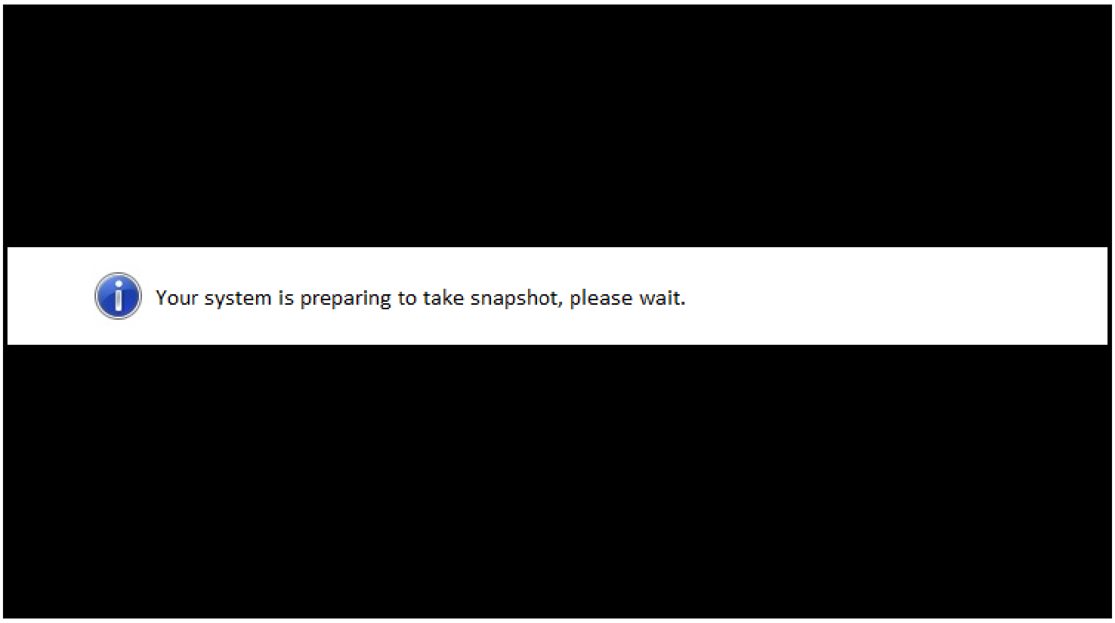
Your system will reboot to disable Write Filter for snapshot taking.

If you don't respond in 28 seconds this action will execute automatically.

7. After restarting, the following message is appeared. Wait a few minutes. Thin client is restarted automatically.

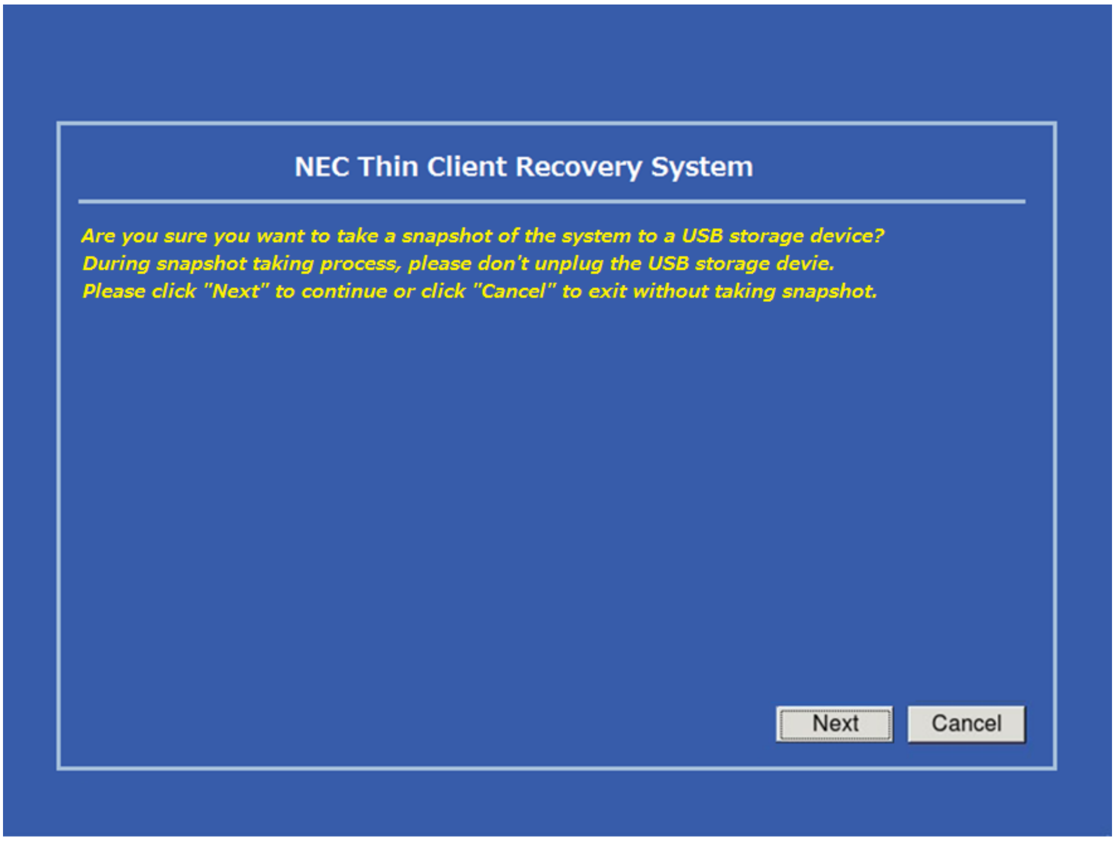

Your system is turning off UWF feature, please wait.

8. After restarting, the following message is appeared. Wait a few minutes. Thin client is restarted automatically.



Your system is preparing to take snapshot, please wait.

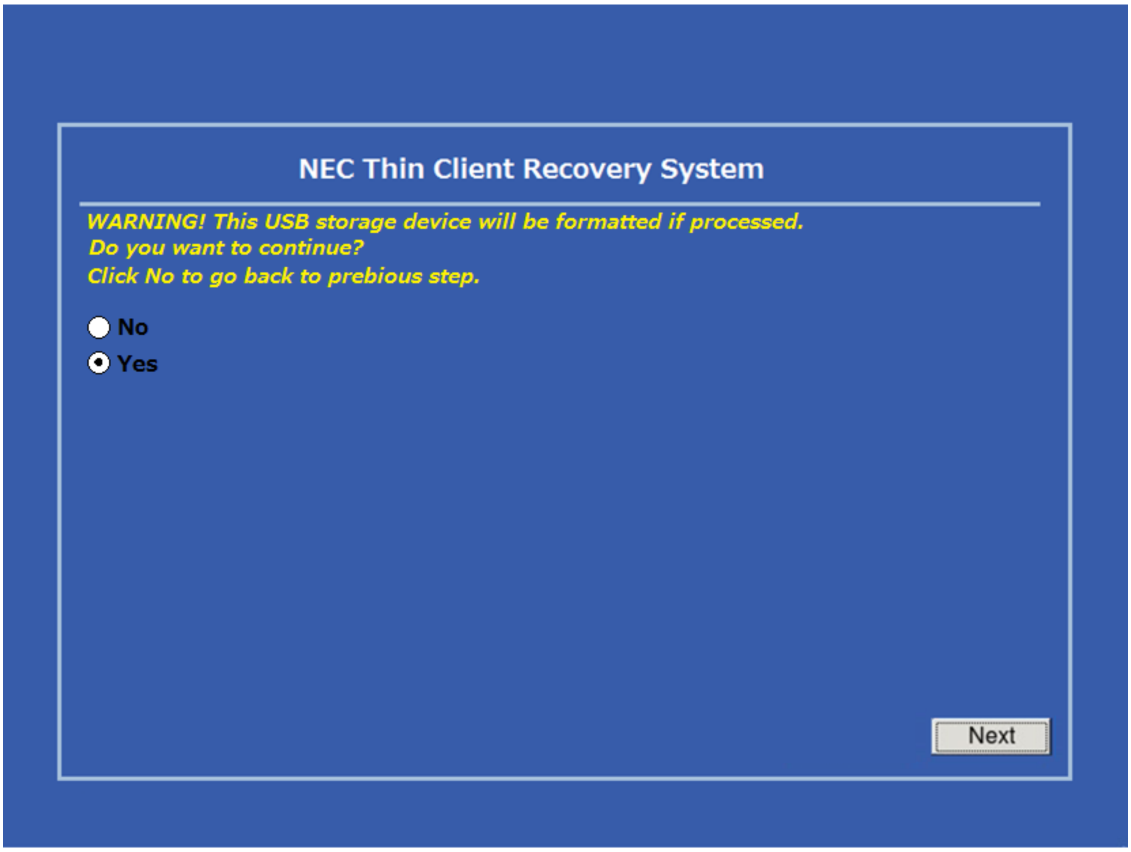
9. After restarting, the NEC Thin Client Recovery System screen appears. Click **Next.**



NEC Thin Client Recovery System

Are you sure you want to take a snapshot of the system to a USB storage device?
During snapshot taking process, please don't unplug the USB storage devie.
Please click "Next" to continue or click "Cancel" to exit without taking snapshot.

10. The following screen is indicated to confirm the formating of USB flash memory. Check **Yes,** and click **Next.**



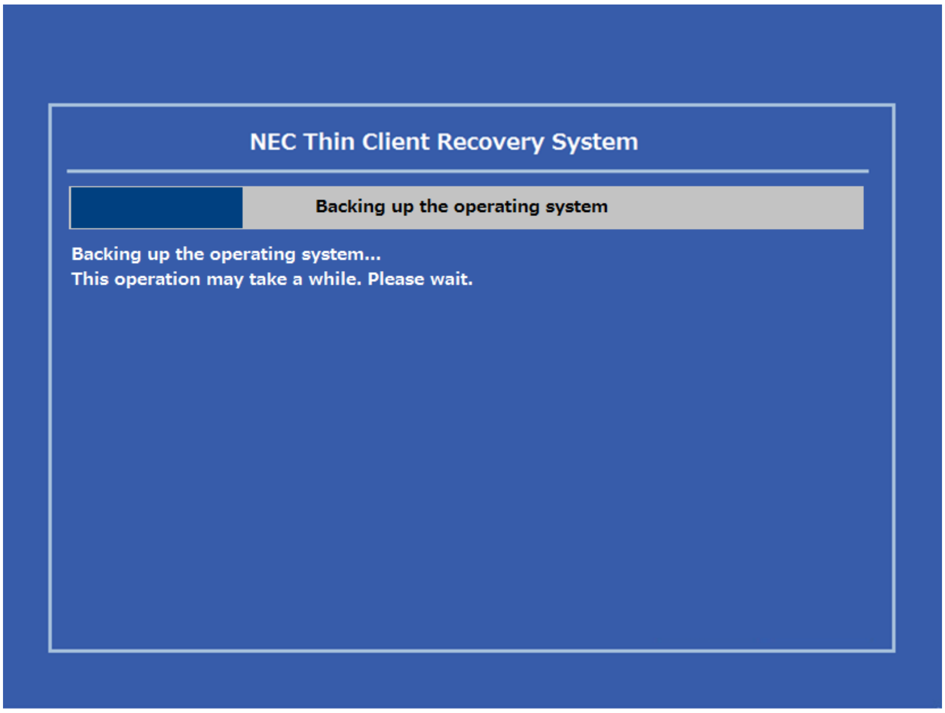
NEC Thin Client Recovery System

WARNING! This USB storage device will be formatted if processed.
Do you want to continue?
Click No to go back to prebious step.

○ No
● Yes

11. After formatting USB flash memory, taking a snapshot launches automatically. Wait a moment until processing is completed automatically.

Note It takes tens of minutes for taking a snapshot, and the system resterts automatically more than one times. System Preparation Utility (Sysprep) executes at background, therefore this process doesn't indicate in desktop.



NEC Thin Client Recovery System

Backing up the operating system

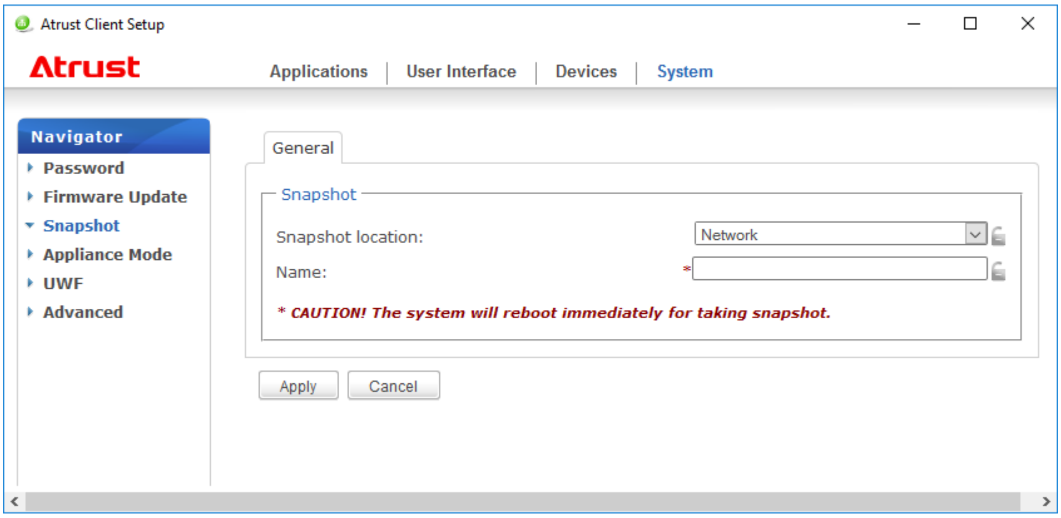
Backing up the operating system...
This operation may take a while. Please wait.

12. When displaying User Account's desktop, taking a snapshot is completed.

2.6.2 Taking a snapshot in a remote management computer

To create a snapshot stored in a remote management computer from the thin client, do the following:

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



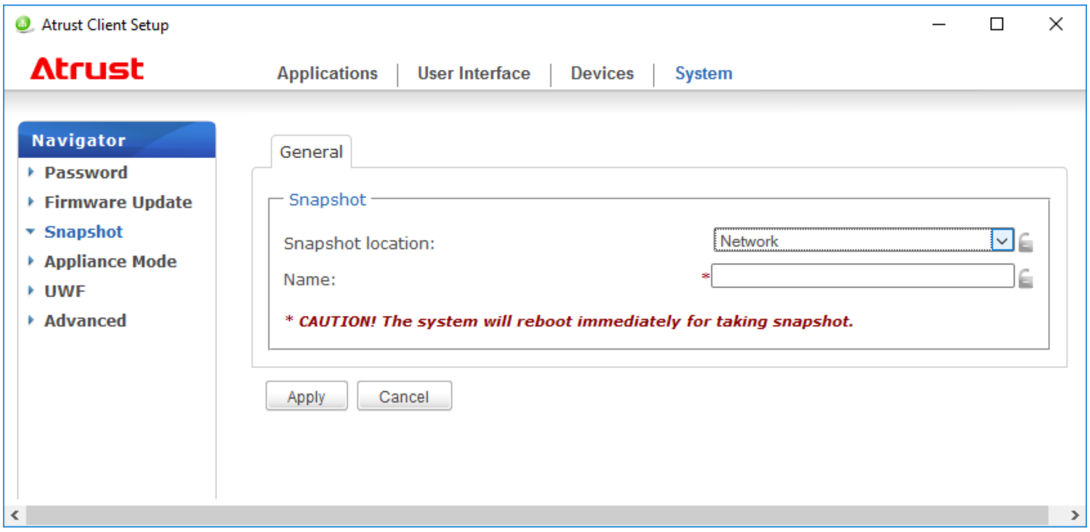
Snapshot

Snapshot location: Network

Name: *

* CAUTION! The system will reboot immediately for taking snapshot.

2. Select the location to save the snapshot from **Snapshot location** in the **Snapshot** section. You can select **Network**.

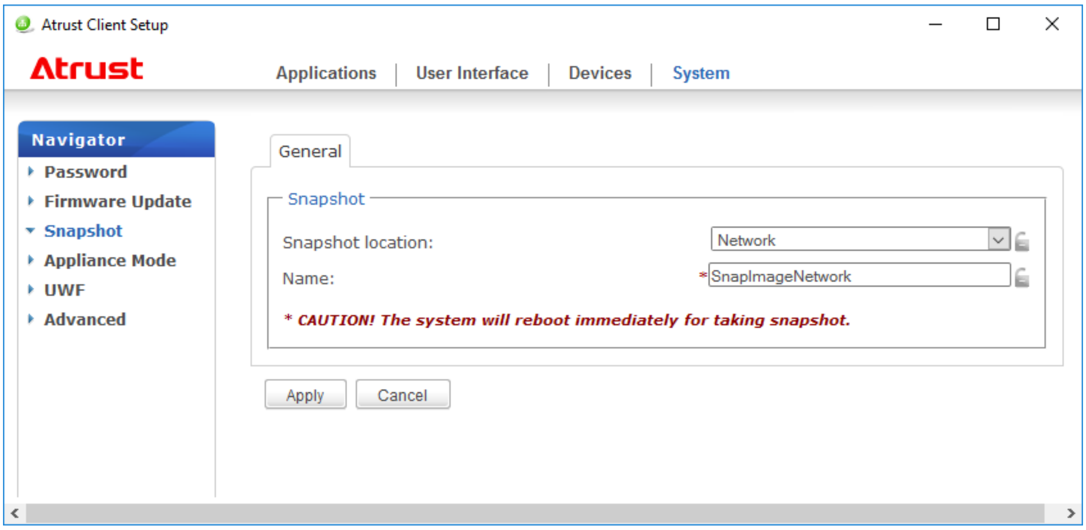


Snapshot location: Network

Name: *

* CAUTION! The system will reboot immediately for taking snapshot.

3. Fill in **Name**.

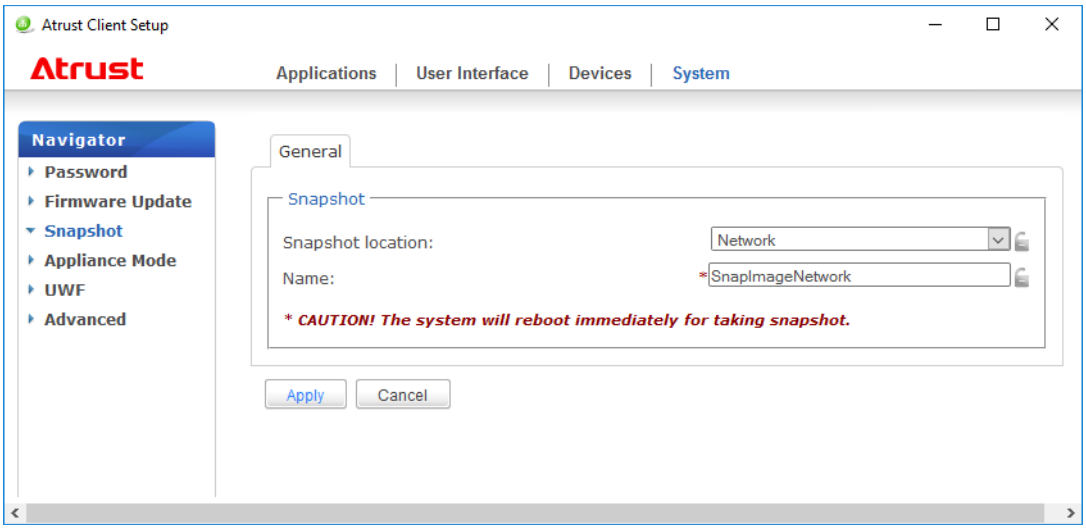


Snapshot location: Network

Name: *SnapImageNetwork

* CAUTION! The system will reboot immediately for taking snapshot.

4. Click **Apply**.

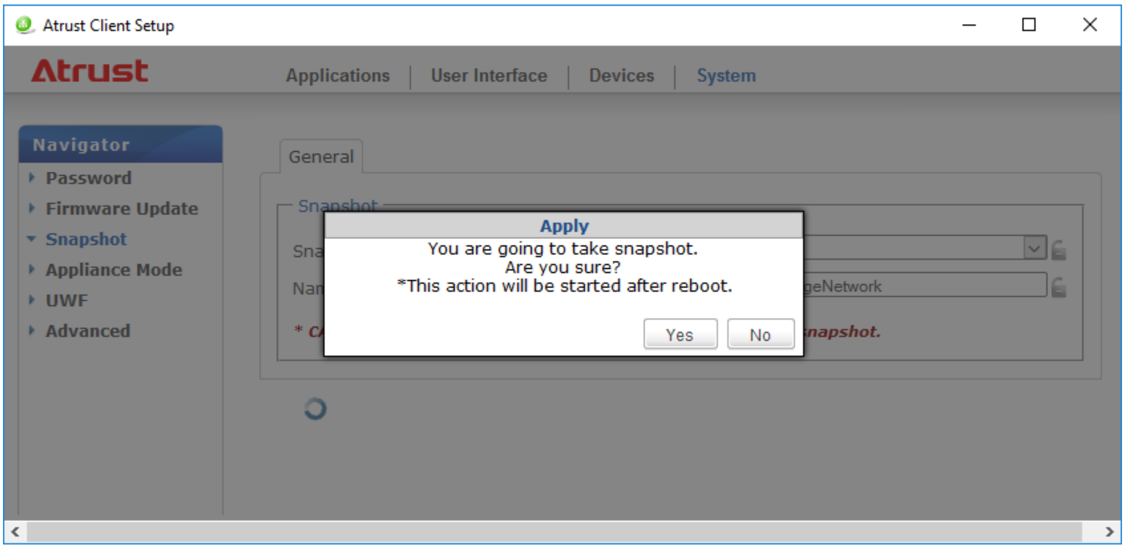


Snapshot location: Network

Name: *SnapImageNetwork

* CAUTION! The system will reboot immediately for taking snapshot.

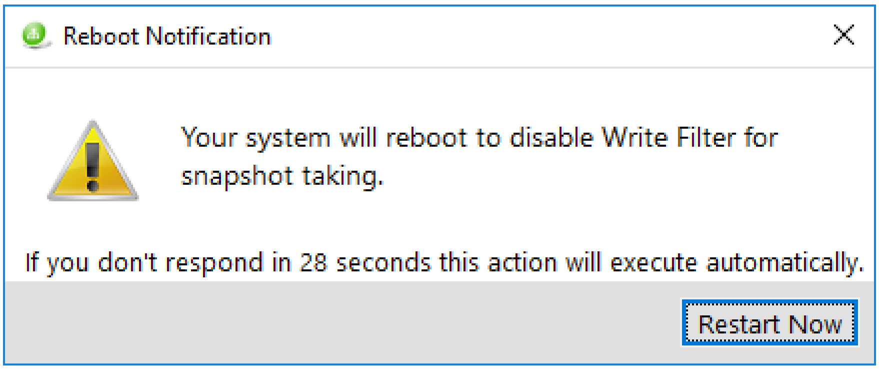
5. A message appears prompting you for confirmation. Click **Yes**.



Apply

You are going to take snapshot.
Are you sure?
*This action will be started after reboot.

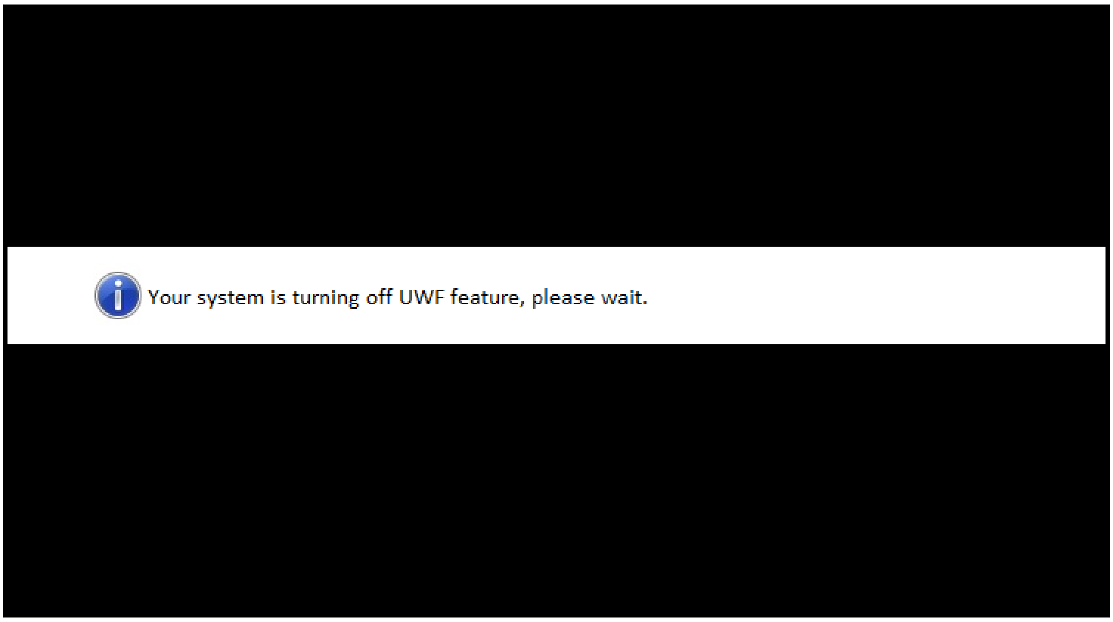
6. The Reboot Notification dialog appears. Click **Restart Now**.



Your system will reboot to disable Write Filter for snapshot taking.

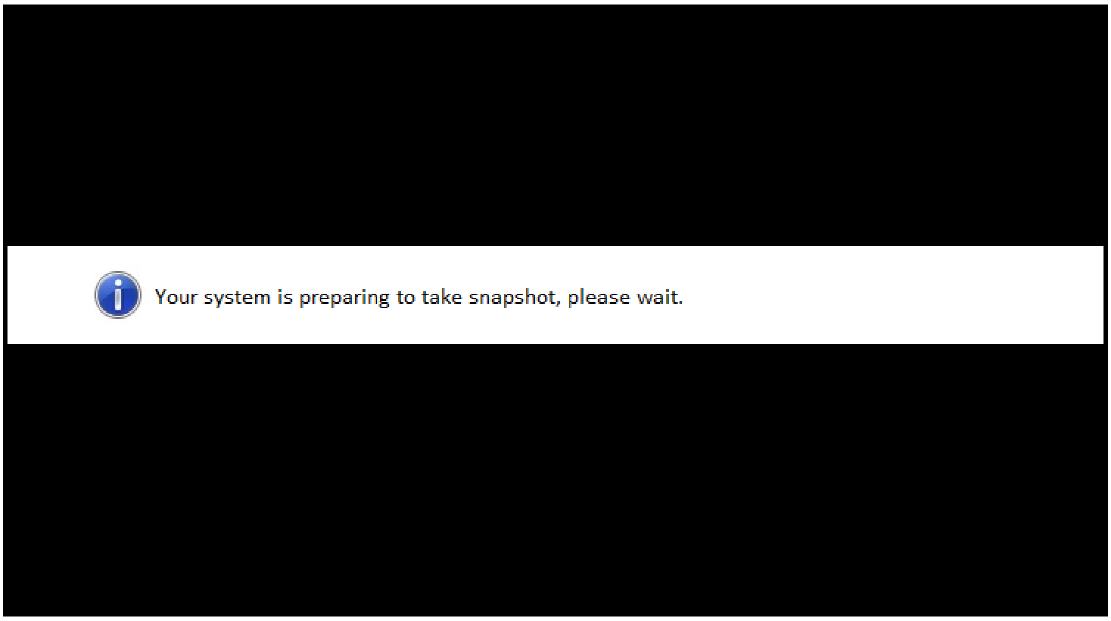
If you don't respond in 28 seconds this action will execute automatically.

7. After restarting, the following message is appeared. Wait a few minutes. Thin client is restarted automatically.



Your system is turning off UWF feature, please wait.

8. After restarting, the following message is appeared. Wait a few minutes. Thin client is restarted automatically.

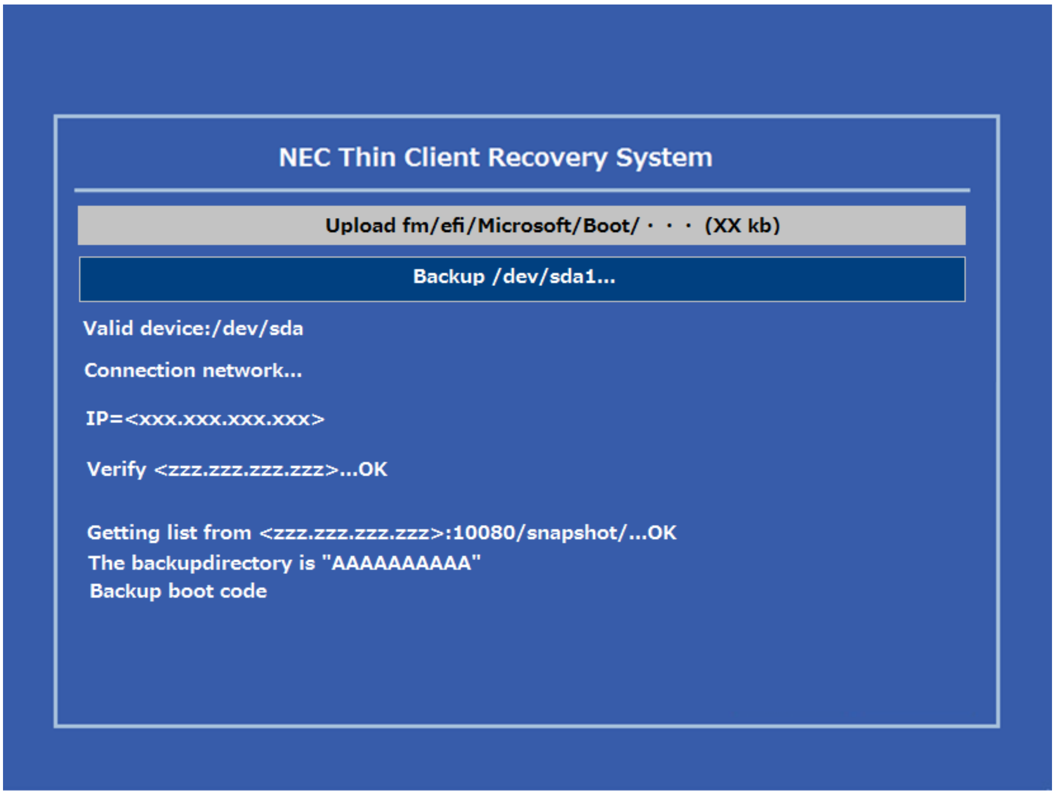


Your system is preparing to take snapshot, please wait.

9. After restarting, the NEC Thin Client Recovery System screen appears. Taking a snapshot launches automatically. Wait a moment until processing is completed automatically.

Note

It takes tens of minutes for taking a snapshot, and the system resterts automatically more than one times. System Preparation Utility (Sysprep) executes at background, therefore this process doesn't indicate in desktop.

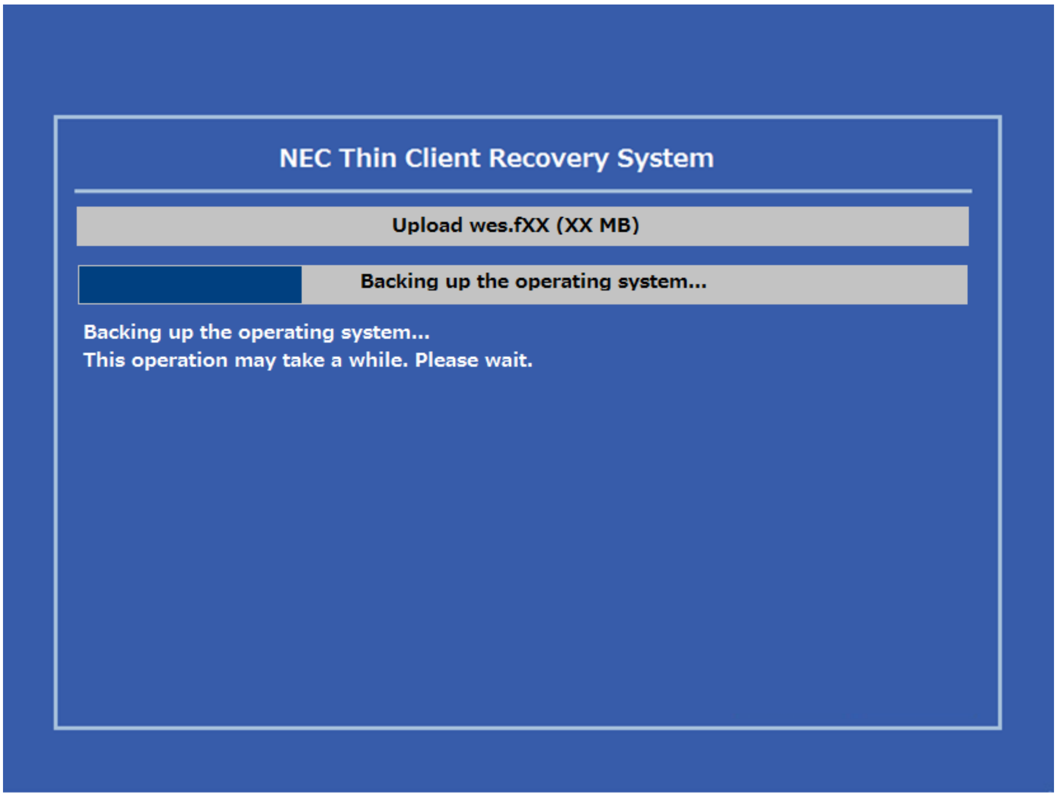


NEC Thin Client Recovery System

Upload fm/efi/Microsoft/Boot/・・・ (XX kb)

Backup /dev/sda1...

```
Valid device:/dev/sda
Connection network...
IP=<xxx.xxx.xxx.xxx>
Verify <zzz.zzz.zzz.zzz>...OK
Getting list from <zzz.zzz.zzz.zzz>:10080/snapshot/...OK
The backupdirectory is "AAAAAAAAAA"
Backup boot code
```



NEC Thin Client Recovery System

Upload wes.fXX (XX MB)

Backing up the operating system...

Backing up the operating system...
This operation may take a while. Please wait.

10. When displaying User Account's desktop, taking a snapshot is completed. A snapshot is uploaded to a remote management computer.

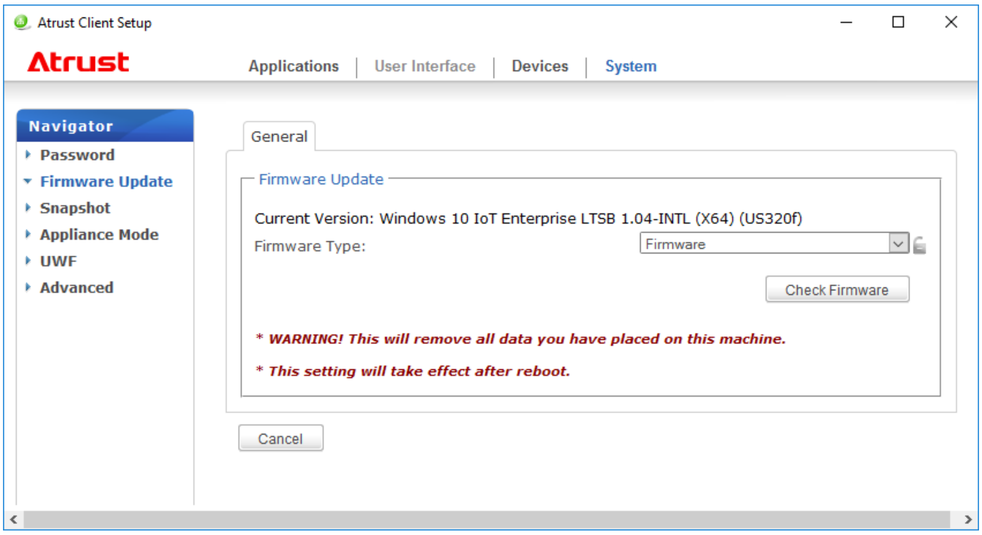
2.7 Deploying a System Image Using a Taken Snapshot

Snapshots can be saved on a remote computer via the network or in the USB flash memory. The system image can be deployed via the network or the USB flash memory depending on where the snapshot is saved.

2.7.1 Deploying a Snapshot System Image via Network

To deploy a system image to US320f by using a snapshot on a remote computer, do the following:

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



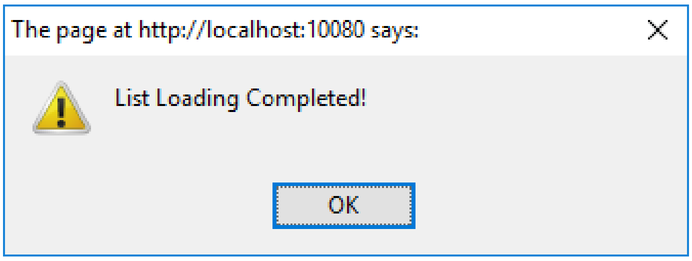
Current Version: Windows 10 IoT Enterprise LTSB 1.04-INTL (X64) (US320f)

Firmware Type: Firmware

* WARNING! This will remove all data you have placed on this machine.

* This setting will take effect after reboot.

2. Select **Snapshot** from **Firmware Type** in the **Firmware Update** section. A list of snapshots is automatically downloaded from the remote computer.
3. When download is completed, a message appears notifying you that the snapshot list has been loaded. Click **OK**.

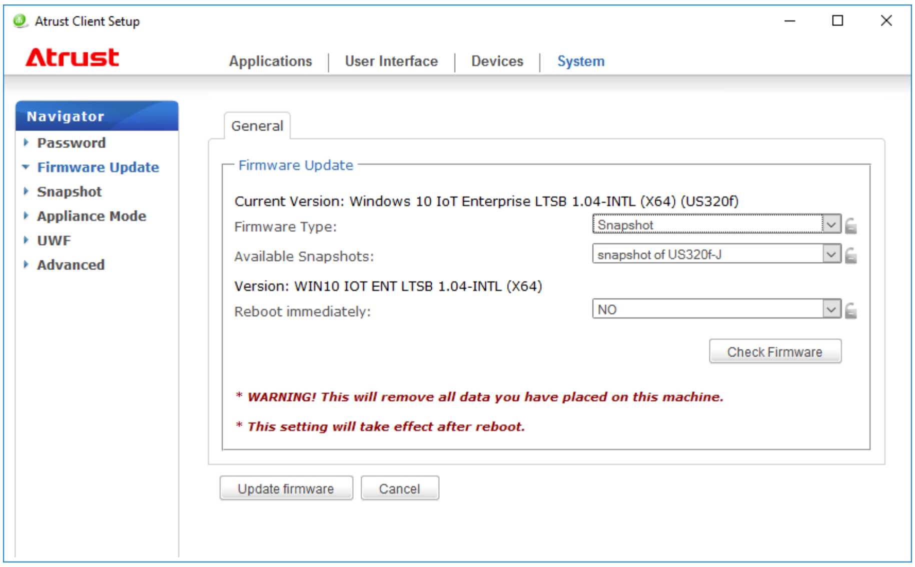


The page at http://localhost:10080 says:

List Loading Completed!

Note Use Atrust Device Manager to manage client snapshots saved on the remote computer. For how to manage client snapshots on Atrust Device Manager, see Atrust Device Manager User's Guide.

4. Select a snapshot and other options from the drop-down list.



Current Version: Windows 10 IoT Enterprise LTSB 1.04-INTL (X64) (US320f)

Firmware Type: Snapshot

Available Snapshots: snapshot of US320f-J

Version: WIN10 IOT ENT LTSB 1.04-INTL (X64)

Reboot immediately: NO

* *WARNING! This will remove all data you have placed on this machine.*

* *This setting will take effect after reboot.*

Snapshot deployment options

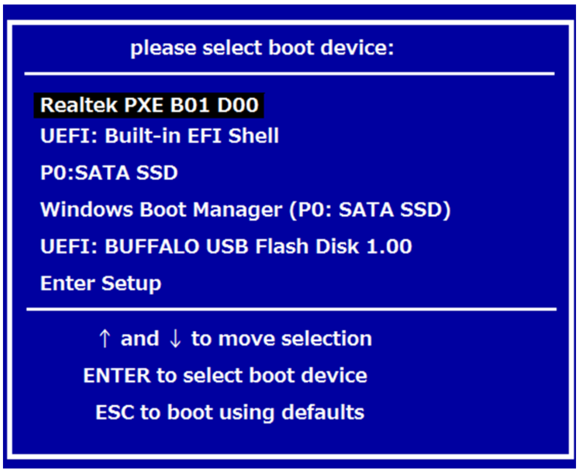
Item	Description
Available Snapshots	Select a snapshot from the snapshot list.
Reboot immediately	Select whether to immediately restart the system or to manually restart the system later to update firmware.

5. Click **Update firmware** to confirm your selections. Snapshot deployment starts after the system restarts.

2.7.2 Deploying a Snapshot System Image from a USB Flash Memory

To deploy a system image to US320f by using a snapshot in the USB flash memory, do the following:

1. Insert the USB flash memory into an empty USB port on the client.
2. Start or restart the client.
3. Press the <F7> key on the keyboard during POST (Power-On Self-Test) to open the **Boot Device** menu.

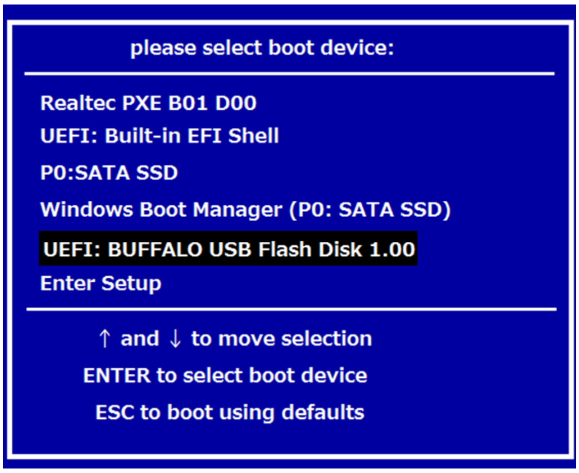


please select boot device:

Realtek PXE B01 D00
UEFI: Built-in EFI Shell
P0:SATA SSD
Windows Boot Manager (P0: SATA SSD)
UEFI: BUFFALO USB Flash Disk 1.00
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

4. Select to boot from the connected <USB flash memory>.

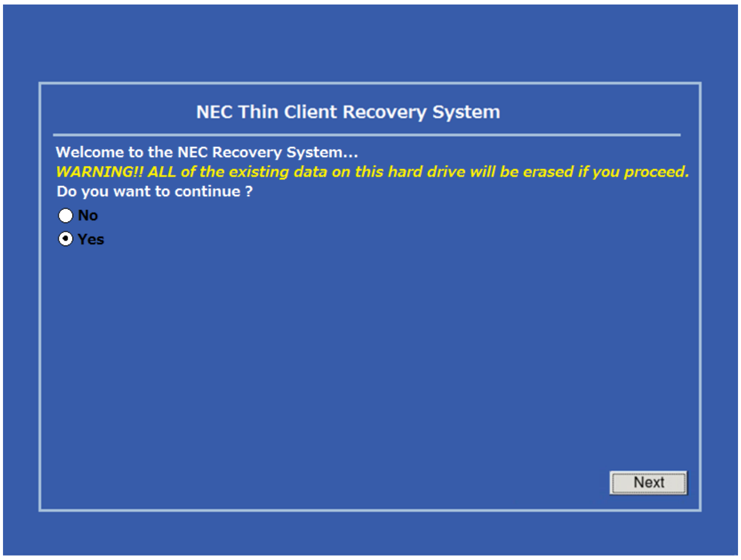


please select boot device:

Realtec PXE B01 D00
UEFI: Built-in EFI Shell
P0:SATA SSD
Windows Boot Manager (P0: SATA SSD)
UEFI: BUFFALO USB Flash Disk 1.00
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

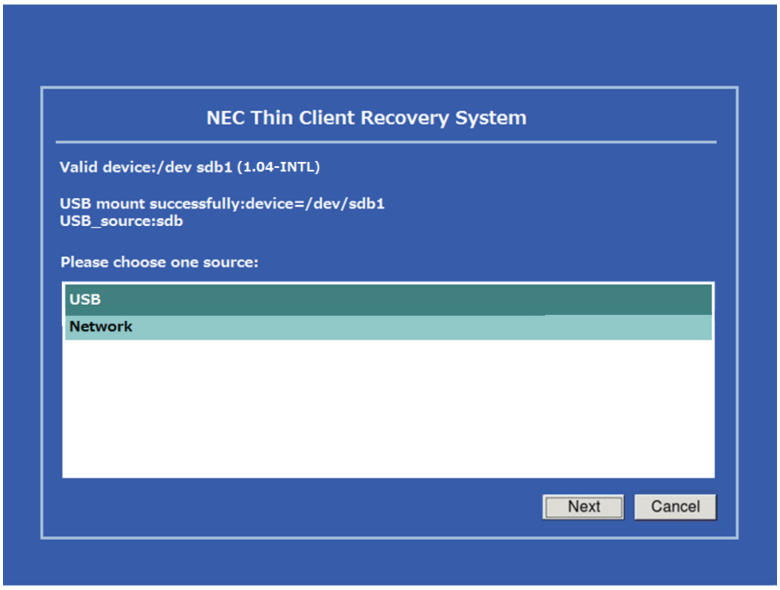
5. Select **Yes** and click **Next**.



NEC Thin Client Recovery System

Welcome to the NEC Recovery System...
WARNING!! ALL of the existing data on this hard drive will be erased if you proceed.
Do you want to continue ?
○ No
● Yes

6. Select **USB** and click **Next**.



NEC Thin Client Recovery System

Valid device:/dev sdb1 (1.04-INTL)

USB mount successfully:device=/dev/sdb1
USB_source:sdb

Please choose one source:

7. The recovery system starts deploying the snapshot to the client.

8. When the process is completed, click **Finish** to restart the client.

2.8 Enabling or Disabling the Appliance Mode

In the Appliance mode, the thin client directly starts up with the Microsoft remote desktop, Citrix ICA, VMware View, or Horizon session launched. After exiting a session, the client will be turned off.

Note

There are two modes for your thin client:

No.	Mode	Description
1	Appliance	The client will automatically start up with the RDP / ICA / View session launched and is shut down after the session ends.
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 Autostart mode, see sections:

- Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"
- Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"
- Chapter 4, "5.11 Configuring Advanced View Connection Settings"

2.8.1 Enabling the Appliance Mode

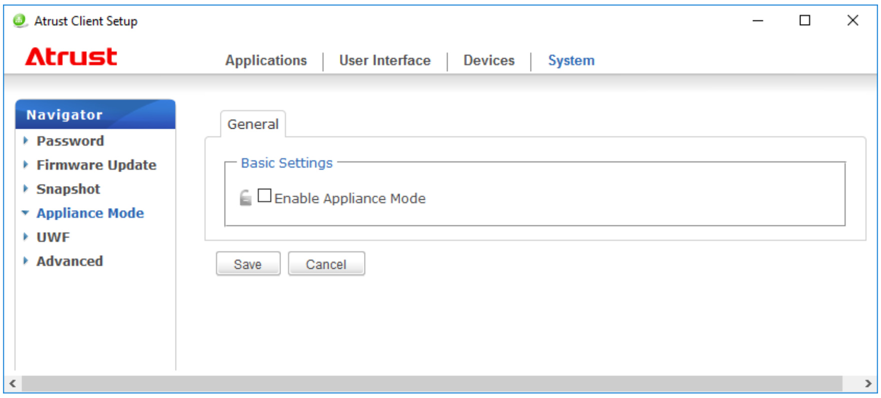
To enable the Appliance mode, do the following:

Note

Ensure that you have configured the connection settings for the desired Microsoft Remote Desktop, Citrix ICA, VMware View, or Horizon 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, see sections:

- Chapter 4, "5.3 Configuring Basic RDP Connection Settings"
- Chapter 4, "5.6 Configuring Basic ICA Connection Settings"
- Chapter 4, "5.9 Configuring Basic VMware Horizon Connection Settings"

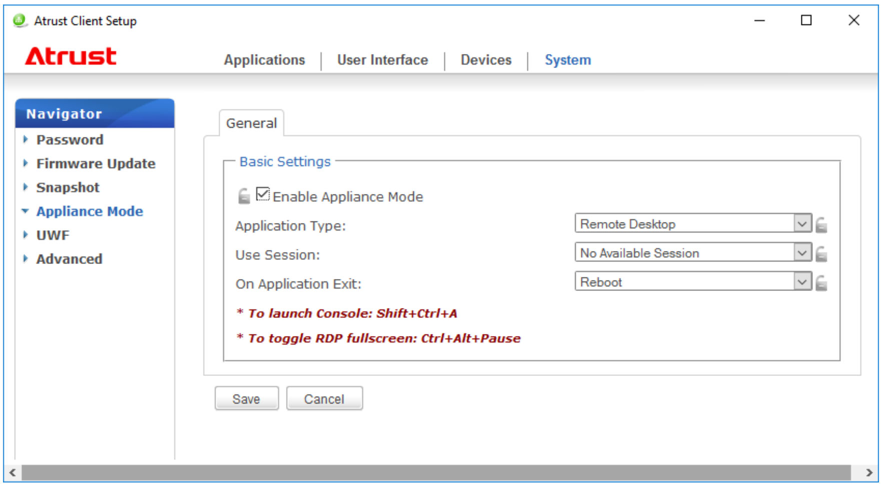
1. On Atrust Client Setup, click **System** > **Appliance Mode**.



□ Enable Appliance Mode

2. Click to check **Enable Appliance Mode**.

3. Other settings of the Appliance mode appear.



☑ Enable Appliance Mode

Application Type: Remote Desktop

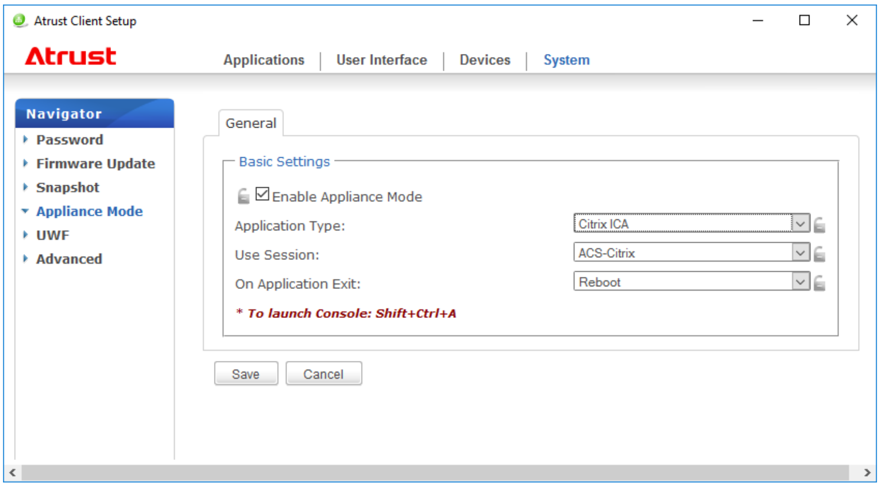
Use Session: No Available Session

On Application Exit: Reboot

* To launch Console: Shift+Ctrl+A

* To toggle RDP fullscreen: Ctrl+Alt+Pause

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.



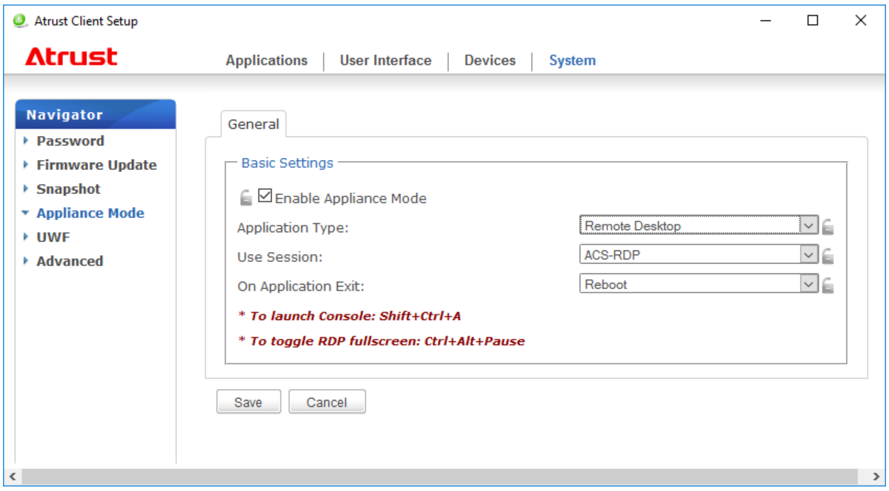
☑ Enable Appliance Mode

Application Type: Citrix ICA

Use Session: ACS-Citrix

On Application Exit: Reboot

* To launch Console: Shift+Ctrl+A



☑ Enable Appliance Mode

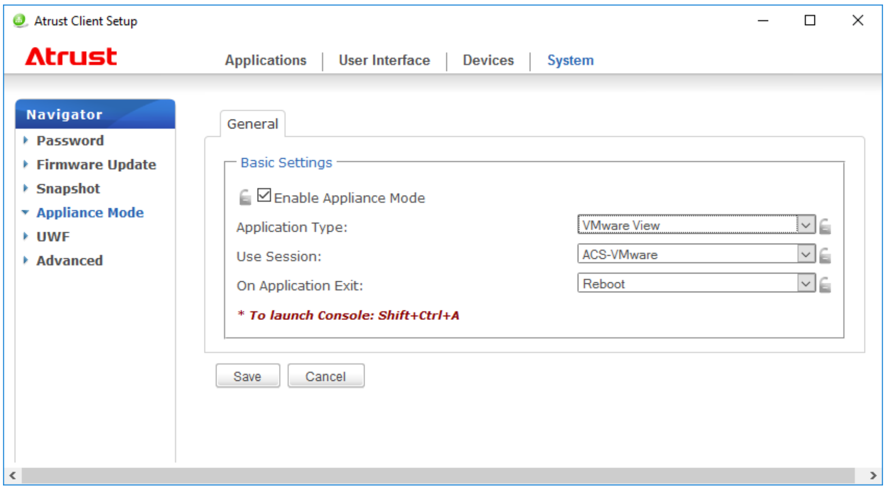
Application Type: Remote Desktop

Use Session: ACS-RDP

On Application Exit: Reboot

* To launch Console: Shift+Ctrl+A

* To toggle RDP fullscreen: Ctrl+Alt+Pause



☑ Enable Appliance Mode

Application Type: VMware View

Use Session: ACS-VMware

On Application Exit: Reboot

* To launch Console: Shift+Ctrl+A

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, see Chapter 4, "2.8.2 Disabling the Appliance Mode".

2.8.2 Disabling the Appliance Mode

To disable the Appliance mode, do the following:

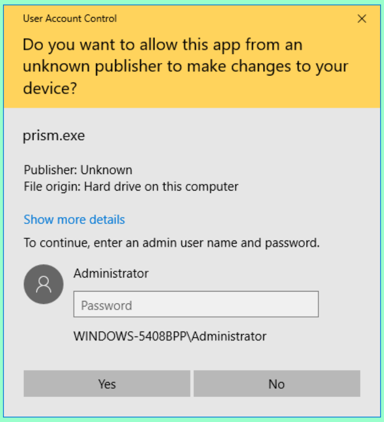
1. In the Appliance mode, exit the Full Screen mode of the RDP / ICA session, or release the keyboard and mouse from the View session (virtual desktop).

   - 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. (Note that you may not be in the Full Screen mode.)
   - To release the keyboard and mouse from the View session (virtual desktop), press Ctrl + Alt.

   Note Note that the View session (virtual desktop) will remain in the background after you release the keyboard and mouse from the View session (virtual desktop).

2. Click Shift +Ctrl + A to launch Atrust Client Setup.

   Note
   - You cannot access the Taskbar of the client operating system in the Appliance mode.
   - When you are using the standard user account, the User Account Control screen appears by default. You must enter the administrator's password to launch Atrust Client Setup.



User Account Control

Do you want to allow this app from an unknown publisher to make changes to your device?

prism.exe

Publisher: Unknown
File origin: Hard drive on this computer

Show more details

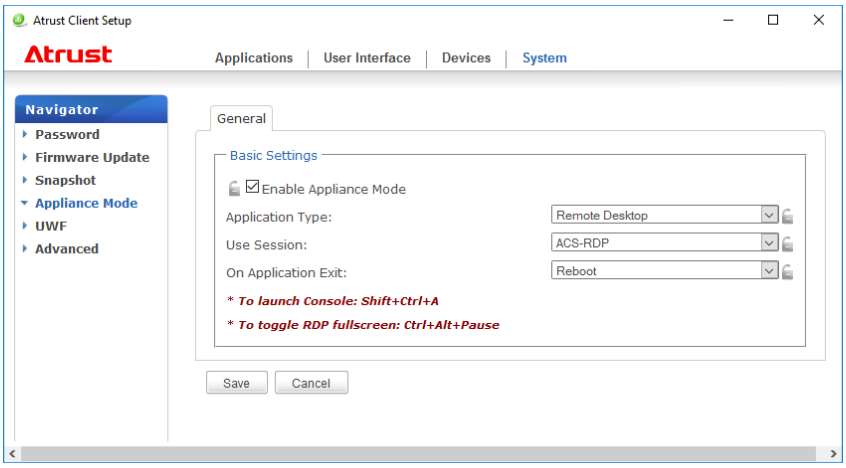
To continue, enter an admin user name and password.

Administrator

Password

WINDOWS-5408BPP\Administrator

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



Atrust Client Setup

Basic Settings

☑ Enable Appliance Mode

Application Type: Remote Desktop

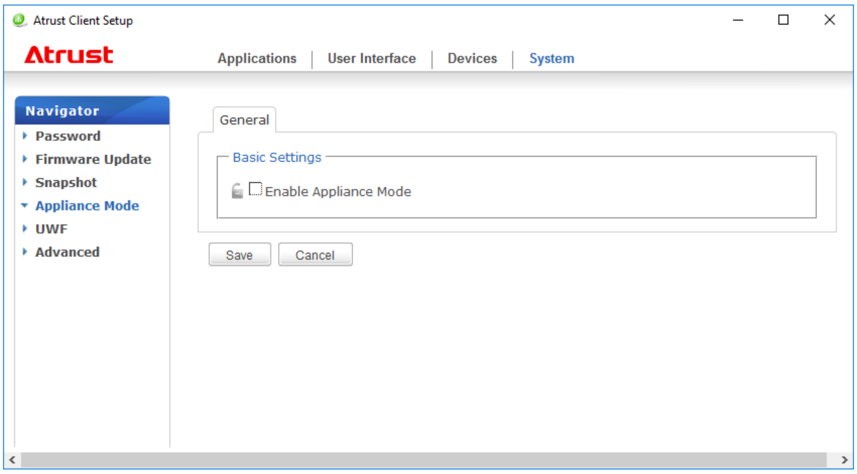
Use Session: ACS-RDP

On Application Exit: Reboot

* *To launch Console: Shift+Ctrl+A*

* *To toggle RDP fullscreen: Ctrl+Alt+Pause*

4. Clear the **Enable Appliance Mode** check box, and then click **Save** to apply the change.



Atrust Client Setup

Atrust

Applications | User Interface | Devices | System

Navigator
- Password
- Firmware Update
- Snapshot
- Appliance Mode
- UWF
- Advanced

General

Basic Settings

□ Enable Appliance Mode

Save Cancel

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 on the View session (virtual desktop) in the background.

6. Sign out from the current RDP / ICA / View session.
7. When you sign out from the session, the client will automatically shut down.
8. Next time, the system starts up with the Appliance mode disabled.

2.9 Configuring UWF (Unified Write Filter)

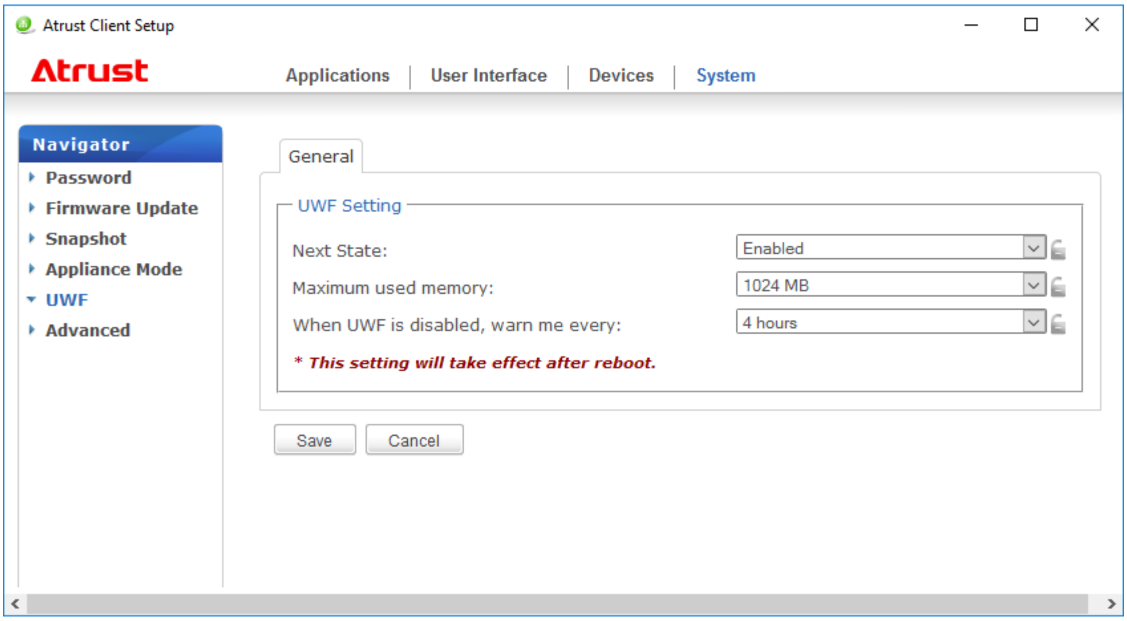
Your US320f is UWF-enabled by default. Unified Write Filter (UWF) is a sector-based write filter intercepting all write attempts to a protected volume and redirecting those write attempts to a RAM cache. With UWF, all system changes will only affect the session where the changes are made. After restart, all changes will be discarded.

Important

- **The UWF function is enabled by default at shipment. Changes made during the session except for changes to Atrust Client Setup settings are discarded after the system restarts. To retain changes to system settings and other data after restart, check that UWF is set to retain changes before changing settings.**
- **The icon in the Notification area of the Taskbar indicates the current UWF status of the system. For details, see the description later in this section.**

To configure the UWF settings, do the following:

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



Next State: Enabled

Maximum used memory: 1024 MB

When UWF is disabled, warn me every: 4 hours

* *This setting will take effect after reboot.*

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.

Important

- **The maximum memory used recommends 1024MB of default value.**
- **There is a possibility that cash of UWF overlays is used by various factors, and when cash exceeds the maximum memory used, there is a fear that the system becomes unstable.**

4. Click **Save** to confirm your selections.

5. You may need to restart the system for the change(s) to take effect.

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.

Important

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.

Note

As a thin client device, your US320f is mainly for access to remote or virtual desktops on servers. Because the hard disk space is limited and protected (UWF-enabled), it is *not* recommended to save data on your US320f. Instead, you can use storage space on remote or virtual desktops, removable storage devices, or networks.

2.10 Enabling / Disabling Automatic Registration and Stealth Mode

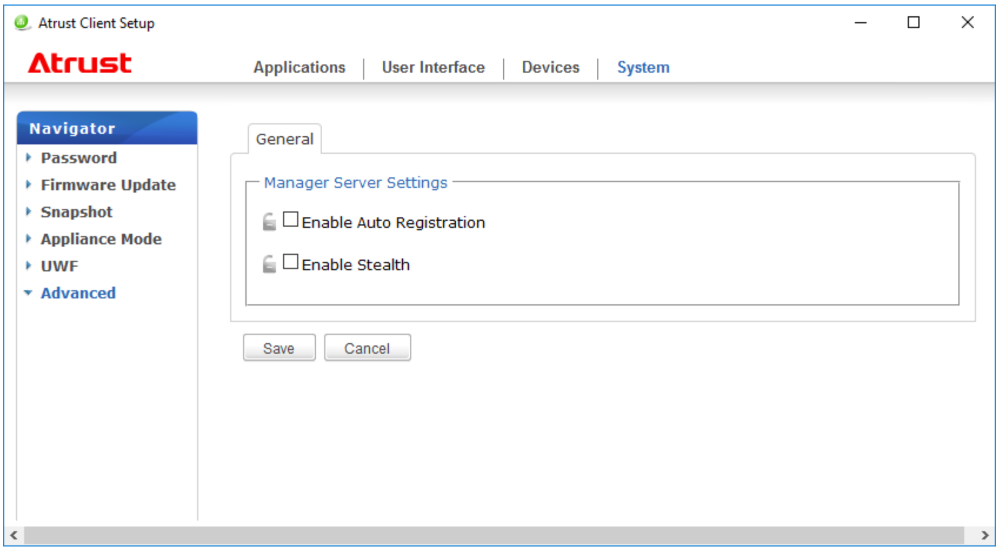
By activating the automatic registration function, US320f can automatically register initial registration to Atrust Device Manager. Also, by enabling the stealth mode, it is possible to prevent US320f from being detected by IP range from Atrust Device Manager.

Important

- **To use the automatic registration function, the setting on the Atrust Device Manager server side must be valid.**
- **It is recommended to enable stealth mode, if you do not manage terminal with Atrust Device Manager.**

The procedure for specifying automatic registration is as follows.

1. Click **System** > **Advanced** on the Atrust Client Setup screen.

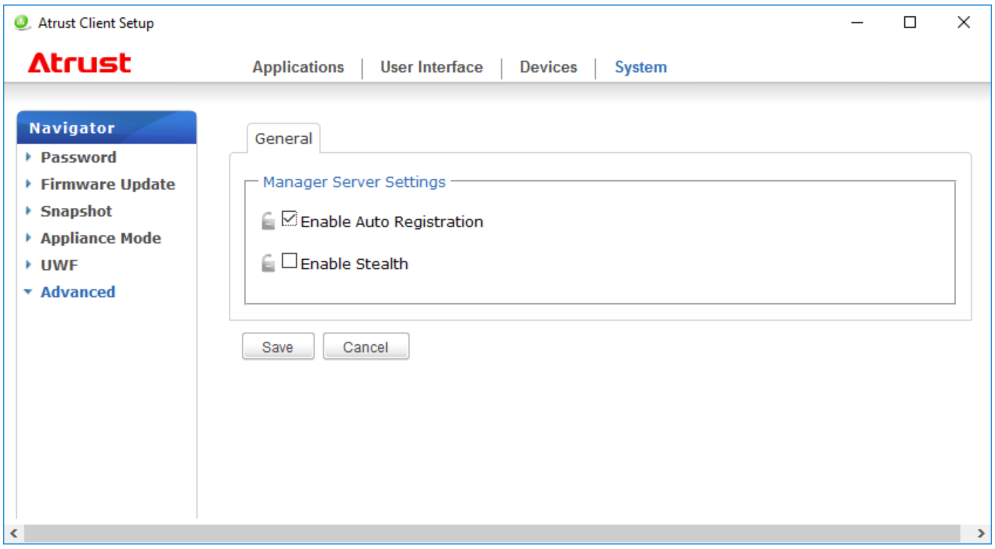


Manager Server Settings

☐ Enable Auto Registration

☐ Enable Stealth

2. Select the **Enable Auto Registration** checkbox.



Manager Server Settings

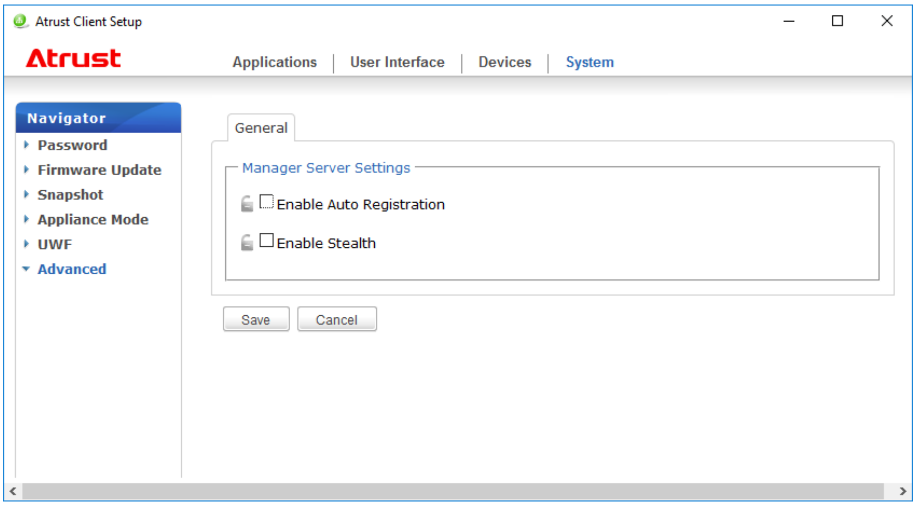
☑ Enable Auto Registration

☐ Enable Stealth

3. Click **Save** to confirm the selection.

The procedure for specifying the stealth mode is as follows.

1. Click **System** > **Advanced** on the Atrust Client Setup screen.

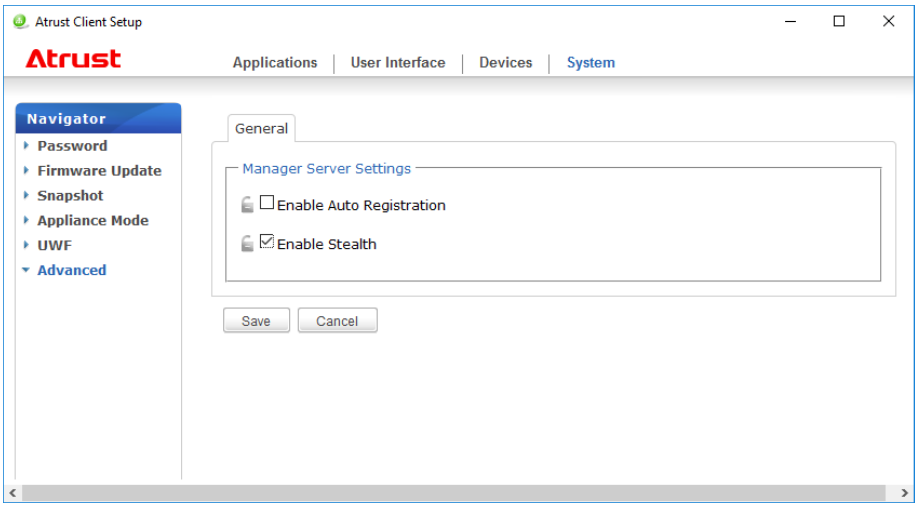


Manager Server Settings

□ Enable Auto Registration

□ Enable Stealth

2. Select the **Enable Stealth** checkbox.



Manager Server Settings

□ Enable Auto Registration

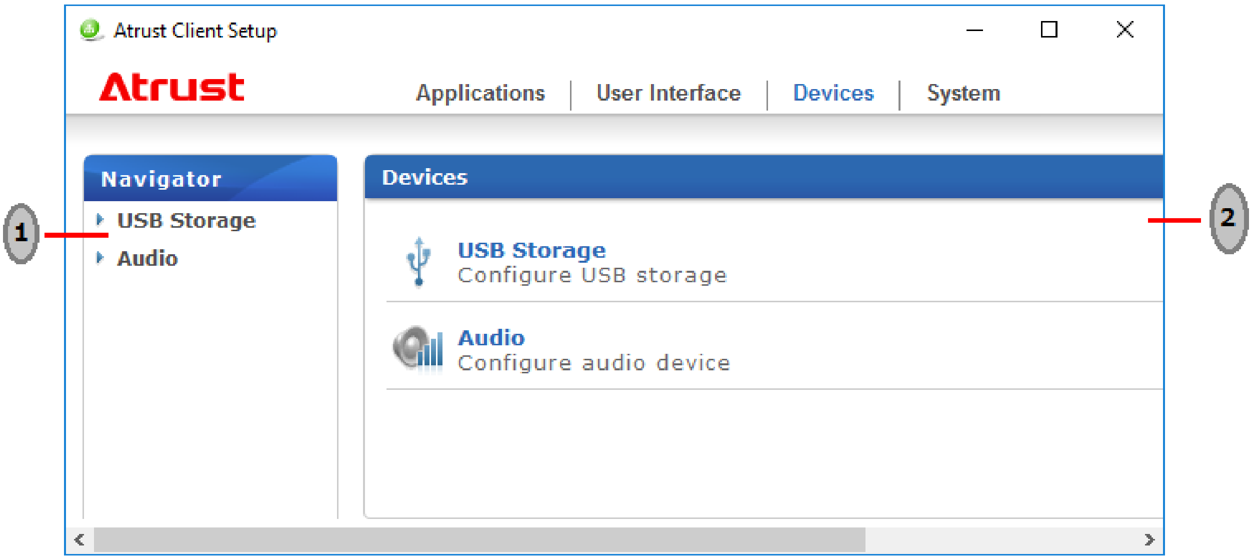
☑ Enable Stealth

3. Click **Save** to confirm the selection.

3. Configuring External Device Settings

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.



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

3.2 Available Settings

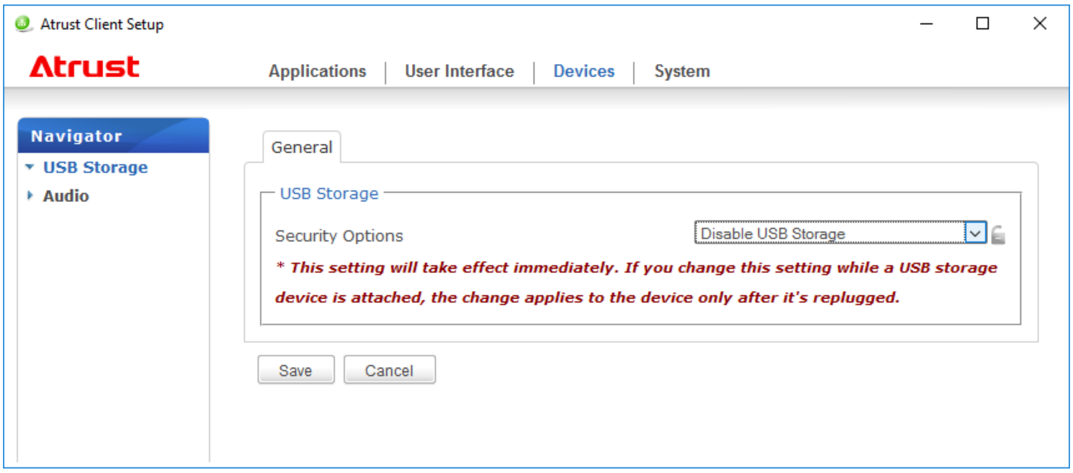
Available settings are shown below:

Tab	Setting	Icon	Description	Section page
Devices	USB Storage		Click to configure settings for USB storage devices.	Chapter 4, "3.3 Configuring Settings for USB Storage Devices".
	Audio		Click to configure settings for audio devices.	Chapter 4, "3.4 Disabling or Enabling Attached Audio Devices".

3.3 Configuring Settings for USB Storage Devices

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

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



Security Options: Disable USB Storage

* This setting will take effect immediately. If you change this setting while a USB storage device is attached, the change applies to the device only after it's replugged.

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

By selecting **Enable USB Storage**, you can map a USB storage device in a remote / virtual desktop session. To map a USB storage device to a virtual desktop session, you must properly configure optional settings for RDP / ICA connection entries on the **Applications** tab. For details, see each of the following sections:

- Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"
- Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"

Important

- **Even after selecting 'Deactive USB Storage', connections to USB FDD, the USB DVD Multi-Drive and the MTP Device will not become inactive**
- **Even if you select Disable USB Storage, the user can use a locally connected USB storage device through redirection in a Citrix ICA and VMware View / Horizon session. To completely prevent USB storage devices from being used in a virtual desktop session, setup in the Citrix and VMware service delivery environment is required.**

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

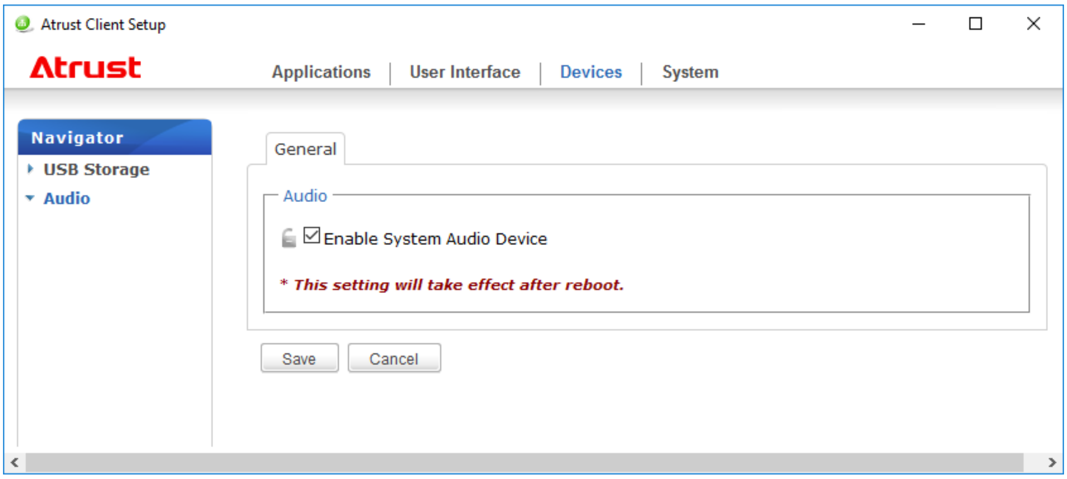
3.4 Disabling or Enabling Attached Audio Devices

To disable/enable attached audio devices, 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, see sections:
  - Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"
  - Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"
  - Chapter 4, "5.11 Configuring Advanced View Connection Settings"

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



Audio

☑ Enable System Audio Device

* This setting will take effect after reboot.

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

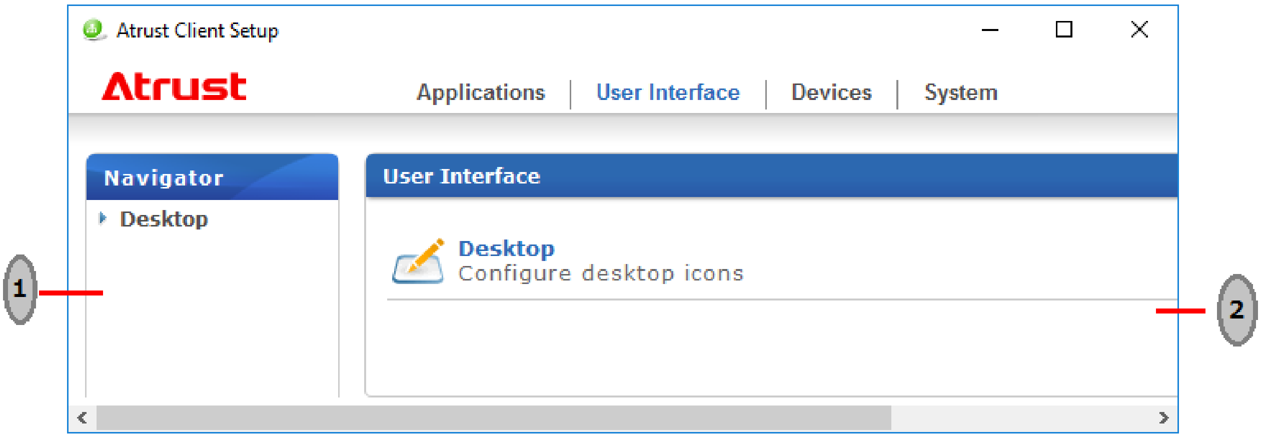
Note

The change will take effect after the client has been restarted.

4. Configuring User Interface Settings

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.



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.

4.2 Available Settings

Tab	Setting	Icon	Description	Section Page
User Interface	Desktop		Click to configure the display of standard desktop shortcuts for quick service access.	Chapter 4, "4.3 Configuring the Display of Standard Desktop Shortcuts for Quick Access".

4.3 Configuring the Display of Standard Desktop Shortcuts for Quick Access

With the **Desktop** setting, you can choose to display or hide standard desktop shortcuts to easily access services. The standard desktop shortcuts are **Remote Desktop Connection**, **Remote Desktop Connection (Span mode)**, **Citrix Receiver**, and **VMware Horizon View Client**. These shortcuts can be used to easily access each service in Citrix XenApp / XenDesktop / VDI-in-a-Box, Microsoft remote desktop / remote application (RemoteApp), and VMware View / VMware Horizon.

Remote Desktop Connection

Remote Desktop Connection (Span mode)

Citrix Receiver

VMware Horizon View Client

Tip

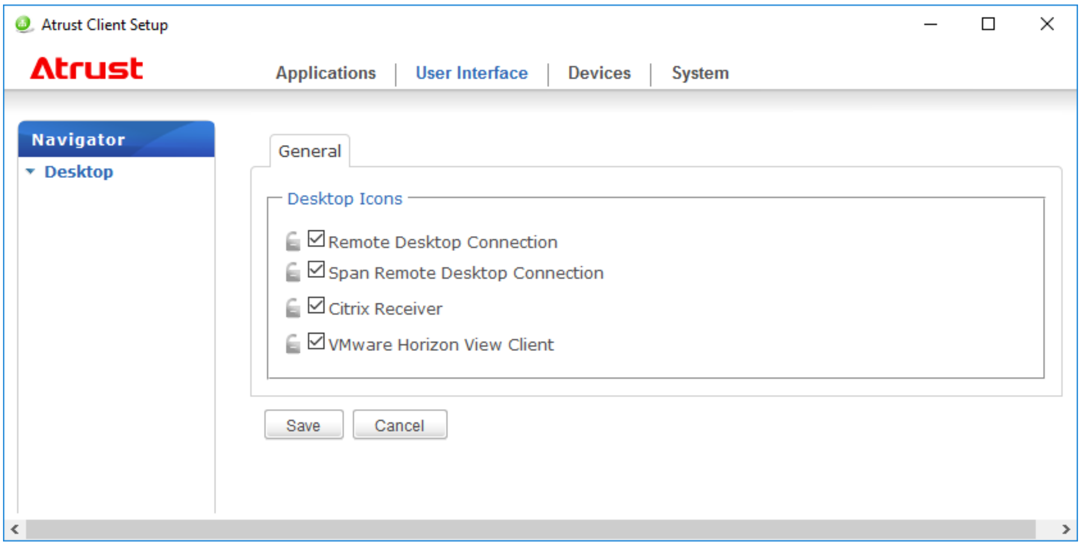
You can use these standard desktop shortcuts to quickly access services. For detailed instructions, see Chapter 3, "1. Standard Shortcuts".

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, see Chapter 4, "5. Configuring Service Access Settings".

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

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



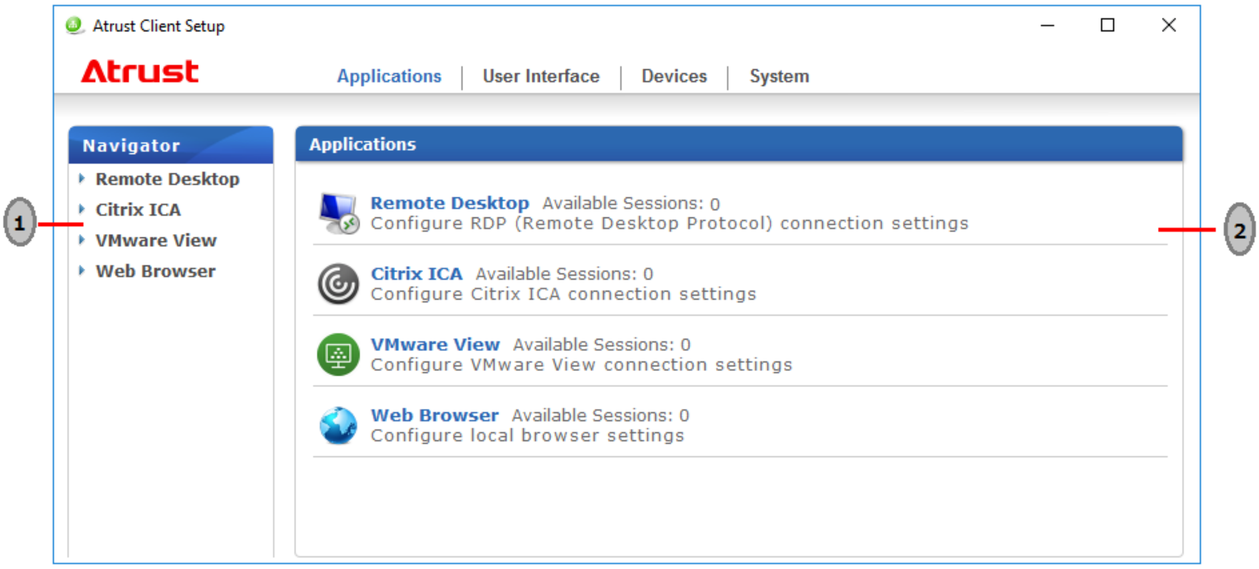
☑ Remote Desktop Connection
☑ Span Remote Desktop Connection
☑ Citrix Receiver
☑ VMware Horizon View Client

2. Select or clear the **Remote Desktop Connection**, **Span Remote Desktop Connection**, **Citrix Receiver**, and **VMware Horizon View Client** check boxes as appropriate.
3. Click **Save** to apply.

5. Configuring Service Access Settings

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.



Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

Web Browser Available Sessions: 0
Configure local browser settings

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.

5.2 Available Settings

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.	• Chapter 4, "5.3 Configuring Basic RDP Connection Settings" • Chapter 4, "5.4 Accessing Remote Desktop Services" • Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"
	Citrix ICA	◎	Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create access shortcuts on the desktop for ICA sessions.	• Chapter 4, "5.6 Configuring Basic ICA Connection Settings" • Chapter 4, "5.7 Accessing Citrix Services" • Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"
	VMware View	🖥	Click to configure VMware View connection settings and create access shortcuts on the desktop for View sessions.	• Chapter 4, "5.9 Configuring Basic VMware Horizon Connection Settings" • Chapter 4, "5.10 Accessing VMware View or Horizon Services" • Chapter 4, "5.11 Configuring Advanced View Connection Settings"
	Web Browser	🌐	Click to configure browser session settings and create access shortcuts on the desktop for browser sessions.	• Chapter 4, "5.12 Configuring Web Browser Settings"

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, visit Microsoft website at www.microsoft.com.

Three connection types are available:

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

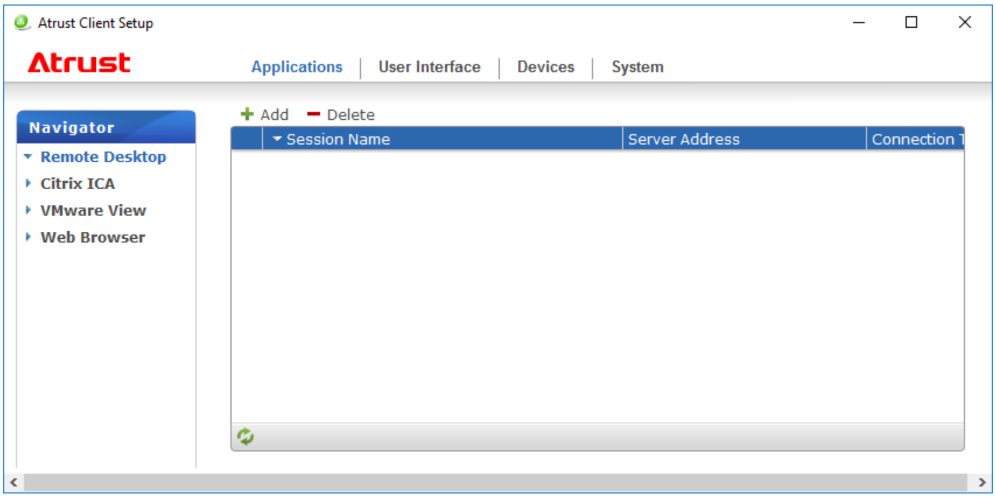
5.3.1 Connection Type: Remote Desktop

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

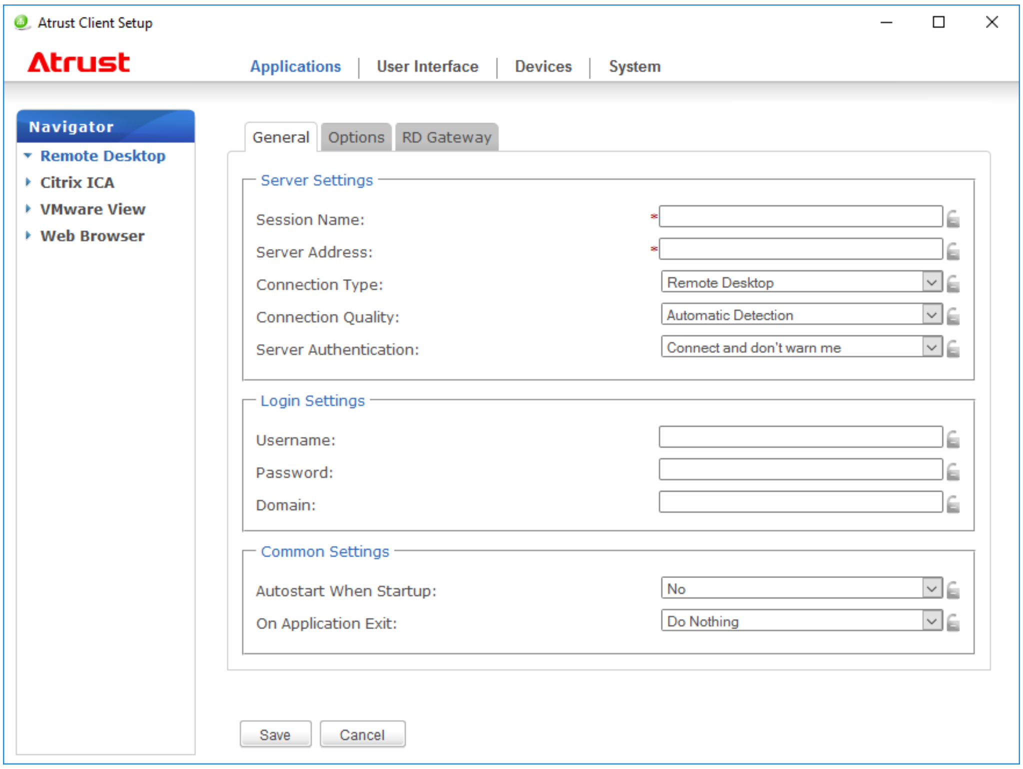
1. On Atrust Client Setup, click **Applications** > **Remote Desktop**.
2. The RDP Connection list appears in the Configuration area.

Note If you have not created any entry, the RDP Connection list will be empty.

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



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



Server Settings

Session Name: *

Server Address: *

Connection Type: Remote Desktop

Connection Quality: Automatic Detection

Server Authentication: Connect and don't warn me

Login Settings

Username:

Password:

Domain:

Common Settings

Autostart When Startup: No

On Application Exit: Do Nothing

Note

- The red asterisks indicate the required fields.
- The remote computer can be a physical server or a virtual machine. 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, see Chapter 4, "5.5 Configuring Advanced RDP Connection Settings".

5.3.2 Connection Type: Remote Web Access

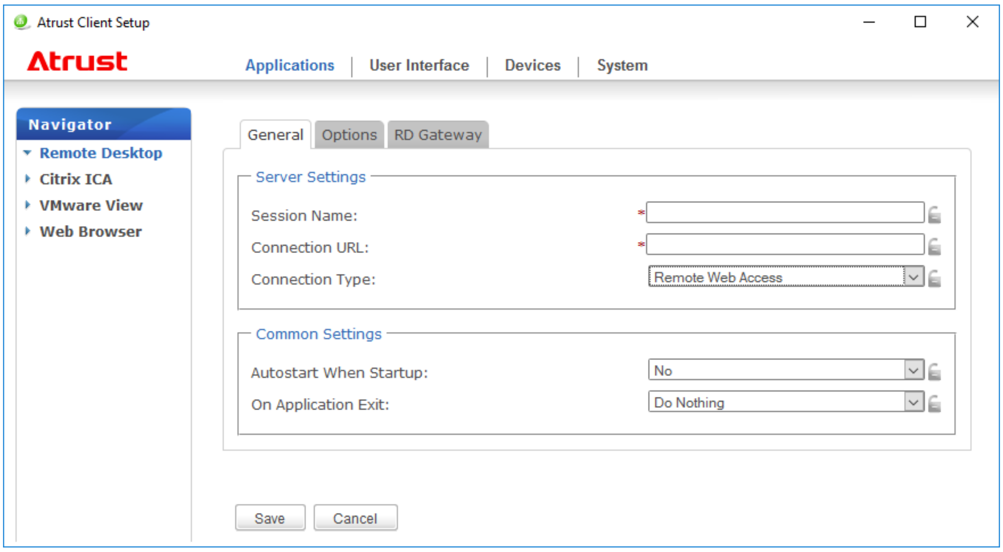
To configure RDP connection settings for Remote Web Access connection type, do the following:

Note Your US320f supports only RD Web Access based on Windows Server 2016 or 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 have not created any entry, the RDP Connection list will be empty.

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



Session Name: *

Connection URL: *

Connection Type: Remote Web Access

Autostart When Startup: No

On Application Exit: Do Nothing

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 system 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, see Chapter 4, "5.5 Configuring Advanced RDP Connection Settings".

5.3.3 Connection Type: Web Feed

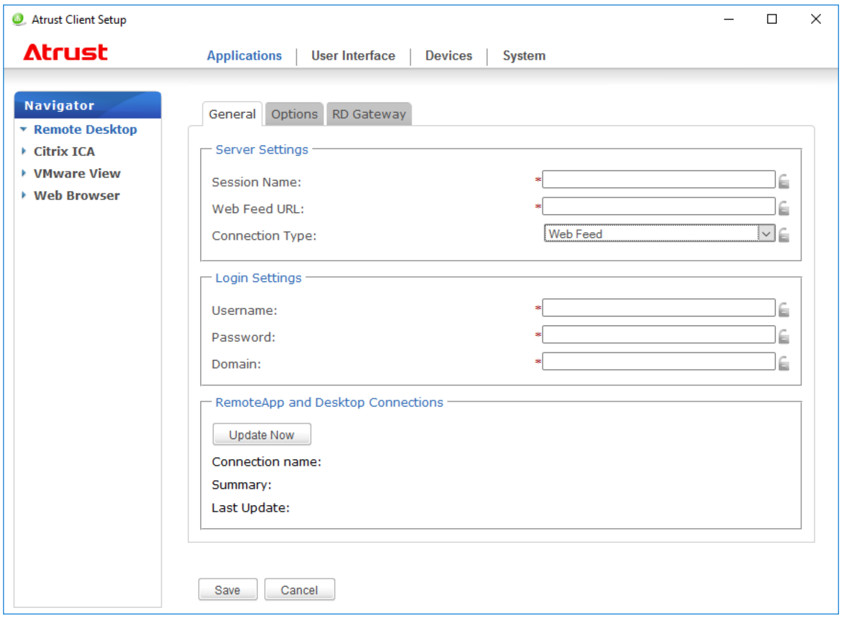
To configure RDP connection settings for Web Feed connection type, do the following:

Note Your US320f supports only RD Web Access based on Windows Server 2016 or 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 have not created any entry, the RDP Connection list will be empty.

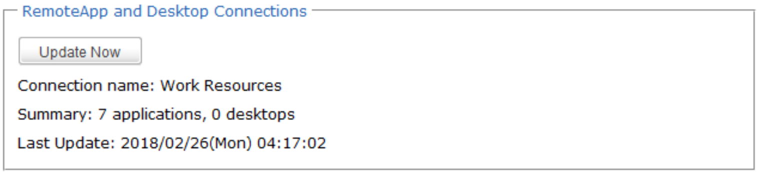
3. Click **Add** on the top of the RDP Connection list to create a new entry of RDP connection.
4. On **General** sub-tab, click the Connection Type drop-down menu to select **Web Feed**.



5. Type in the session name, 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 system administrator about the appropriate Web Feed URL.

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



Connection name: Work Resources
Summary: 7 applications, 0 desktops
Last Update: 2018/02/26(Mon) 04:17:02

7. Click **Save** to add this RDP connection entry.

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, see Chapter 4, "5.5 Configuring Advanced RDP Connection Settings".

5.4 Accessing Remote Desktop Services

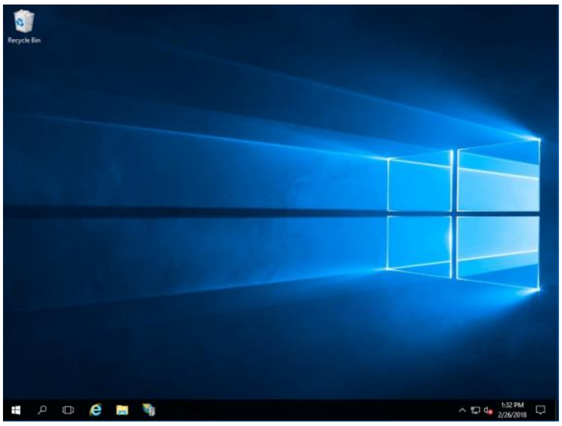
5.4.1 Connection Type: Remote Desktop

To access Remote Desktop services, do the following:

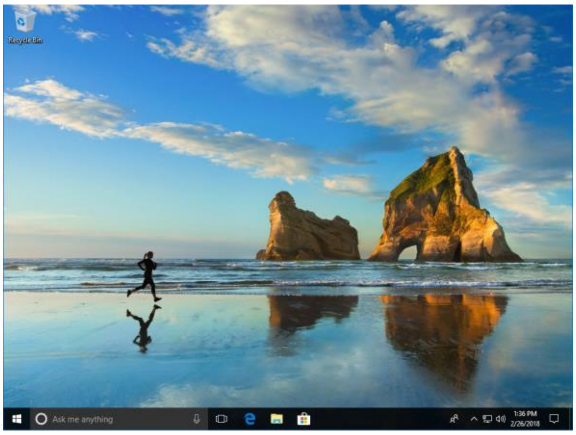
Note You can also access Remote Desktop services through the standard desktop shortcut **Remote Desktop Connection**. For detailed instructions on how to access services via this standard shortcut, see Chapter 3, "3. Accessing Microsoft Remote Desktop Services".

1. Follow the on-screen instructions and provide required credentials if needed.
2. 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, see Chapter 4, "5.5 Configuring Advanced RDP Connection Settings".



Example: Windows Server 2016

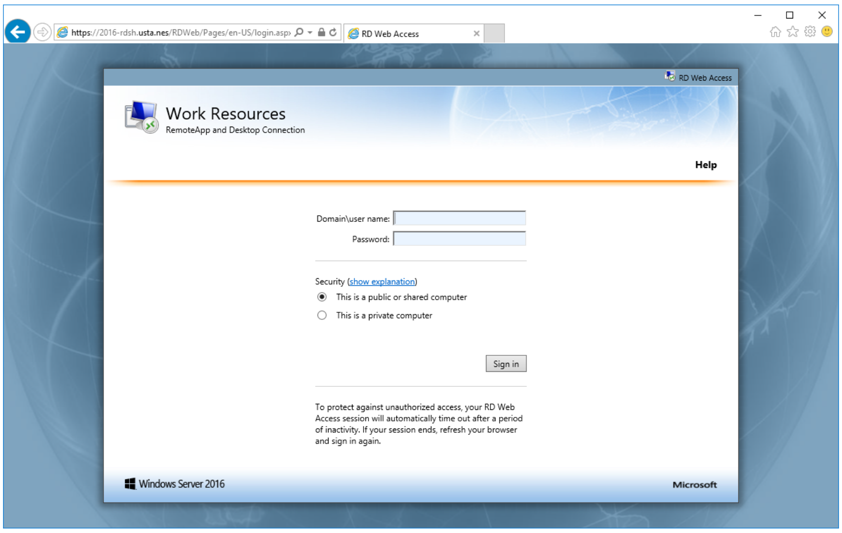


Example: Windows 10 Enterprise

5.4.2 Connection Type: Remote Web Access

To access remote applications/desktops, do the following:

1. Follow the on-screen instructions and provide required credentials if needed.
2. A window appears prompting for credentials.



https://2016-rdsh.usta.nes/RDWeb/Pages/en-US/login.aspx
RD Web Access
RD Web Access
Work Resources
RemoteApp and Desktop Connection
Help

Domain\user name:

Password:

Security (show explanation)

● This is a public or shared computer

○ This is a private computer

Sign in

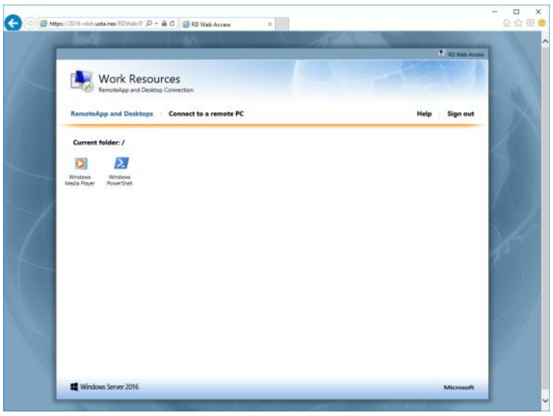
To protect against unauthorized access, your RD Web Access session will automatically time out after a period of inactivity. If your session ends, refresh your browser and sign in again.

Windows Server 2016
Microsoft

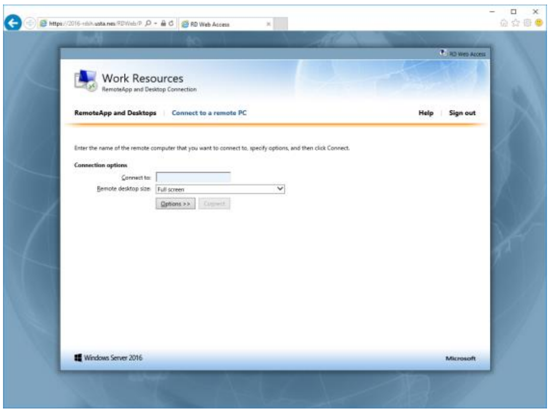
Note

- A warning message about security might appear. Consult your system administrator for details and ensure the connection is secure *first*. To bypass this message, 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**.



Current folder: /



Enter the name of the remote computer that you want to connect to, specify options, and then click Connect.

Connection options

Connect to:

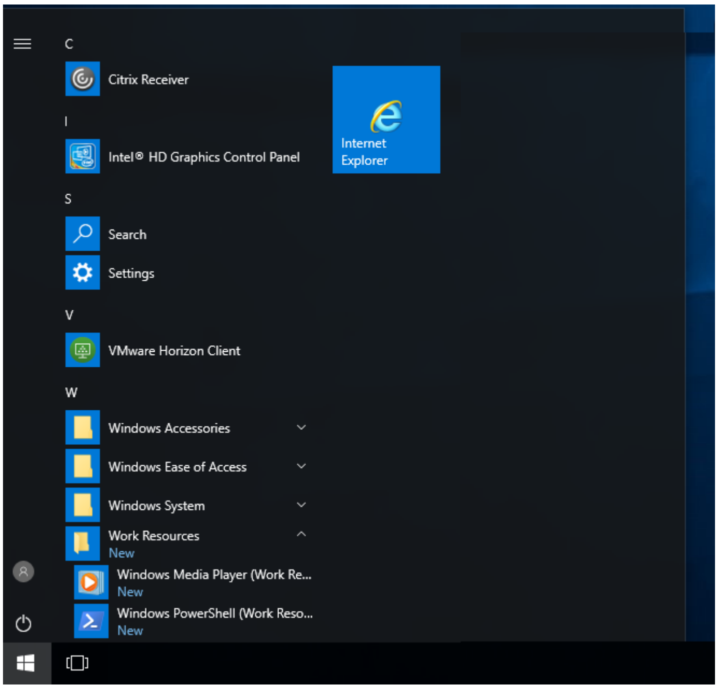
Remote desktop size: Full screen

Options >> Connect

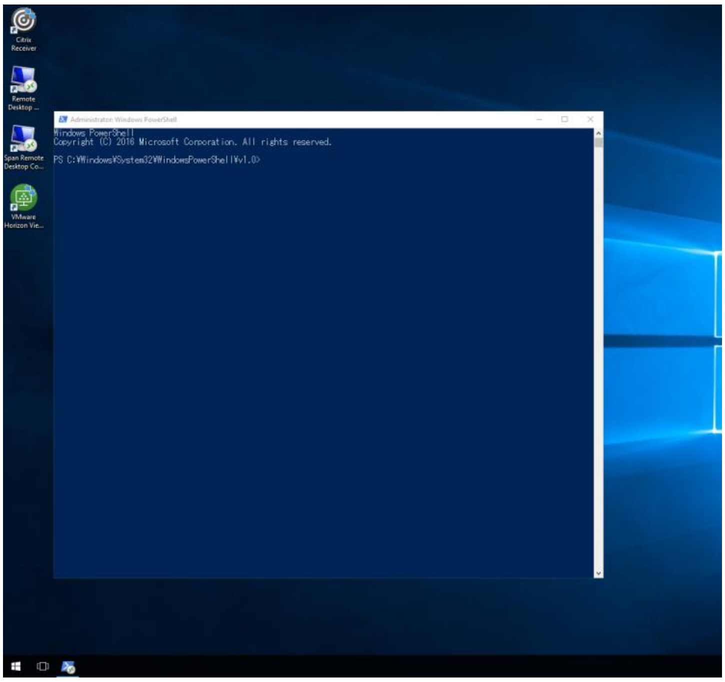
5.4.3 Connection Type: Web Feed

To access remote applications, do the following:

1. Start the application by clicking the **Work Resources (RADC)** folder on the start menu.



2. The applications are opened on the desktop.



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:¥Windows¥System32¥WindowsPowerShell¥v1.0>
```

5.5 Configuring Advanced RDP Connection Settings

The table below provides a description of each setting item for RDP connections. See this table to configure advanced settings and customize your US320f desktop shortcuts or Start screen tiles for service access.

Note Note that available settings vary with the selected connection type.

5.5.1 Settings for the Connection Type of Remote Desktop

Note

- For descriptions of settings for the connection type of Remote Web Access, see Chapter 4, "5.5.2 Settings for the Connection Type of Remote Web Access".
- For descriptions of settings for the connection type of Web Feed, see Chapter 4, "5.5.3 Settings for the Connection Type of Web Feed".

■ General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Remote Desktop sessions.</td></tr>
<tr><td><b>Server Address</b></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><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>Remote Desktop</b> is selected.
Three connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Remote Desktop</b></td><td>Provides access to remote desktops/applications.</td></tr>
<tr><td><b>Remote Web Access</b></td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr>
<tr><td><b>Web Feed</b></td><td>Provides access to remote applications through published Start screen tiles.</td></tr>
</table></td></tr>
<tr><td><b>Connection Quality</b></td><td>Select the setting that best describes the quality of your network connection.
Four options are available: <b>Very Fast (LAN)</b>, <b>Fast (Broadband)</b>, <b>Slow (Modem)</b>, and <b>Automatic Detection</b></td></tr>
<tr><td><b>Server Authentication</b></td><td>Select what to do next if the client cannot verify the identity of the remote computer. Three options are available: <b>Connect and don't warn me</b>, <b>Warn me</b>, and <b>Do not connect</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Connect and don't warn me</b></td><td>Connects anyway without any warning.</td></tr>
<tr><td><b>Warn me</b></td><td>Warns and allows users to choose whether to connect or not.</td></tr>
<tr><td><b>Do not connect</b></td><td>Disallows the connection.</td></tr>
</table></td></tr>
<tr><th colspan="2">Login Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Username</b></td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td><b>Password</b></td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td><b>Domain</b></td><td>Type in the domain of the server.
<b>NOTE:</b> Leave this field blank if the server doesn't belong to any domain.</td></tr>
</table>

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a Remote Desktop session automatically or not when Windows 10 IoT starts. If <b>Yes</b> is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a Remote Desktop session is ended. Four options are available: <b>Do Nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do Nothing</b></td><td>Does not perform any processing after exiting the session.</td></tr>
<tr><td><b>Restart Application</b></td><td>Opens a Remote Desktop session again.</td></tr>
<tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr>
<tr><td><b>Shutdown</b></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><b>Start the following program on connection</b></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)

<b>NOTE:</b> Remote Application sessions are Remote sessions used to access only specific applications rather than full desktops.
<b>NOTE:</b> 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, visit Microsoft Support website at support.microsoft.com.</td></tr>
<tr><td><b>Start in the following folder</b></td><td>Type in the location of the desired application (on the host server) if <b>Start the following program on connection</b> is enabled.
<b>NOTE:</b> You can type in the location/path of the desired application in this field, and specify only the name of the application in <b>Program path and file name</b> (the next field). Or, you can type in the full path and name of the application in <b>Program path and file name</b>, and leave this field empty.</td></tr>
<tr><td><b>Program path and file name</b></td><td>Type in the path and name of the desired application if <b>Start the following program on connection</b> is enabled.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Windows Media Player</b></td><td>C:\Programs Files (x86)\Windows Media Player\wmplayer.exe</td></tr>
<tr><td><b>Adobe Reader X</b></td><td>C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32</td></tr>
</table>
<b>NOTE:</b> The file extension can be omitted.</td></tr>
</table>

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: **Full Screen**, **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.
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 Embedded-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). **NOTE:** To use a local or network printer in a Remote Desktop session, you need to add the printer to your thin client, then enable **Clipboard Redirection**. **NOTE:** To add a local or network printer to a Windows 10 IoT based thin client, open **Control Panel** and select **Hardware and Sound** > **Devices and Printers** > **Add Printer**, then follow the on-screen instructions.
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.

<table>
<tr><th colspan="2">Local Resources Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Remote Audio Playback</b></td><td>Click the drop-down menu to configure the computer sounds and audio playback setting in a Remote Desktop session. Three options are available: <b>Play on this computer, Do not play,</b> and <b>Play on remote computer</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Play on this computer</b></td><td>Allows computer sounds and audio playback in a Remote Desktop session using locally attached audio devices.</td></tr>
<tr><td><b>Do not play</b></td><td>Disables computer sounds and audio playback in a Remote Desktop session.</td></tr>
<tr><td><b>Play on remote computer</b></td><td>Leave computer sounds and audio playback at the remote computer.</td></tr>
</table></td></tr>
<tr><td><b>Remote Audio Recording</b></td><td>Click the drop-down menu to configure the audio recording setting in a Remote Desktop session. Two options are available: <b>Recording from this computer</b> and <b>Do not record</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Recording from this computer</b></td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr>
<tr><td><b>Do not record</b></td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr>
</table>
<b>NOTE:</b> When <b>Play on remote computer</b> is selected on the drop-down menu of <b>Remote Audio Playback</b>, this setting item will be grayed out.</td></tr>
<tr><td><b>Apply Windows key combinations</b></td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: <b>On this computer</b>, <b>On the remote computer</b>, <b>Only when using the full screen</b>.</td></tr>
<tr><td><b>Drives</b></td><td>Click the drop-down menu to enable/disable locally attached drives in a Remote Desktop session.</td></tr>
<tr><td><b>Supported plug and play devices</b></td><td>Click the drop-down menu to enable/disable the supported plug and play devices in a Remote Desktop session.</td></tr>
<tr><td><b>RemoteFX USB redirection</b></td><td>Click to enable/disable locally attached RemoteFX USB devices.

<b>NOTE:</b> 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, follow the steps below:
1. Sign in to your US320f with an administrative account.
2. Disable UWF (Unified Write Filter).
3. Click Run, type “gpedit.msc” to start Group Policy Editor
4. On the opened window, select <b>Computer Configuration</b> > <b>Administrative Templates</b> > <b>Windows Components</b> > <b>Remote Desktop Services</b> > <b>Remote Desktop Connection Client</b> > <b>RemoteFX USB Device Redirection</b> > <b>Allow RDP redirection of other supported RemoteFX USB devices from this computer</b>.
5. Select <b>Enabled</b> and to which users this setting applies: <b>Administrators Only</b> or <b>Administrators and Users</b>, and then click <b>OK</b>.
6. Enable UWF through Atrust Client Setup.</td></tr>
</table>

■ **RD Gateway Sub-tab**

<table>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>RD Gateway Server Settings</b></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: <b>Automatically detect RD Gateway server settings</b>, <b>Use these RD Gateway server settings</b>, and <b>Do not use an RD Gateway server</b>.</td></tr>
<tr><td><b>Server Name</b></td><td>Type the IP address / URL / FQDN of the RD Gateway server.
<b>NOTE:</b> Consult your network administrator for details.</td></tr>
<tr><td><b>Logon method</b></td><td>Click the drop-down menu to select the logon method. Three options are available: <b>Allow me to select later</b>, <b>Ask for password (NTLM)</b>, and <b>Smart card</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Allow me to select later</b></td><td>Users can select a logon method while connecting to the server.</td></tr>
<tr><td><b>Ask for password (NTLM)</b></td><td>Users will be prompted for a password while connecting to the server.</td></tr>
<tr><td><b>Smart card</b></td><td>Users will be prompted for a smart card while connecting to the server.</td></tr>
</table>
</td></tr>
<tr><td><b>Bypass RD Gateway server for local addresses</b></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>
</table>

Logon Settings	
Item	**Description**
Use my RD Gateway credentials for the remote computer	Check to use the same set of credentials for authenticating to both the RD Gateway server and the remote computer.

5.5.2 Settings for the Connection Type of Remote Web Access

Note

- For descriptions of settings for the connection type of Remote Desktop, see Chapter 4, "5.5.1 Settings for the Connection Type of Remote Desktop".
- For descriptions of settings for the connection type of Web Feed, see Chapter 4, "5.5.3 Settings for the Connection Type of Web Feed".

■ **General Sub-tab**

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Remote Web Access sessions.</td></tr>
<tr><td><b>Connection URL</b></td><td>Type in the connection URL through which RD Web Access is available.</td></tr>
<tr><td><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>Remote Web Access</b> is selected. Three connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Remote Desktop</b></td><td>Does not perform any processing after exiting the session.</td></tr>
<tr><td><b>Remote Web Access</b></td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr>
<tr><td><b>Web Feed</b></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><b>Autostart When Startup</b></td><td>Select whether to open a Remote Desktop session automatically or not when Windows 10 IoT starts.
If <b>Yes</b> is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a Remote Desktop session is ended. Four options are available: <b>Do Nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do Nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr>
<tr><td><b>Restart Application</b></td><td>Opens a Remote Desktop session again.</td></tr>
<tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr>
<tr><td><b>Shutdown</b></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.

5.5.3 Settings for the Connection Type of Web Feed

Note

- For descriptions of settings for the connection type of Remote Desktop, see Chapter 4, "5.5.1 Settings for the Connection Type of Remote Desktop".
- For descriptions of settings for the connection type of Remote Web Access, see Chapter 4, "5.5.2 Settings for the Connection Type of Remote Web Access".

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Web Feed sessions.</td></tr>
<tr><td><b>Web Feed URL</b></td><td>Type in the computer name or IP address of the server/virtual machine where to deliver a Web Feed session.</td></tr>
<tr><td><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>Web Feed</b> is selected. Three connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Remote Desktop</b></td><td>Provides access to remote desktops/applications.</td></tr>
<tr><td><b>Remote Web Access</b></td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr>
<tr><td><b>Web Feed</b></td><td>Provides access to remote applications through published Start screen tiles.</td></tr>
</table>
</td></tr>
<tr><th colspan="2">Login Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Username</b></td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td><b>Password</b></td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td><b>Domain</b></td><td>Type in the domain of the server.
<b>NOTE:</b> Leave this field blank if the server doesn't belong to any domain.</td></tr>
<tr><th colspan="2">RemoteApp and Desktop Connection</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Update Now</b></td><td>Click to fetch and update the published applications list from the server.</td></tr>
</table>

■ Options Sub-tab

Window setting	
Item	**Description**
Color Depth	Select the color depth for the remote desktop session. You can select from **15 Bit**, **16 Bit**, **24 Bit** and **32 Bit**. NOTE: If remote FX is enabled, 32 bits / pixel will be applied no matter what color depth is selected. NOTE: You can set an upper limit on the color depth of Remote Desktop sessions on the host server. In this case, you can not exceed the predefined upper limit regardless of which color depth you choose.
Resolution	Select the display resolution of the remote desktop session. You can select from **Full screen**, **1920 x 1200**, **1920 x 1080**, **1680 x 1050**, **1400 x 1050**, **1440 x 900**, **1280 x 1024**, **1280 x 768**, **1280 x 720**, **1024 x 768**, **800 x 600**, and **640 x 480**.
Multi-monitor	Enable or disable multiple displays for Remote Desktop sessions.Enable or disable multiple displays for Remote Desktop sessions.
Display connection bar when I use the full screen	Select whether to display the connection bar in full screen mode.
Local resource settings	
Item	**Description**

Apply Windows key combinations	Select the Windows key combination assignment destination. You can select from three options: **On this computer, On the remote computer, Only when using the full screen.**
Remote FX USB redirect	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, follow the steps below: 1. Sign in to your US320f with an administrative account. 2. Disable UWF (Unified Write Filter). 3. Click Run, type “gpedit.msc” to start Group Policy Editor 4. 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**. 5. Select **Enabled** and to which users this setting applies: **Administrators Only** or **Administrators and Users**, and then click **OK**. 6. 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.

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.

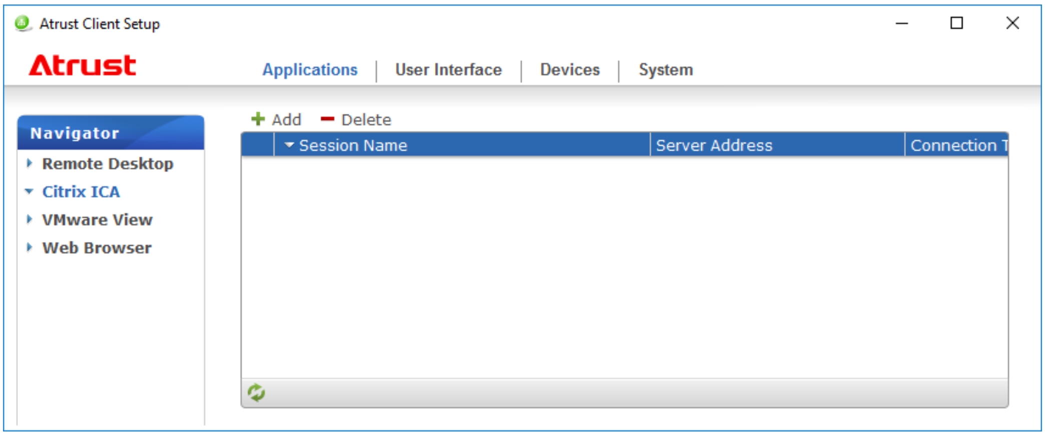
Note

- For more information on Citrix desktop virtualization solutions, visit Citrix website at www.citrix.com or Citrix Knowledge Center at support.citrix.com.
- 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, see Chapter 3, "2. Accessing Citrix Services".
- 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.

5.6.1 Connection Type: Web Logon

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

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

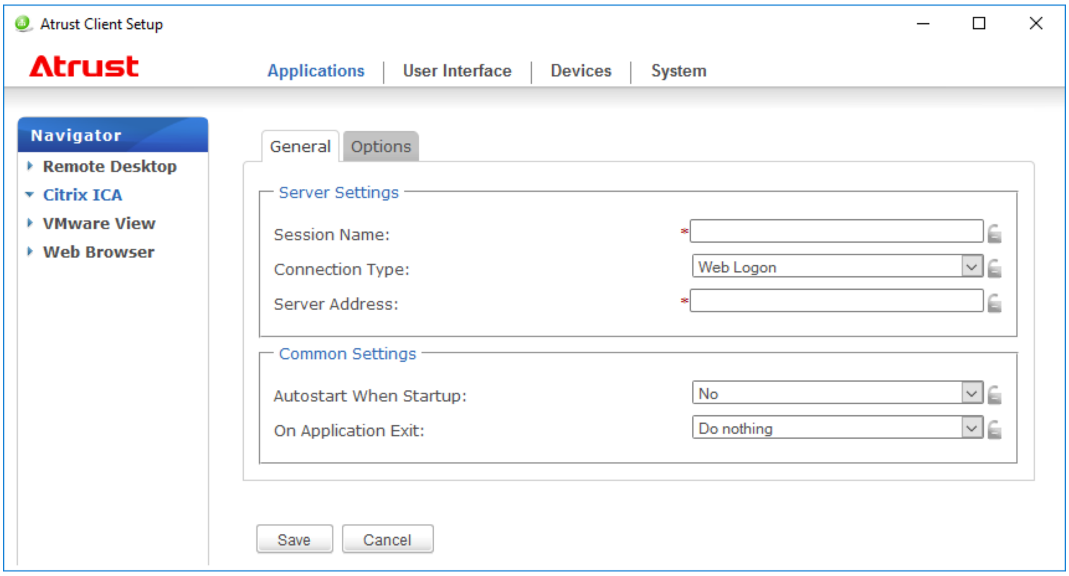


Note

If you have not created any entry, the ICA Connection list will be empty.

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

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



Session Name: *

Connection Type: Web Logon

Server Address: *

Autostart When Startup: No

On Application Exit: Do nothing

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

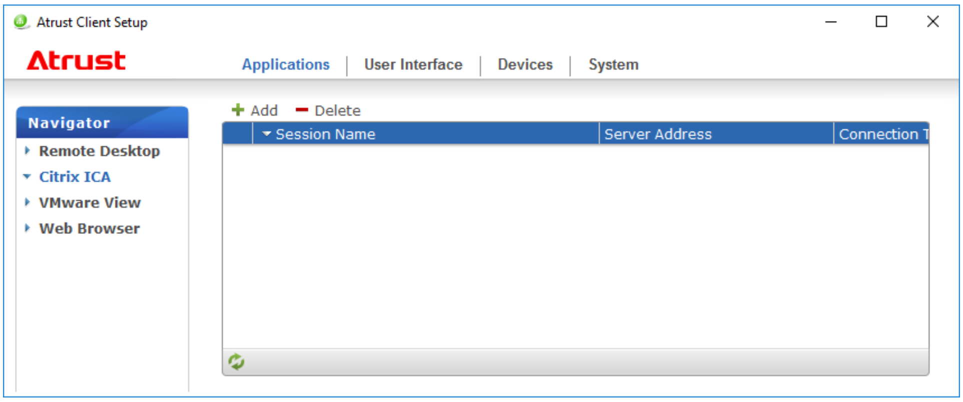
5. Click **Save** to add this ICA connection entry. The access shortcut will be created automatically on the desktop.

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, see Chapter 4, "5.8 Configuring Advanced ICA Connection Settings".

5.6.2 Connection Type: XenDesktop

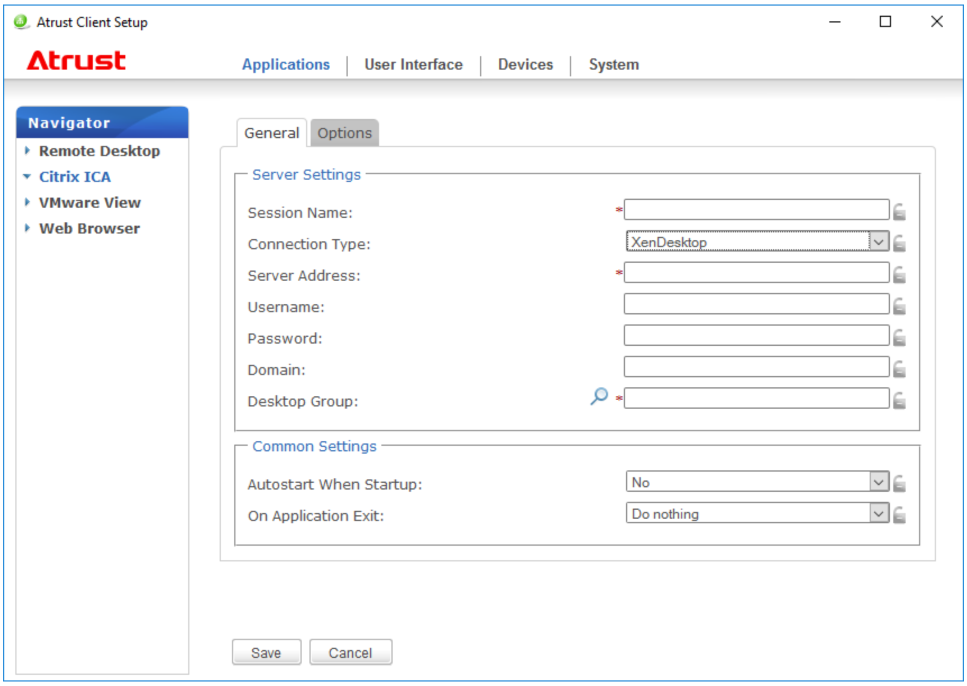
To configure ICA connection settings for the connection type of XenDesktop, do the following:

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



Note If you have not created any entry, the ICA Connection list will be empty.

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



Connection Type: XenDesktop

Autostart When Startup: No

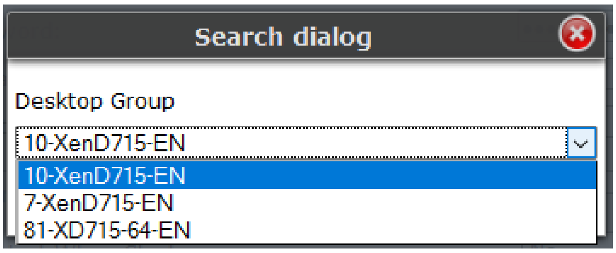
On Application Exit: Do nothing

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 system 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.



Desktop Group

10-XenD715-EN

10-XenD715-EN
7-XenD715-EN
81-XD715-64-EN

7. The selected desktop group name automatically appears in the Desktop Group field.

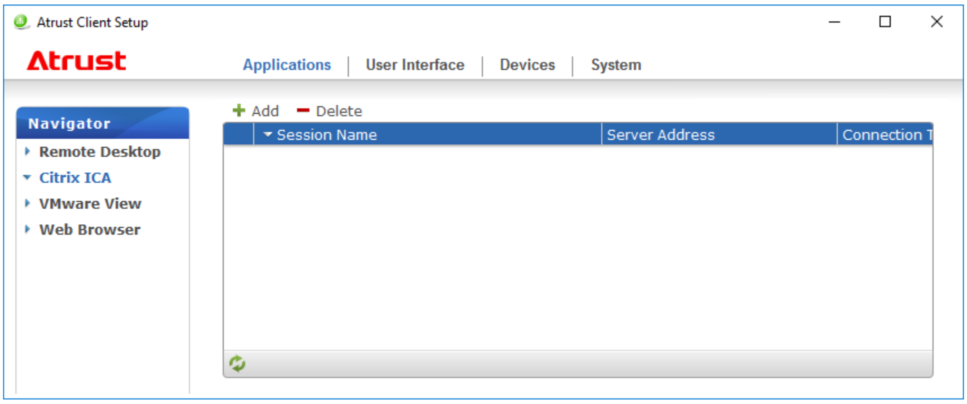
8. Click **Save** to confirm. The access shortcut will be created automatically on the desktop.

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, see Chapter 4, "5.8 Configuring Advanced ICA Connection Settings".

5.6.3 Connection Type: XenApp

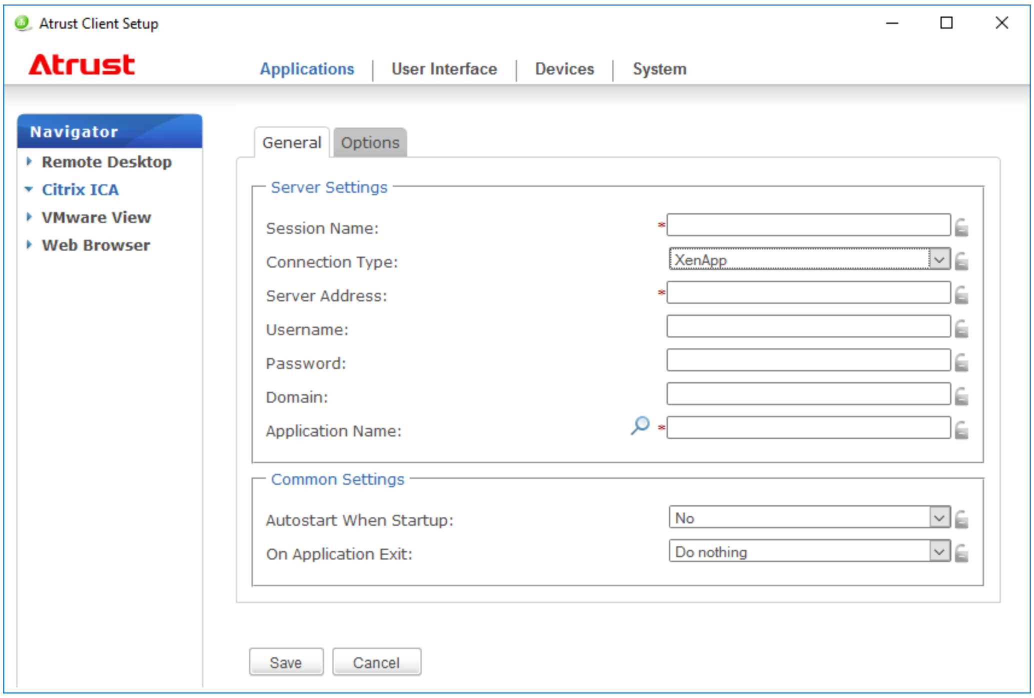
To configure ICA connection settings for the connection type of XenApp, do the following:

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



Note If you have not created any entry, the ICA Connection list will be empty.

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



Server Settings

Session Name:

Connection Type: XenApp

Server Address:

Username:

Password:

Domain:

Application Name:

Common Settings

Autostart When Startup: No

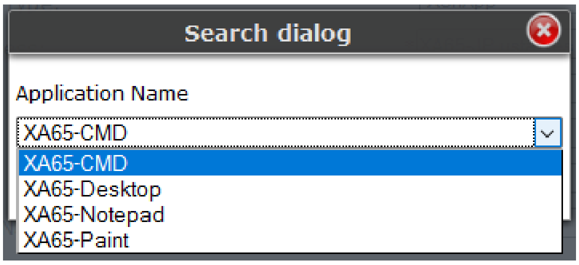
On Application Exit: Do nothing

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 system 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.

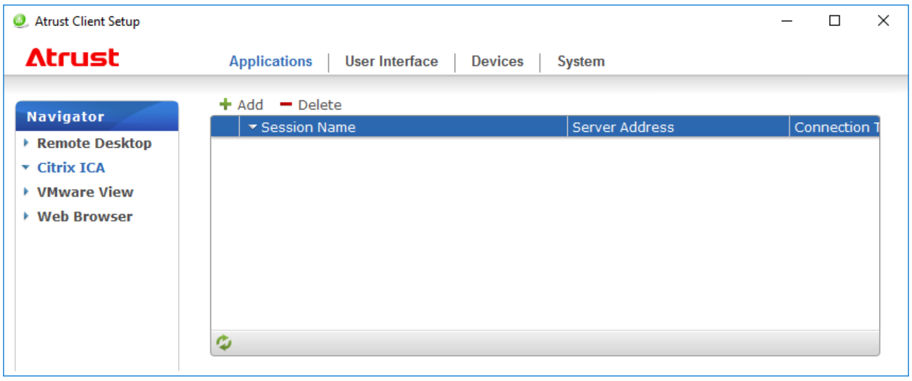
Note

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, see Chapter 4, "5.8 Configuring Advanced ICA Connection Settings".

5.6.4 Connection Type: Server Connection

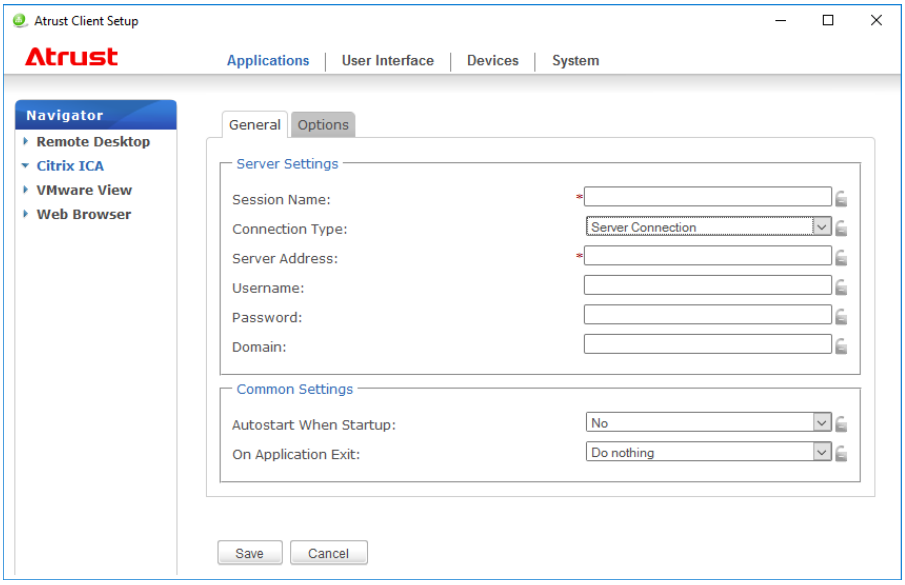
To configure ICA connection settings for the connection type of Server Connection, do the following:

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



Note If you have not created any entry, the ICA Connection list will be empty.

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



Session Name: *
Connection Type: Server Connection
Server Address: *
Username:
Password:
Domain:

Autostart When Startup: No
On Application Exit: Do nothing

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 system 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, see Chapter 4, "5.8 Configuring Advanced ICA Connection Settings".

5.7 Accessing Citrix Services

Use the access shortcut to Citrix services you created by using Atrust Client Setup as described below.

5.7.1 For Connection Types of XenDesktop, XenApp, and Server Connection

To access Citrix services, 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, see Chapter 3, "2. Accessing Citrix Services".

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

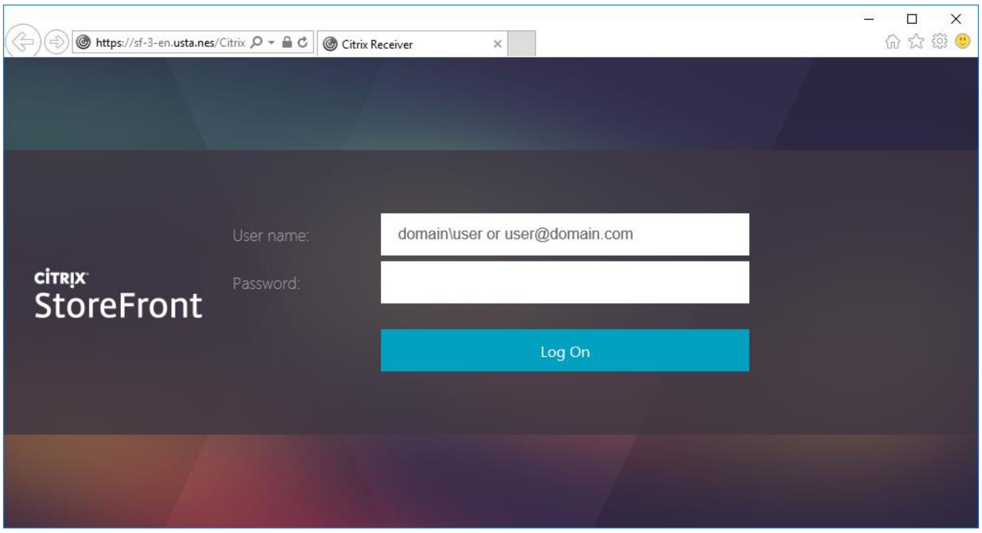
5.7.2 For Connection Types of Web Logon

To access Citrix services, 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, see Chapter 3, "2. Accessing Citrix Services".

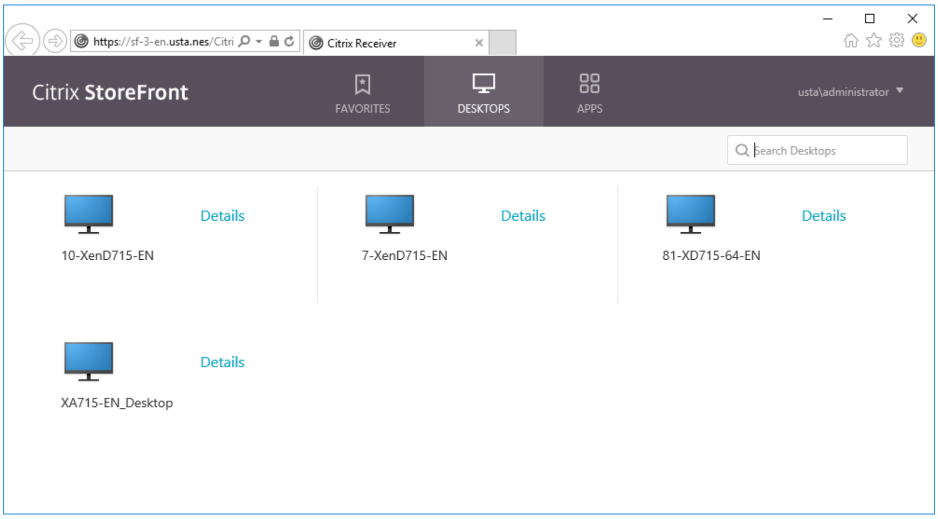
2. The Web browser is launched with the Citrix Logon screen.


https://sf-3-en.usta.nes/Citrix
Citrix Receiver
CITRIX
StoreFront
User name:
domain\user or user@domain.com
Password:
Log On

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

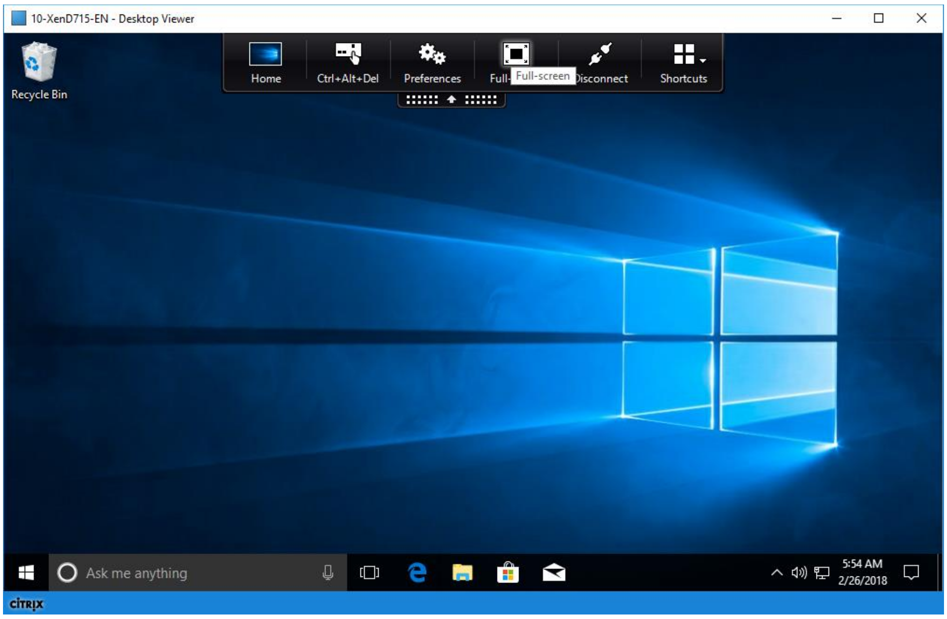
Note If your service-hosted server doesn't belong to any domain, type in the server name instead if required.

4. Connection icons appear.



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

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



5.8 Configuring Advanced ICA Connection Settings

This section provides a description of each setting item for ICA connections.

Read this section to configure advanced settings and customize shortcuts on the desktop and Start menu for service access.

Note Note that available settings vary depending on the selected connection type.

5.8.1 Settings for the Connection Type of Web Logon

Note

- For descriptions of available settings for the connection type of XenDesktop, see Chapter 4, "5.8.2 Settings for the Connection Type of XenDesktop".
- For descriptions of available settings for the connection type of XenApp, see Chapter 4, "5.8.3 Settings for the Connection Type of XenApp".
- For descriptions of settings for the connection type of Server Connection, see Chapter 4, "5.8.4 Settings for the Connection Type of Server Connection".

■ **General Sub-tab**

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Web Logon sessions.</td></tr>
<tr><td><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>Web Logon</b> is selected. Four connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr>
<tr><td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr>
<tr><td><b>XenApp</b></td><td>Provides application delivery services.</td></tr>
<tr><td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr>
</table>
<b>NOTE:</b> When <b>Web Logon</b> is selected, your US320f 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, see Chapter 4, "5.7 Accessing Citrix Services".</td></tr>
<tr><td><b>Server Address</b></td><td>Type in the computer name or IP address of the server or virtual machine to which to deliver the Web Logon session.</td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a Citrix ICA session automatically or not when US320f starts. If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a Citrix ICA session is ended. Four options are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do nothing</b></td><td>Returns to the Windows 10 IoT desktop.</td></tr>
<tr><td><b>Restart Application</b></td><td>Opens a Citrix ICA session again.</td></tr>
<tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr>
<tr><td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr>
</table></td></tr>
</table>

■ Options Sub-tab

<table>
<tr><th colspan="2">Web Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Mode Setting</b></td><td>Click the drop-down menu to select the desired browser window mode.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Full Screen-</b></td><td>The browser is opened in the Full Screen mode.</td></tr>
<tr><td><b>Normal Mode</b></td><td>The browser is opened in the Normal mode.</td></tr>
</table>
<b>NOTE:</b> This setting item is available only when <b>Web Logon</b> is selected in the Connection Type field. This type of connection allows you to access services through the interface of the Web browser.
<b>NOTE:</b> The used Web browser for service access is always the Internet Explorer, no matter which browser you set as the default.</td></tr>
</table>

5.8.2 Settings for the Connection Type of XenDesktop

Note

- For descriptions of available settings for the connection type of Web Logon, see Chapter 4, "5.8.1 Settings for the Connection Type of Web Logon".
- For descriptions of available settings for the connection type of XenApp, see Chapter 4, "5.8.3 Settings for the Connection Type of XenApp".
- For descriptions of settings for the connection type of Server Connection, see Chapter 4, "5.8.4 Settings for the Connection Type of Server Connection".

■ General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>XenDesktop</b> is selected. Four connection types are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr>
<tr><td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr>
<tr><td><b>XenApp</b></td><td>Provides application delivery services.</td></tr>
<tr><td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr>
</table></td></tr>
<tr><td><b>Server Address</b></td><td>Type in the IP address / FQDN of the server through which XenDesktop is accessible.</td></tr>
<tr><td><b>Username</b></td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td><b>Password</b></td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td><b>Domain</b></td><td>Type in the domain of the server.</td></tr>
<tr><td><b>Desktop Group</b></td><td>Type in the desktop group.
<b>NOTE:</b> You can use the Search icon (🔍) in front of the field to discover available desktop groups. For detailed instructions, see Chapter 4, "5.6.2 Connection Type: XenDesktop".</td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a Citrix ICA session automatically or not when US320f starts.
If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a Citrix ICA session is ended. Four options are available: <b>Do nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.</td></tr>
</table>

Option	Description
Do nothing	Returns to the Windows Embedded 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.

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.

Item	Description
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, 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.

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.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE: Mapping Local Serial Ports** is not available because US320f has no serial port.
Mapping Local Printers	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If **Yes** is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions.

Connection Settings

Item	Description
Network Protocol	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: **TCP/IP**, **TCP/IP + HTTP server location**, and **SSL/TLS + HTTPS server location**.
Audio Quality	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**.

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

<table>
<tr><td></td><td><table><tr><td></td><td>during a low-speed connection.</td></tr><tr><td><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr></table></td></tr>
<tr><td><b>Encryption</b></td><td>Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic, RC5 128 bit (login only)</b>, <b>RC5 40 bit</b>, <b>RC5 56 bit</b>, <b>RC5 128 bit</b>.</td></tr>
<tr><td><b>Apply Windows key combinations (e.g Alt + Tab)</b></td><td>Click the drop-down menu to select where to apply Windows key combinations.
Three options are available: <b>On the local desktop</b>, <b>On the remote desktop</b>, <b>In full screen desktops only</b>.</td></tr>
</table>

5.8.3 Settings for the Connection Type of XenApp

Note

- For descriptions of available settings for the connection type of Web Logon, see Chapter 4, "5.8.1 Settings for the Connection Type of Web Logon".
- For descriptions of available settings for the connection type of XenDesktop, see Chapter 4, "5.8.2 Settings for the Connection Type of XenDesktop".
- For descriptions of settings for the connection type of Server Connection, see Chapter 4, "5.8.4 Settings for the Connection Type of Server Connection".

■ General Sub-tab

<table>
<tr><th colspan="2">Server Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Type in the name for Citrix ICA sessions.</td></tr>
<tr><td><b>Connection Type</b></td><td>This table only provides descriptions for available settings when <b>XenApp</b> is selected. Four connection types are available:<table><tr><th>Option</th><th>Description</th></tr><tr><td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr><tr><td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr><tr><td><b>XenApp</b></td><td>Provides application delivery services.</td></tr><tr><td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr></table></td></tr>
<tr><td><b>Server Address</b></td><td>Type in the IP address and FQDN of the server through which XenApp is accessible.</td></tr>
<tr><td><b>Username</b></td><td>Type in the user/account name used for authentication.</td></tr>
<tr><td><b>Password</b></td><td>Type in the password of the user account used for authentication.</td></tr>
<tr><td><b>Domain</b></td><td>Type in the domain of the server.
<b>NOTE:</b> Type in the full computer/server name if your XenApp server doesn't belong to any domain.</td></tr>
<tr><td><b>Application Name</b></td><td>Type in the application name.
<b>NOTE:</b> You can use the Search icon (🔍) in front of the field to discover available applications. For detailed instructions, see Chapter 4, "5.6.3 Connection Type: XenApp".</td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a Citrix ICA session automatically or not when US320f starts.
If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a Citrix ICA session is ended. Four options are available: <b>Do nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.<table><tr><th>Option</th><th>Description</th></tr><tr><td><b>Do nothing</b></td><td>Returns to the Windows 10 IoT desktop.</td></tr><tr><td><b>Restart Application</b></td><td>Opens a Citrix ICA session again.</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr><tr><td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr></table></td></tr>
</table>

■ Options Sub-tab

<table>
<tr><th colspan="2">Window Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Requested Color Quality</b></td><td>Click the drop-down menu to select the desired color quality for a Citrix ICA session.<table><tr><th>Option</th><th>Description</th></tr><tr><td><b>No preference</b></td><td>No preference for a specific color quality.</td></tr><tr><td><b>Better Speed (16-bit)</b></td><td>The 16-bit color quality is used for better display speed.</td></tr><tr><td><b>Better Appearance (32-bit)</b></td><td>The 32-bit color quality is used for better desktop appearance.</td></tr></table></td></tr>
<tr><td><b>Window Size</b></td><td>Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: <b>Default</b>, <b>Seamless</b>, <b>Full Screen</b>, <b>640 x 480</b>, <b>800 x 600</b>, <b>1024 x 768</b>, <b>1280 x 1024</b>, and <b>1600 x 1200</b>.

<b>NOTE:</b> When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size.
<b>NOTE:</b> For more information about how to disable the XenDesktop toolbar, visit Citrix websites at support.citrix.com or www.citrix.com for online help.
<b>NOTE:</b> 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.</td></tr>
<tr><th colspan="2">Device Mapping</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Mapping Local Drive</b></td><td>Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.</td></tr>
<tr><td><b>Mapping Local Serial Ports</b></td><td>Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions.
<b>NOTE: Mapping Local Serial Ports</b> is not available because US320f has no serial port.</td></tr>
<tr><td><b>Mapping Local Printers</b></td><td>Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions through this connection.</td></tr>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Network Protocol</b></td><td>Click the drop-down menu to select the protocol(s) used for connection. Three options are available: <b>TCP/IP</b>, <b>TCP/IP + HTTP server location</b>, and <b>SSL/TLS + HTTPS server location</b>.</td></tr>
<tr><td><b>Audio Quality</b></td><td>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: <b>High - high definition audio</b>, <b>Medium - optimized for speech</b>, <b>Low - for low-speed connections</b>, and <b>Off</b>.<table><tr><th>Option</th><th>Description</th></tr><tr><td><b>High - high definition audio</b></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><b>Medium - optimized for speech</b></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><b>Low - for low-speed connections</b></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><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr></table></td></tr>
<tr><td><b>Encryption</b></td><td>Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic</b>, <b>RC5 128 bit (login only)</b>, <b>RC5 40 bit</b>, <b>RC5 56 bit</b>, <b>RC5 128 bit</b>.</td></tr>
</table>

Apply Windows key combinations (e.g Alt + Tab)	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**.

5.8.4 Settings for the Connection Type of Server Connection

Note

- For descriptions of available settings for the connection type of Web Logon, see Chapter 4, "5.8.1 Settings for the Connection Type of Web Logon".
- For descriptions of available settings for the connection type of XenDesktop, see Chapter 4, "5.8.2 Settings for the Connection Type of XenDesktop".
- For descriptions of settings for the connection type of XenApp, see Chapter 4, "5.8.3 Settings for the Connection Type of XenApp".

■ General Sub-tab

Server Settings	
Item	**Description**
Session Name	Type in the name for Citrix ICA sessions.
Connection Type	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>
Server Address	Type in the IP address and FQDN of the XenApp server. **NOTE:** Server Connection only supports connections to XenApp servers.
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:** Type in the full computer/server name if the server doesn't belong to any domain.
Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when Windows Embedded 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. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Do nothing**</td><td>Returns to the Windows 10 IoT desktop.</td></tr><tr><td>**Restart Application**</td><td>Opens a Citrix ICA session again.</td></tr><tr><td>**Reboot**</td><td>Restarts your thin client.</td></tr><tr><td>**Shutdown**</td><td>Turns off your thin client.</td></tr></table>

■ Options Sub-tab

<table>
<tr><th colspan="2">Window Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Requested Color Quality</b></td><td>Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: <b>No preference</b>, <b>Better Speed (16-bit)</b>, and <b>Better Appearance (32-bit)</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>No preference</b></td><td>No preference in a specific color quality.</td></tr>
<tr><td><b>Better Speed (16-bit)</b></td><td>The 16-bit color quality is used for better display speed.</td></tr>
<tr><td><b>Better Appearance (32-bit)</b></td><td>The 32-bit color quality is used for better desktop appearance.</td></tr>
</table></td></tr>
<tr><td><b>Window Size</b></td><td>Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: <b>Default</b>, <b>Seamless</b>, <b>Full Screen</b>, <b>640 x 480</b>, <b>800 x 600</b>, <b>1024 x 768</b>, <b>1280 x 1024</b>, and <b>1600 x 1200</b>.

<b>NOTE:</b> When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size.
<b>NOTE:</b> For more information about how to disable the XenDesktop toolbar, visit Citrix websites at support.citrix.com or www.citrix.com for online help.
<b>NOTE:</b> 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.</td></tr>
<tr><th colspan="2">Device Mapping</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Mapping Local Drive</b></td><td>Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.</td></tr>
<tr><td><b>Mapping Local Serial Ports</b></td><td>Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions.
<b>NOTE: Mapping Local Serial Ports</b> is not available because US320f has no serial port.</td></tr>
<tr><td><b>Mapping Local Printers</b></td><td>Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions through this connection.</td></tr>
<tr><th colspan="2">Connection Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Network Protocol</b></td><td>Click the drop-down menu to select the protocol(s) used for connection. Three options are available: <b>TCP/IP</b>, <b>TCP/IP + HTTP server location</b>, and <b>SSL/TLS + HTTPS server location</b>.</td></tr>
<tr><td><b>Audio Quality</b></td><td>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:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>High - high definition audio</b></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><b>Medium - optimized for speech</b></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><b>Low - for low-speed connections</b></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><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr>
</table></td></tr>
<tr><td><b>Encryption</b></td><td>Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic</b>, <b>RC5 128 bit (login only)</b>, <b>RC5 40 bit</b>, <b>RC5 56 bit</b>, <b>RC5 128 bit</b>.</td></tr>
<tr><td><b>Apply Windows key combinations (e.g Alt + Tab)</b></td><td>Click the drop-down menu to select where to apply Windows key combinations. Three options are available: <b>On the local desktop</b>, <b>On the remote desktop</b>, <b>In full screen desktops only</b>.</td></tr>
</table>

5.9 Configuring Basic VMware Horizon Connection Settings

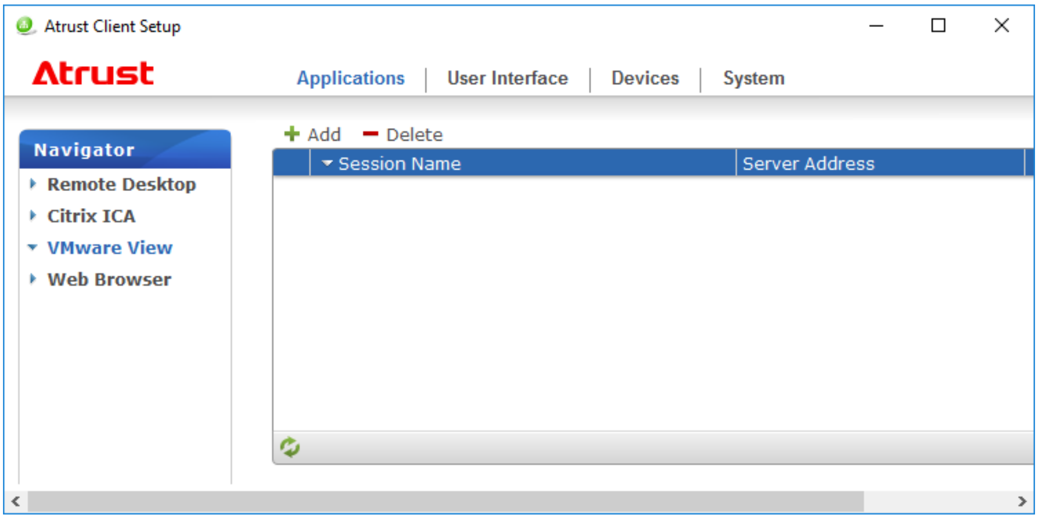
The **VMware View** setting enables you to configure VMware View connection settings for VMware View service and create shortcuts on the desktop and Start menu for service access. You can access on-demand desktop services for work simply through these shortcuts.

Note

- For more information on VMware desktop virtualization solutions, visit VMware website at www.vmware.com.
- You can also access VMware View or Horizon services through the standard desktop shortcut **VMware Horizon View Client**. For detailed instructions on how to access services via the standard desktop shortcut, see Chapter 3, "4. Accessing VMware View and Horizon Services".

To configure VMware View connection settings, do the following:

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

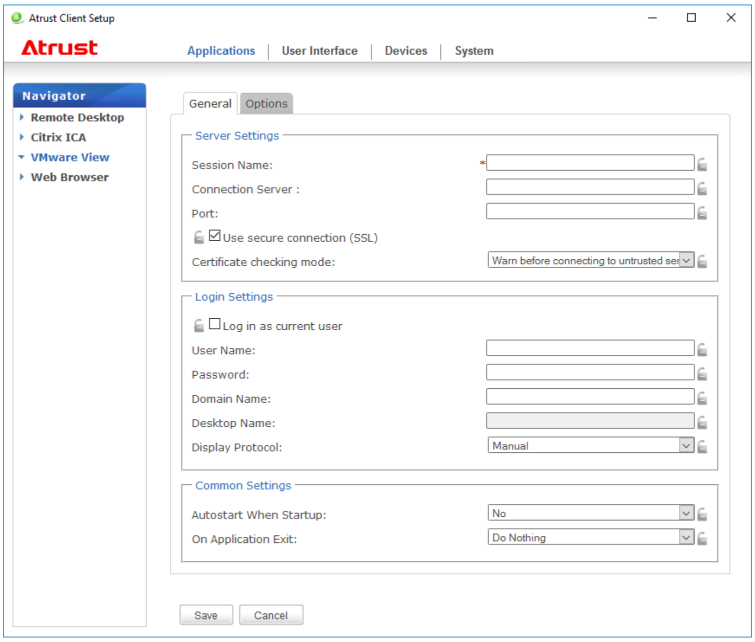


Note

If you have not created any entry, the View Connection list will be empty.

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

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



Server Settings

Session Name: *

Connection Server :

Port:

☑ Use secure connection (SSL)

Certificate checking mode: Warn before connecting to untrusted ser

Login Settings

□ Log in as current user

User Name:

Password:

Domain Name:

Desktop Name:

Display Protocol: Manual

Common Settings

Autostart When Startup: No

On Application Exit: Do Nothing

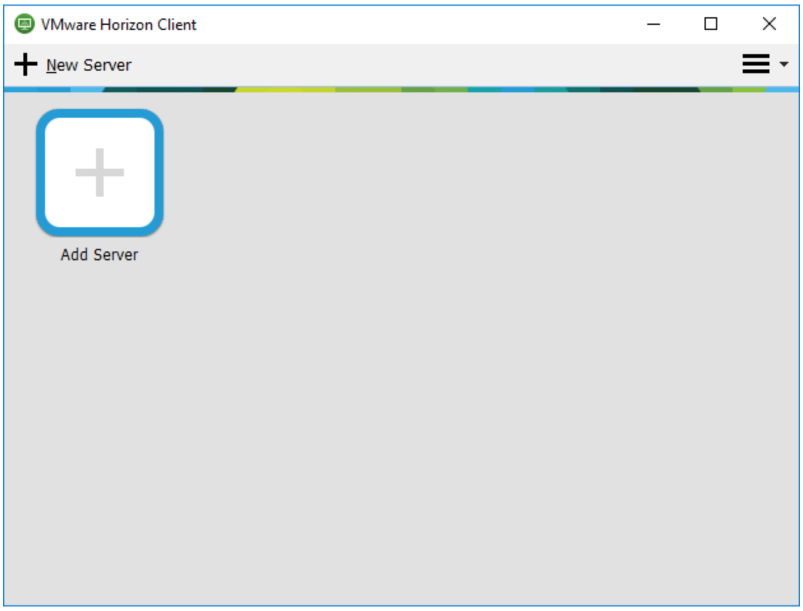
Note This is the only required field for the creation of a service access shortcut on the desktop. Other data can be provided during the period of service access. Depending on your needs, you might choose to type in more other data.

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

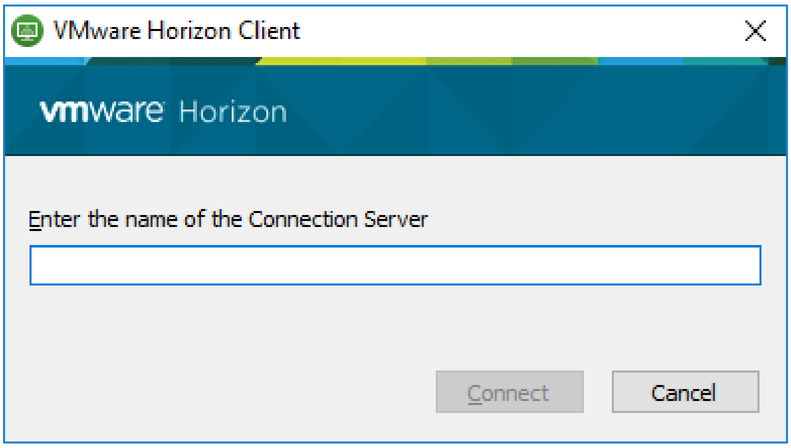
5.10 Accessing VMware View or Horizon Services

To access VMware View or Horizon services, 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**.

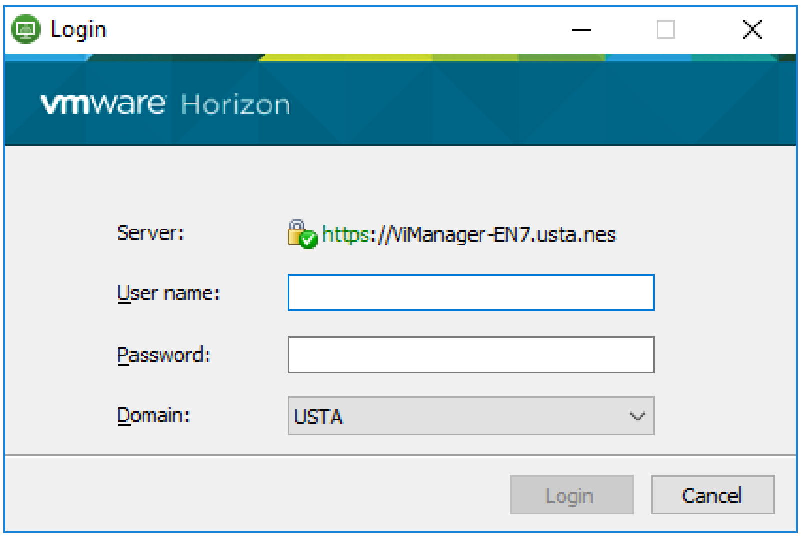


5. By default, a secure connection (HTTPS) is required to connect to the View Connection server. You therefore need to install a certificate.

Note For how to install a certificate, see Chapter 5, "14. Installing the Certificate".

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**.



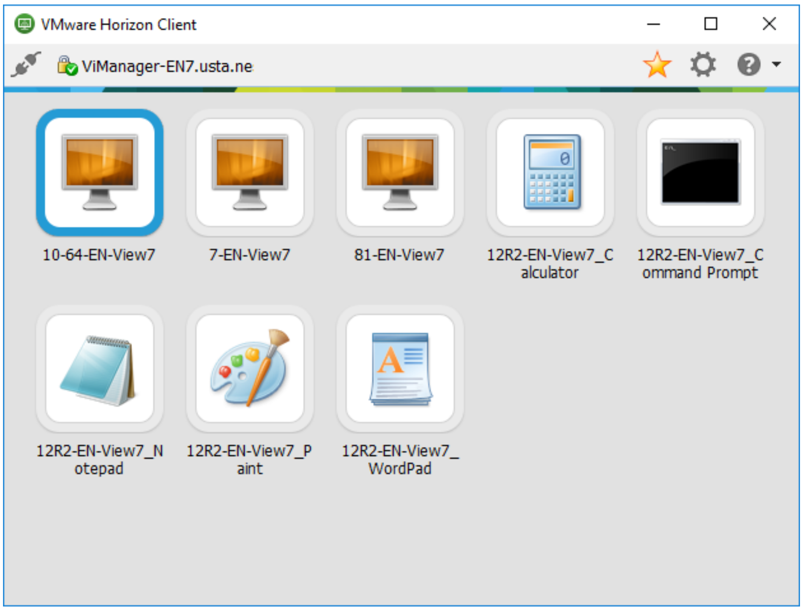
Server: https://ViManager-EN7.usta.nes

User name:

Password:

Domain: USTA

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



9. The virtual desktop will be displayed on the screen.

5.11 Configuring Advanced View Connection Settings

This section provides a description of each setting item for VMware View connections.

Read this section 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><b>Session Name</b></td><td>Type in the name for VMware View or Horizon sessions.</td></tr>
<tr><td><b>Connection Server</b></td><td>Type in the computer name or IP address of the View Connection Server.
<b>NOTE:</b> For more information on View Connection Server, visit VMware website at www.vmware.com.</td></tr>
<tr><td><b>Port</b></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><b>Use secure connection (SSL)</b></td><td>Check/Uncheck to enable/disable secure connection.</td></tr>
<tr><td><b>Certificate checking mode</b></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: <b>Do not verify server identity certificates</b>, <b>Warn before connecting to untrusted servers</b>, and <b>Never connect to untrusted servers</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do not verify server identity certificates</b></td><td>Do not verify the identity of the remote server and connect to it anyway.</td></tr>
<tr><td><b>Warn before connecting to untrusted servers</b></td><td>Warns and allows users to choose whether to connect or not.</td></tr>
<tr><td><b>Never connect to untrusted servers</b></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><b>Log in as current user</b></td><td>Check to log in to VMware View or Horizon services with the current user credentials. When checked, the User Name, Password, and Domain Name fields will be grayed out.</td></tr>
<tr><td><b>User Name</b></td><td>Type in the user name for authentication.</td></tr>
<tr><td><b>Password</b></td><td>Type in the password for authentication.</td></tr>
<tr><td><b>Domain Name</b></td><td>Type in the domain name of the View Connection Server.</td></tr>
<tr><td><b>Desktop Name</b></td><td>Type in the desktop name. Or, leave it blank for users to select one.
<b>NOTE:</b> If <b>Manual</b> is selected for the Display Protocol field below, this field will be grayed out.</td></tr>
<tr><td><b>Display Protocol</b></td><td>Click the drop-down menu to select the display protocol. Three options are available: <b>Manual</b>, <b>PCoIP</b>, <b>VMware Blast</b>, and <b>Microsoft RDP</b>.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Manual</b></td><td>Manually select the desired display protocol.</td></tr>
<tr><td><b>PCoIP</b></td><td>Use VMware PCoIP as the display protocol.</td></tr>
<tr><td><b>VMware Blast</b></td><td>Use VMware Blast as the display protocol.</td></tr>
<tr><td><b>Microsoft RDP</b></td><td>Use Microsoft RDP as the display protocol.</td></tr>
</table></td></tr>
</table>

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a VMware View or Horizon session automatically or not when US320f starts. If <b>Yes</b> is selected, when you log in to the system, the VMware View or Horizon session will be opened automatically.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a VMware View or Horizon session is ended.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do Nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr>
<tr><td><b>Restart Application</b></td><td>Opens a VMware View or Horizon session again.</td></tr>
<tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr>
<tr><td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr>
</table>
</td></tr>
</table>

■ **Options Sub-tab**

<table>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Display</b></td><td>Click the drop-down menu to select the desired display size of a View desktop.
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Full Screen</b></td><td>Opens the selected View desktop in full screen.</td></tr>
<tr><td><b>Multi Monitor</b></td><td>Opens the selected View desktop in multiple displays.</td></tr>
<tr><td><b>Large Window</b></td><td>Opens the selected View desktop in a large window.</td></tr>
<tr><td><b>Small Window</b></td><td>Opens the selected View desktop in a small window.</td></tr>
</table>
</td></tr>
</table>

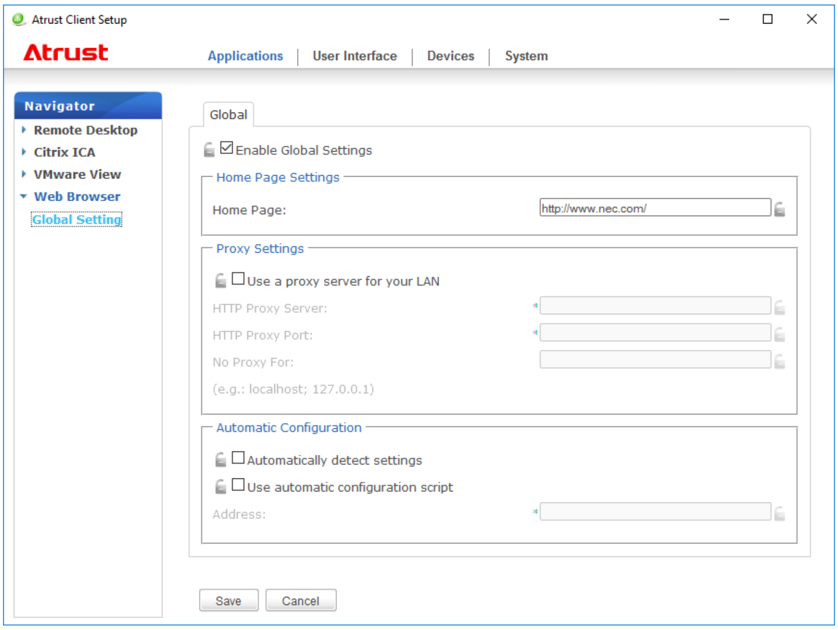
5.12 Configuring Web Browser Settings

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

5.12.1 Configuring General Browser Session Settings

To configure general browser session settings, do the following:

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



☑ Enable Global Settings

Home Page Settings

Home Page: http://www.nec.com/

Proxy Settings

□ Use a proxy server for your LAN

HTTP Proxy Server:

HTTP Proxy Port:

No Proxy For:

(e.g.: localhost; 127.0.0.1)

Automatic Configuration

□ Automatically detect settings

□ Use automatic configuration script

Address:

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

Global	
Item	**Description**
Enable Global Settings	Select this check box to enable global settings.
Home Page 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.

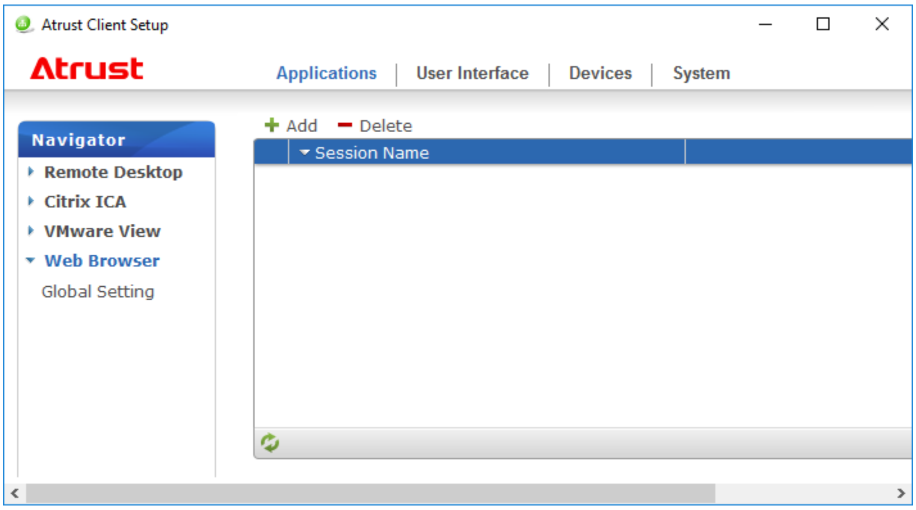
5.12.2 Configuring Specific Browser Session Settings

To configure specific browser session settings and create shortcuts on the desktop and Start menu, 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.

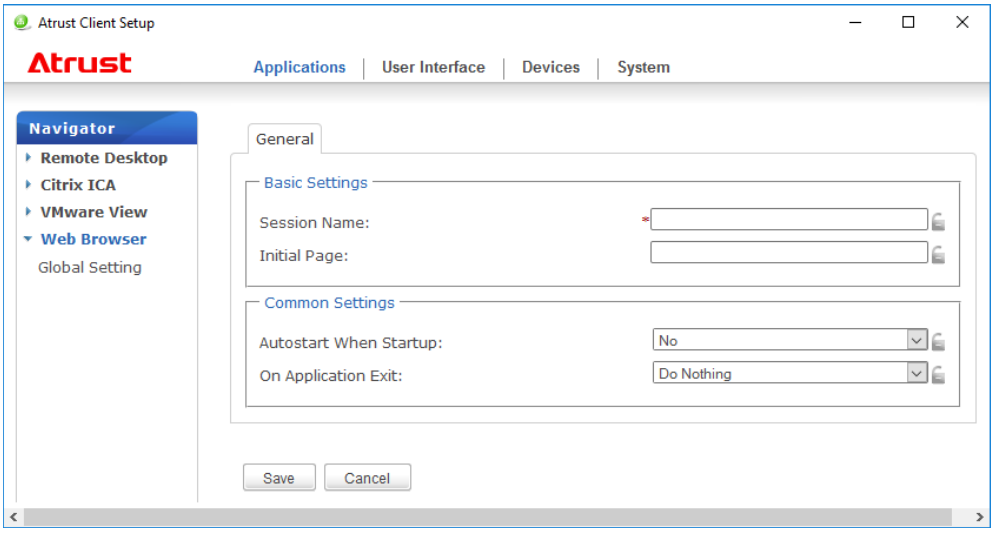
1. On Atrust Client Setup, click **Applications** > **Web Browser**.
2. The Browser Session list appears in the Configuration area.



Note

> If you have not created 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 (see the table below for descriptions).



Session Name: *

Initial Page:

Autostart When Startup: No

On Application Exit: Do Nothing

<table>
<tr><th colspan="2">General Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Session Name</b></td><td>Specify the browser session name.</td></tr>
<tr><td><b>Initial Page</b></td><td>Specify the URL of the page that opens when the browser session starts.</td></tr>
<tr><th colspan="2">Common Settings</th></tr>
<tr><th>Item</th><th>Description</th></tr>
<tr><td><b>Autostart When Startup</b></td><td>Select whether to open a browser session automatically or not when Windows 10 IoT starts.</td></tr>
<tr><td><b>On Application Exit</b></td><td>Select what to do when a browser session is ended. Four options are available:
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td><b>Do Nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr>
<tr><td><b>Restart Application</b></td><td>Opens a Remote Desktop session again.</td></tr>
<tr><td><b>Reboot</b></td><td>Restarts your thin client.</td></tr>
<tr><td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr>
</table>
</td></tr>
</table>

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

NEC Express5800 Series
US320f

5

Chapter 5 Administrative Utilities and Settings

This chapter provides the information related to administrative utilities and settings.

1. **Launching UWF Automatically**
   Describes utilities to be launched automatically.
2. **Utilities Affected by Shutdown and Restart**
   Describes utilities that are affected by shutdown or restart.
3. **Using the Unified Write Filter (UWF)**
   Describes details of UWF (Unified Write Filter), system change under UWF environment, and UWF command line options.
4. **Automatic Sign-In**
   Describes how to configure automatic sign-in.
5. **Saving Files and Using Local Drives**
   Describes how to save files and how to use local drives.
6. **Participating in Domains**
   Describes how to participate in domain.
7. **Using the Net and Tracert Utilities**
   Describes how to use network utilities.
8. **Managing Users and Groups with Accounts**
   Describes how to create, modify, and configure the user account.
9. **Changing the Computer Name of a Thin Client**
   Describes how to change computer name of US320f.
10. **Setting Date and Time**
    Describes how to set date and time of US320f.
11. **Configuring Dual Monitor Display**
    Describes how to configure dual monitor display, and how to use the span mode.
12. **Installing CMO Terminal Agent**
    Describes how to install CMO Terminal Agent.
13. **Wireless LAN Settings**
    Describes how to configure wireless LAN settings.
14. **Installing the Certificate**
    Describes how to retain certificates under the UWF environment.

1. Launching UWF Automatically

The Unified Writer Filter utility is automatically launched when the system starts. This utility provides a secure environment for thin client computing by protecting the thin client from undesired flash memory writes. The active (green), inactive (red), or changed (orange) status of the filter is indicated by the color of the Unified Writer Filter status icon in the system tray on the taskbar. For details about the Unified Writer Filter, see Chapter 5, "3 Using the Unified Write Filter (UWF)".

2. Utilities Affected by Shutdown and Restart

The following utilities are affected by restarting and shutting down the thin client:

- Unified Writer Filter overlay

  To retain the setting changes after US320f is restarted, you need to disable the Unified Writer Filter. For details, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)”.

  If UWF is not disabled, the new settings will be lost when the thin client is shut down or restarted. The Unified Writer Filter overlay contents are not lost when you simply log off and on again as the same or a different user.

  Writing the UWF overlay while UWF is enabled can be authorized by the administrator by executing a UWF command line option or by specifying a setting in the **Unified Writer Filter Control** dialog box. For details, see Chapter 5, "3. Using the Unified Write Filter (UWF)".

- Power Management

  A monitor saver turns off the video signal to the monitor, allowing the monitor to enter a power-saving mode after a designated idle time. Power settings are available in **Start** > **Control Panel** > **Power Options**.

- Wake-on-LAN

  This standard Windows 10 IoT feature discovers all thin clients in your LAN, and enables you to wake them up by clicking a button. This feature allows Atrust Device Manager, for example, to perform image updates and remote administration functions on devices that have been shut down or are on standby. To use this feature, the thin client power must remain on.

3. Using the Unified Write Filter (UWF)

The Unified Writer Filter provides a secure environment for thin-client computing by protecting the thin client from undesired flash memory writes (flash memory is where the operating system and functional software components reside). By preventing excessive flash write activity, the Unified Writer Filter also extends the life of the thin client. It gives the appearance of read-write access to the flash memory by employing an overlay to intercept all flash writes and returning success to the process that requested the I/O.

Protected and cached flash memory contents can be used while the thin client is active, but they are lost when the thin client is restarted or shut down. To preserve selected changes, disable UWF in the Atrust Client Setup dialog box, change the settings, and then enable UWF again. (See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".) The Unified Writer Filter can be enabled and disabled by using the command line (uwfmgr). The Unified Writer Filter can commit (write) the specified files to the flash memory from the overlay. (If more changes are made on files that have been committed, these files must be committed again if the changes also need to be preserved.) The enabled/disabled status of the Unified Writer Filter is indicated by the Unified Writer Filter status icon in the system tray. Green indicates that the Unified Writer Filter is enabled, red indicates that the Unified Writer Filter is disabled, and orange indicates that the status has been changed and will be applied at the next restart.)

Important

The administrator should periodically check the status of the UWF overlay and restart the thin client if the UWF overlay is more than 80% full.

Do not write data exceeding the maximum size of the UWF overlay, as this will make the thin client unstable.

Tip

Remote Desktop Services Client Access License (RDS CAL) is always preserved, regardless of whether it is added to the exceptions list of the UWF

3.1 Running Unified Writer Filter Command Line Options

US320f allows you to enable or disable UWF and change the overlay size using Atrust Client Setup.

If you need to configure UWF in detail, you can use command line options. There are several command line options you can use to control UWF (command line arguments cannot be combined). For how to configure UWF on Atrust Client Setup, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".

Use the following guidelines for the command line options for UWF. (Click **Start** > **Run**, and open the Command Prompt window by typing "cmd" in the **Open** box.)

Tip

> If you open the Command Prompt window and enter uwfmgr help or uwfmgr ?, all available commands are displayed. For example, for information about the Volume parameter, enter uwfmgr Volume help or uwfmgr Volume ?.

UWFMGR.EXE

Get-Config

Displays the UWF configuration for the current and next sessions.

Filter

Configures general UWF settings.

Enable

Enables UWF in the next session after system restart.

Disable

Disables UWF in the next session after system restart.

Reset-Settings

Restores the original settings captured at installation.

Volume

Configures the settings of the volumes protected by UWF.

Get-Config {<volume> | all}

Displays the exclusion settings for the specified volume or all volumes (if "all" is specified). Information includes both the current and the next sessions.

Protect {<volume> | all}

Adds the specified volume to the list of volumes protected by UWF. UWF starts protection of the volume after the next system restart if UWF filtering is enabled.

Unprotect <volume>

Removes the specified volume from the list of volumes protected by UWF. UWF stops protection of volume after the next system restart.

File

Configures files excluded from UWF.

Get-Exclusions {<volume> | all}

Displays a list of excluded files and directories for the specified volume or all volumes (if "all" is specified). Information includes both the current and the next sessions.

Add-Exclusion <file>

Adds the specified file to the excluded file list of the volume protected by UWF. The file is no longer subject to protection by UWF. The exclusion takes effect after the next system restart.

Remove-Exclusion <file>

Removes the specified file from the excluded file list of the volume protected by UWF. The file is now subject to protection by UWF. The removal of exclusion takes effect after the next system restart.

Commit <file>

Commits (writes) the changes made to the specified file to the volume protected by UWF.

Commit-Delete <file>

Deletes the specified file from overlay and volume.

Registry

Configures registry keys excluded from UWF.

Get-Exclusions

Displays all registry keys contained in the exclude registry list for the current and next sessions.

Add-Exclusion <key>

Adds the specified registry key to the excluded registry list. The exclusion takes effect after the next system restart.

Remove-Exclusion <key>

Removes the specified registry key from the excluded registry list. The removal of exclusion takes effect after the next system restart.

Commit <key> <value>

Commits (writes) the changes made to the specified key and value.

Commit-Delete <key> [<value>]

Deletes the specified registry key and value and commits the deletion. If the value is empty, delete all values and subkeys and commit the deletion.

Overlay

Configures the UWF overlay settings.

Get-Config

Displays the UWF overlay configuration for the current and next session.

Get-AvailableSpace

Displays the free disk space available for the UWF overlay.

Get-Consumption

Displays the disk space currently occupied by the UWF overlay.

Set-Size <size>

Sets the maximum size of the UWF overlay (in MB) for the next session after the system restarts.

Set-Type {RAM | DISK}

Sets the overlay storage type to RAM-based or DISK-based. UWF must be disabled in the current session to set the overlay storage type to DISK-base.

Set-WarningThreshold <size>

Sets the threshold (in MB) for a warning alarm to be issued in the current session.

Set-CriticalThreshold <size>

Sets the threshold (in MB) for a critical alarm to be issued in the current session.

Important **You can change the maximum size of the UWF overlay by using Atrust Client Setup. See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)" for how to change this setting. The overlay storage type and threshold values for issuing warning or critical alarms cannot be changed by using Atrust Client Setup.**

Servicing

Configures UWF Servicing Mode.

Enable

Enables UWF Servicing Mode in the next session after the system restarts.

Disable

Disables UWF Servicing Mode in the next session after the system restarts.

Update-Windows

Command used to apply the Windows Update program to standalone devices.

Get-Config

Displays the UWF Servicing Mode configuration for the current and next sessions.

Important **US320f does not support Windows Update in UWF Servicing Mode. Do not use UWF Servicing Mode.**

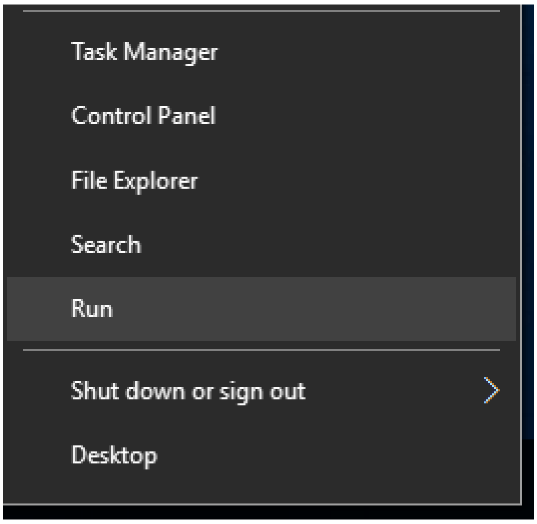
To upgrade the firmware of US320f, use Atrust Device Manager (ADM). For detailed information, see Chapter 6, "1. Using Atrust Device Manager (ADM) Software for Remote Administration".

4. Automatic Sign-In

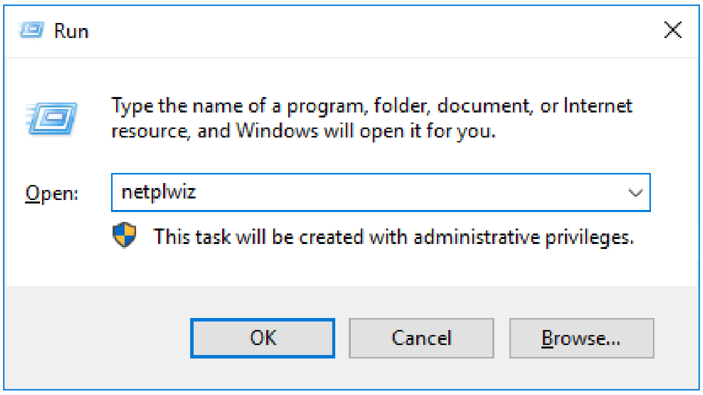
On US320f, the workgroup computers are configured to automatically sign-in with the default User account. If the default password is changed, auto sign-in password must also be changed in the following procedure:

Important **This procedure cannot be used for a computer that belongs to a domain.**

1. Sign in as an Administrator.
2. Click **Run** on the Start menu.



3. Type **netplwiz** in the **Open** dialog box, and then click **OK**.

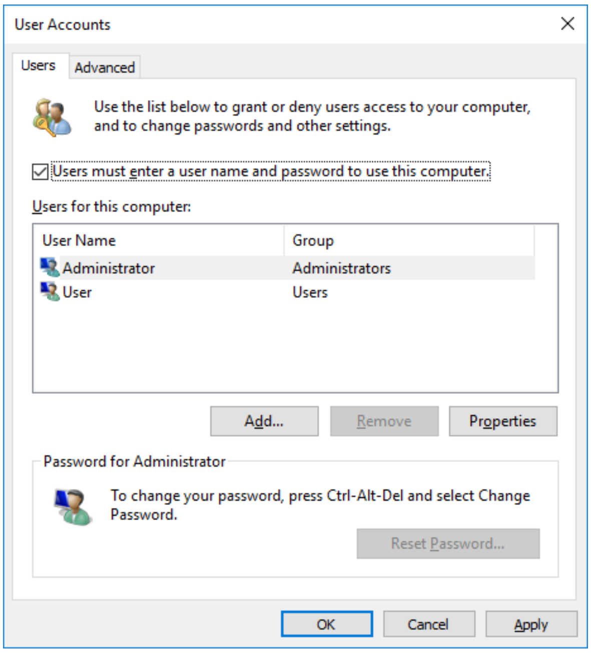

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: netplwiz

This task will be created with administrative privileges.

4. Click the **Users** tab in the **User Accounts** dialog box, and select the **Users must enter a user name and password to use this computer** check box.



User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

Users for this computer:

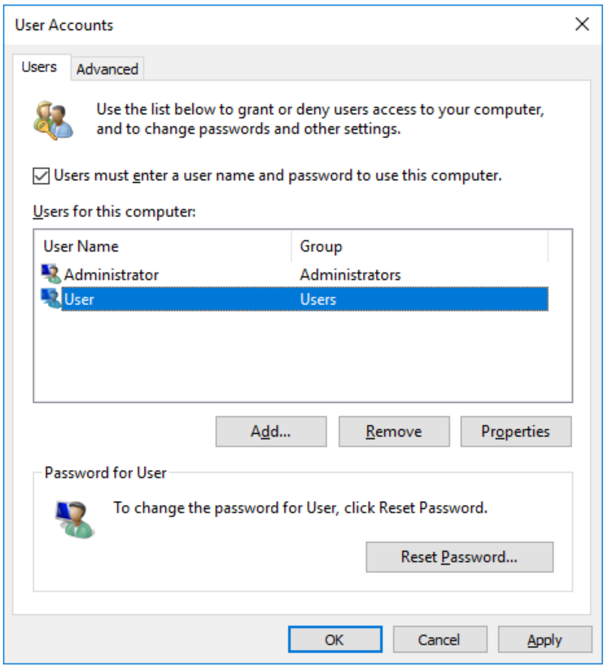
User Name	Group
Administrator	Administrators
User	Users

Password for Administrator

To change your password, press Ctrl-Alt-Del and select Change Password.

5. Select the name of the user for which you want to configure auto sign-in from the list of users.

   * As an example, select the User account



User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☑ Users must enter a user name and password to use this computer.

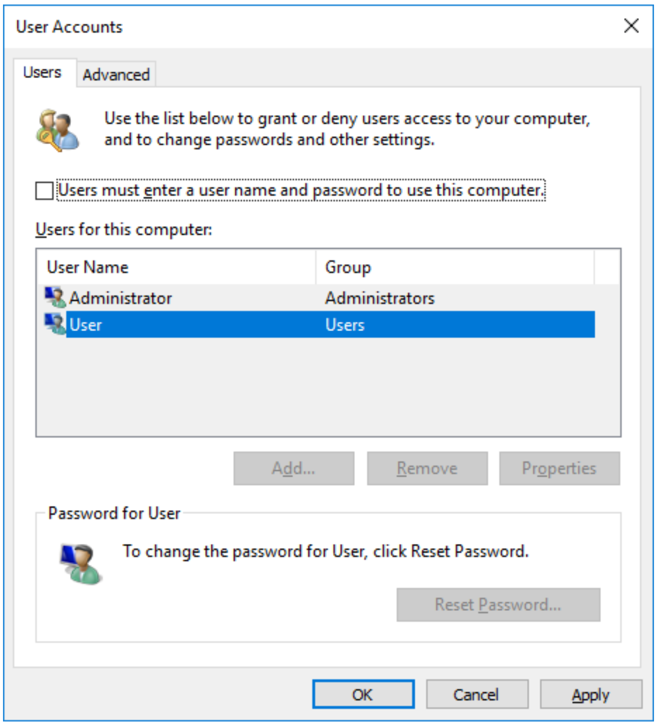
Users for this computer:

User Name	Group
Administrator	Administrators
User	Users

Password for User

To change the password for User, click Reset Password.

6. Clear the **Users must enter a user name and password to use this computer** checkbox, and click **OK**.



Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☐ Users must enter a user name and password to use this computer.

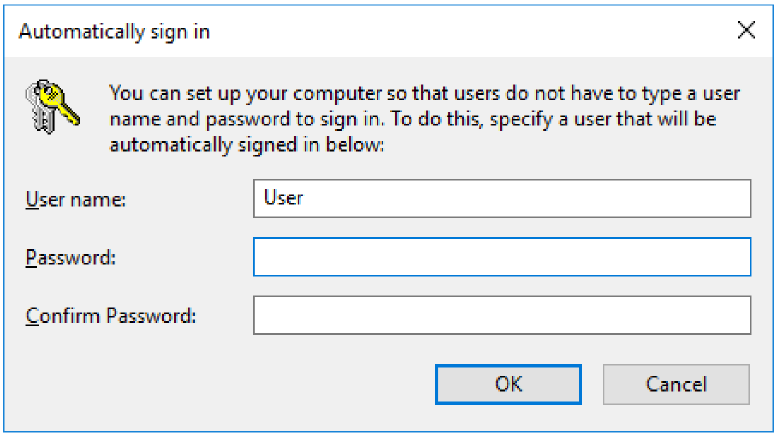
Users for this computer:

User Name	Group
Administrator	Administrators
User	Users

Password for User

To change the password for User, click Reset Password.

7. The **Automatically sign in** dialog appears. Type the password to be used at sign-in in the **Password** and **Confirm Password** boxes, and then click **OK**.



You can set up your computer so that users do not have to type a user name and password to sign in. To do this, specify a user that will be automatically signed in below:

User name: User

Password:

Confirm Password:

8. Restart the computer to make sure that you can sign in to the system as the configured user.

5. Saving Files and Using Local Drives

Administrators need to know the following information about local drives and saving files.

Saving Files

Thin clients use an embedded operating system with a fixed amount of flash memory. It is recommended that you save files you want to keep on a server rather than on a thin client.

Drive C and flash memory

Drive C is the on-board non-volatile flash memory. It is recommended that you avoid writing to drive C. Writing to drive C reduces the size of the flash memory. If the flash memory size is reduced to under 3 MB, the thin client will become unstable.

Important **It is highly recommended that 3 MB of flash memory be left unused. If the free flash memory size is reduced to 2 MB, the thin client image will be irreparably damaged and it will be necessary for you to contact an authorized service center to repair the thin client.**

When UWF is enabled, changes made on local drives are saved in the UWF overlay. If the UWF overlay is about to overflow, the operation of the thin client becomes unstable. Items that are written to the UWF overlay (or directly to the flash memory if UWF is disabled) during normal operations include:

- Favorites
- Created connections
- Delete/edit connections
- Application cache

6. Participating in Domains

You can participate in domains by joining the thin client to a domain or by using roaming profiles.

Participating in Domains

The administrator can join the thin client to the domain in the **Change Computer Name** dialog box (**Start Button Right Click Menu** > **System** > **Change Settings** > **Computer Name** tab **Change**).

Important **US320f can not participate in domain from Settings > Account > Access work or school > Connect. This is a specification limitation of US320f. To participate in the domain of US320f, use the system property dialog.**

6.1 About Domain User Profile

When joining the thin client to a domain, disable the Unified Writer Filter so that the domain information can be permanently stored on the thin client. The Unified Writer Filter should remain disabled through the next boot as information is written to the thin client on the boot after joining the domain. This is especially important when joining an Active Directory domain. For details about disabling and enabling the Unified Writer Filter, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)". If you did not sign-in with the domain account and enabled the UWF, the profile of the domain account is created at every sign-in. To avoid this, sign in with the domain account before enabling the UWF.

If you activate UWF without signing in with domain account after joining US320f to the domain, the domain user profile created after starting US320f next time and Initial sign-in with UWF enabled are lost by shutting down or restarting US 320f. Therefore, it is important to note that a new domain user profile will be created each time US320d is restarted.

On the other hand, even if you first sign-in with UWF disabled and create a domain user profile, after UWF activation, any changes made to the domain user profile will be lost due to US320f shutdown and reboot. Note that the domain cache maintained in US320f remains as it was created when UWF is invalidated, and application of client settings by domain group policy is also lost due to shutdown and restart of US320f.

Also, it is not realistic to create and maintain profiles of all domain users using US320f with UWF invalid status.

For the domain user profile, it is necessary to set it appropriately beforehand with sufficient preliminary verification in consideration of the system environment to be used and the influence on the application, depending on the specification specific to the thin client as mentioned above.

6.2 Change password of domain computer account when UWF is enabled

Microsoft Windows-based computer that joined a domain uses the domain controller to periodically change the computer account password for security purposes. If the thin client is a member of such a domain, password processing is applied to the thin client as well. If UWF is enabled, the thin client will successfully change this password on the domain controller, but since UWF is enabled, the new password will not be retained the next time the thin client is started. In this case, you have the following options.

- Set "1" to the DisablePasswordChange registry entry and disable machine account password change on the thin client.
- Refer to the Microsoft manual for each operating system to disable machine account password change on the Windows based server. For example, to disable machine account password changes on Windows 2008 Server, set RefusePasswordChange registry entry "1" on all domain controllers in the domain, not on each workstation. Even after setting above, the thin client tries to change the password every 30 days, but it is rejected by the server.

6.2.1 Disabling Password Changes for Domain Computer Account in US320f

Following the steps will invalidate periodic computer account password changes after joining the domain.

1. Click **Start** > **Run** to start Registry Editor. Enter **regedit** in the **Name** text box and click **OK**.
2. Find the following registry subkey location and click it.

   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
3. In the right pane, right-click DisablePasswordChange.
4. Click **Modify** on the **Edit** menu.
5. Enter **1** in the **Value data** text box and click **OK**.
6. Quit Registry Editor.

6.2.2 Disabling Change of Domain Controller's Computer Account Password

1. Click **Start** > **Run** to start Registry Editor. Enter **regedit** in the **Name** text box and click **OK**.
2. Find the following registry subkey location and click it.

   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
3. On the **Edit** menu, point to **New** and click **DWORD Value**.
4. Enter RefusePasswordChange as the Registry entry name and click **Enter**.
5. On the **Edit** menu, click **Modify**.
6. Enter **1** in the **Value data** text box and click **OK**.
7. Quit Registry Editor.

7. Using the Net and Tracert Utilities

Net and Tracert utilities are available for administrative use (for example, to determine the route taken by packets across an IP network). For more information about these utilities, go to: http://www.microsoft.com.

8. Managing Users and Groups with Accounts

Use the **Accounts** window (**Start** > **Settings** > **Accounts**) to create and manage user accounts, create and manage groups, and configure advanced user profile properties. By default, a new user is only a member of the **Users** group and is not locked down. As the administrator, you can select the attributes and profile settings for users.

This section provides quick-start guidelines on:

- Creating User Accounts
- Editing User Accounts
- Configuring User Profiles

8.1 Creating User Accounts

Only administrators can create new user accounts locally or remotely.
However, due to local flash memory/disk space constraints, the number of additional users on the thin client should be kept to a minimum.

Important **To retain the setting changes after US320f is restarted, you need to disable the Unified Writer Filter. For details, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".**

1. Log in as an administrator and open the **Accounts** window (**Start** > **Settings** > **Accounts > Other people**).
2. Click the **+** button in **Add someone else to this PC**.
3. When you finish creating the user account, the user you created appears in the **Account** window.

8.2 Editing User Accounts

To edit default settings for standard users and administrator accounts, follow the steps below.

1. Sign in as an administrator and open the **Account** window (**Start** > **Settings** > **Account > Other people**)).
2. Click the **+** button in **Add someone else to this PC**.
3. Select **User** in the left pane and click the account whose setting you want to change to change the setting.

8.3 Configuring User Profiles

Open the **User Profile** window (**Start Button Right Click Menu** > **System** > **Advanced System Settings** > **Set User Profile**) and use the command buttons such as **Change Type**, **Delete**, **Copy Destination**, etc. in accordance with the Microsoft manual provided by the wizard to set the Default, Administrator, and User Profiles stored in the thin client.

9. Changing the Computer Name of a Thin Client

Administrators can use the **Computer Name** tab in the **System Properties** dialog box (**Start** > **Control Panel** > **System** > **Advanced system settings**) to change the computer name of a thin client. When changing the computer name, disable the UWF so that the new computer name can be permanently stored on the thin client. The UWF should remain disabled through the next boot as information is written to the thin client on the boot after restart. This is especially important when changing the computer name. For details about disabling and enabling the UWF, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".

Follow the steps below to make the computer name change permanent.

1. Disable the UWF (Unified Write Filter).
2. Change the computer name.
3. Reboot the thin client.
4. Enable the UWF (Unified Write Filter).
5. Reboot the thin client.

10. Setting Date and Time

The local time utility can be set to synchronize the thin client clock to a time server automatically at a designated time, or manually.

Maintain the correct time because some applications require access to local thin client time. You can open the "Date and time" dialog box by double-clicking the "Date and time" icon in the control panel.

11. Configuring Dual Monitor Display

You can set up dual monitors using the **Screen Resolution** window. To display the **Screen Resolution** window, click the **Display** icon in the control panel or click the **System** > **Display** setting (see the manual of Microsoft Corporation at http://www.microsoft.com).

Note that triple screen output is not available.

Important

NEC only supports genuine optional monitors. When using another monitor in the actual operating environment, thoroughly evaluate the operation with the specified settings based on the actual operating environment and confirm that there is no problem.

12. Installing CMO Terminal Agent

To access NEC Client Management Option (CMO) services from US320f, use CMO Terminal Agent. CMO Terminal Agent is not installed on US320f by default; however, US320f includes the following installers:

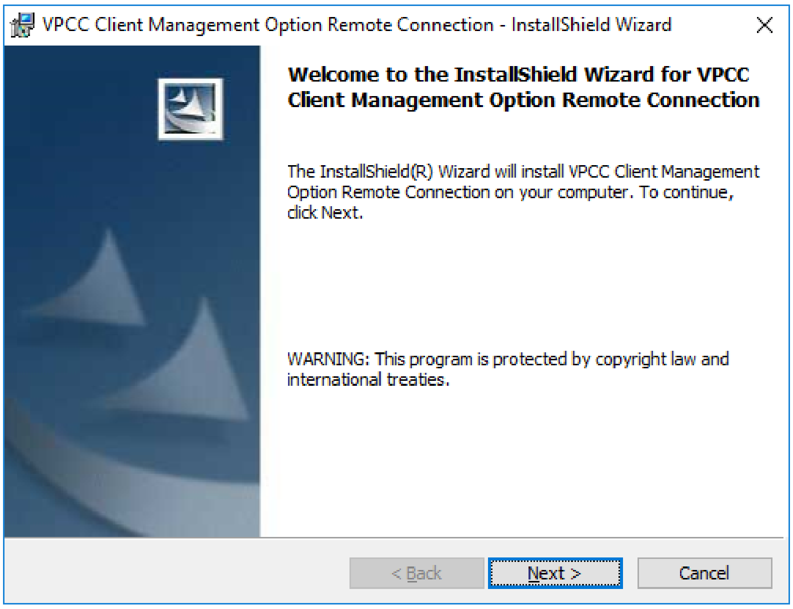
- CMO Terminal Agent Version 6.0
- CMO Terminal Agent Version 6.2

Important

- **When installing or uninstalling CMO Terminal Agent, be sure to disable UWF (Unified Writer Filter) and then enable it again after installation or uninstallation is complete. For how to configure UWF, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".**
- **When installing or uninstalling CMO Terminal Agent, you need to apply the shortcuts of CMO Terminal Agent to the User account before enabling UWF (Unified Writer Filter). It takes some time before the shortcuts are displayed on the Start screen of a user account other than Administrator after sign-in. If you enable UWF without applying the shortcuts when using a User account, the settings will be discarded every time the system restarts and the shortcuts will take a long time to appear. (In the case of uninstallation, the deleted shortcuts remain and take time to disappear.)**
- **When downgrading CMO Terminal Agent Version 6.2 to Version 6.0, first uninstall Version 6.2, and then install Version 6.0.**
- **CMO Terminal Agent cannot be downgraded by performing an overwrite install. To downgrade CMO Terminal Agent, uninstall the new version of CMO Terminal Agent and then install the old version of CMO Terminal Agent.**
- **Upgrade from CMO Terminal Agent Version 6.0 to Version 6.1 is not possible.**

Install CMO Terminal Agent as follows:

1. Sign in to US320f as an Administrator.
2. Double-click the CMO Terminal Agent installer icon on the desktop.
3. The wizard to install CMO Terminal Agent appears. Click **Next**.



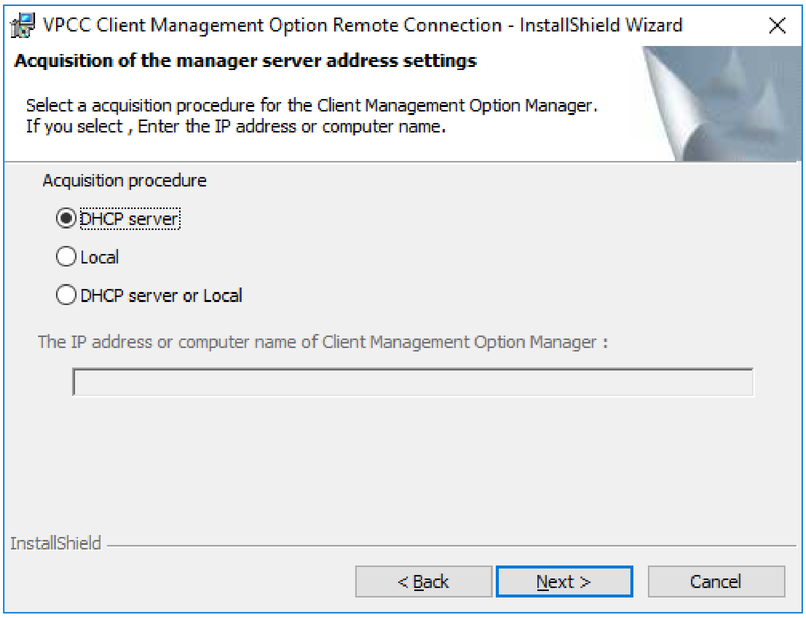
VPCC Client Management Option Remote Connection - InstallShield Wizard

Welcome to the InstallShield Wizard for VPCC Client Management Option Remote Connection

The InstallShield(R) Wizard will install VPCC Client Management Option Remote Connection on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

4. Select the method for obtaining Client Management Option Manager that is appropriate for your environment, and then click **Next**.



VPCC Client Management Option Remote Connection - InstallShield Wizard

Acquisition of the manager server address settings

Select a acquisition procedure for the Client Management Option Manager.
If you select , Enter the IP address or computer name.

Acquisition procedure

● DHCP server

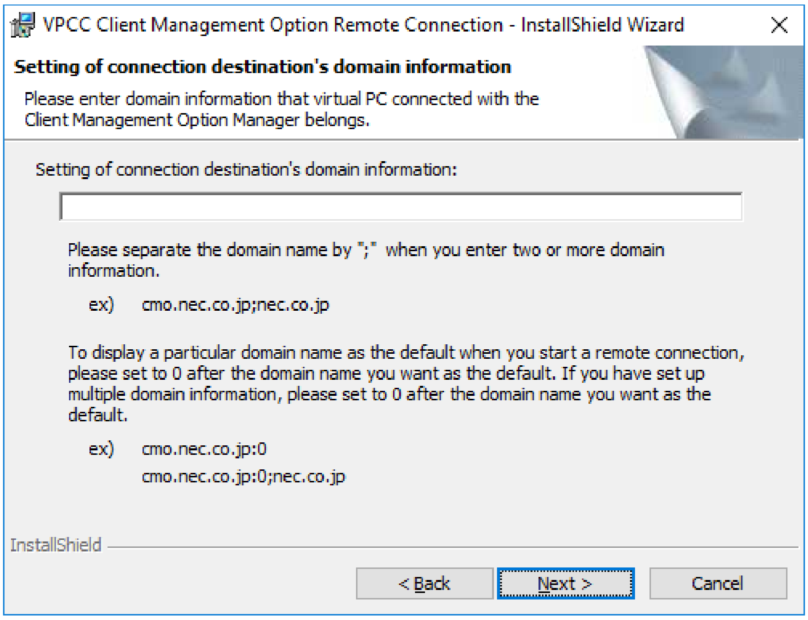
○ Local

○ DHCP server or Local

The IP address or computer name of Client Management Option Manager :

5. Type in the domain information, and then click **Next**.

   * If you selected **DHCP Server** in step 4, this step is skipped.



VPCC Client Management Option Remote Connection - InstallShield Wizard

Setting of connection destination's domain information

Please enter domain information that virtual PC connected with the Client Management Option Manager belongs.

Setting of connection destination's domain information:

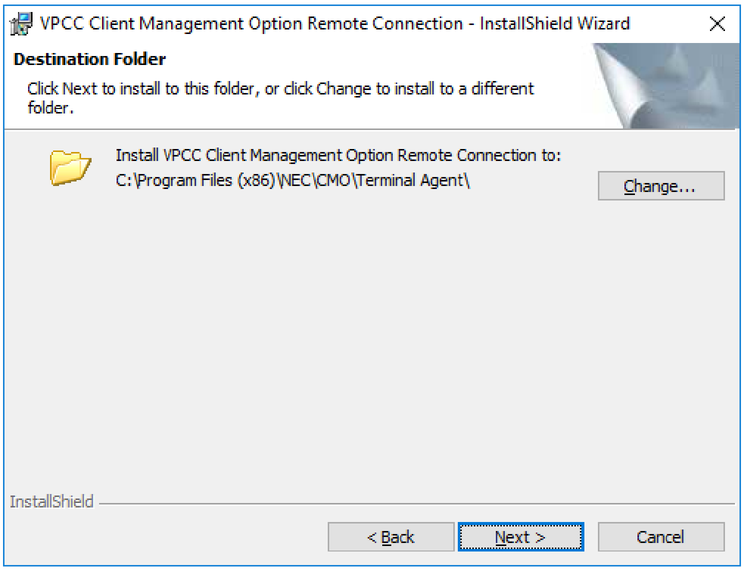
Please separate the domain name by ";" when you enter two or more domain information.

ex) cmo.nec.co.jp;nec.co.jp

To display a particular domain name as the default when you start a remote connection, please set to 0 after the domain name you want as the default. If you have set up multiple domain information, please set to 0 after the domain name you want as the default.

ex) cmo.nec.co.jp:0
cmo.nec.co.jp:0;nec.co.jp

6. Specify the installation folder, and then click **Next**.



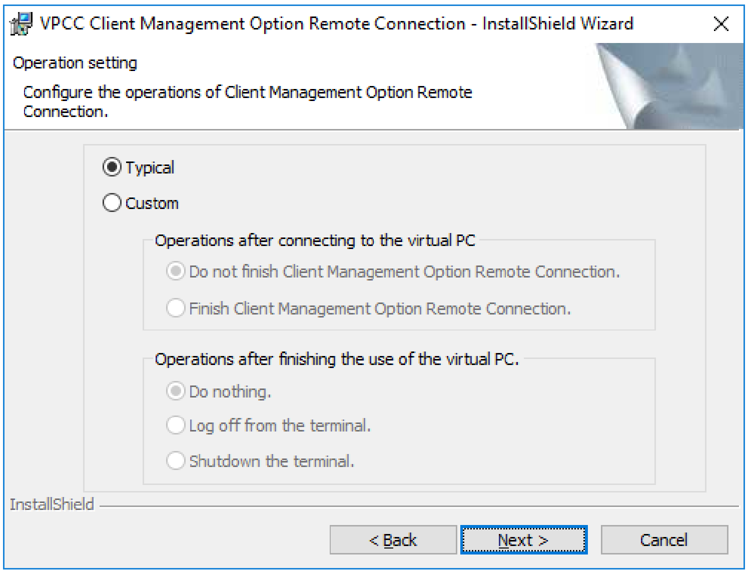
VPCC Client Management Option Remote Connection - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install VPCC Client Management Option Remote Connection to:
C:\Program Files (x86)\NEC\CMO\Terminal Agent\

7. Select the behavior of client management option remote connection and click **Next**.



VPCC Client Management Option Remote Connection - InstallShield Wizard

Operation setting

Configure the operations of Client Management Option Remote Connection.

● Typical

○ Custom

Operations after connecting to the virtual PC

● Do not finish Client Management Option Remote Connection.

○ Finish Client Management Option Remote Connection.

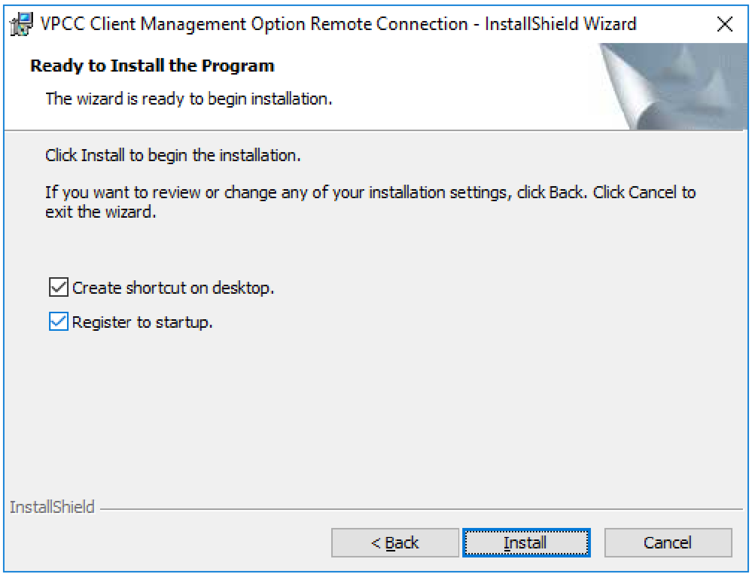
Operations after finishing the use of the virtual PC.

● Do nothing.

○ Log off from the terminal.

○ Shutdown the terminal.

8. Click **Install**.



VPCC Client Management Option Remote Connection - InstallShield Wizard

Ready to Install the Program

The wizard is ready to begin installation.

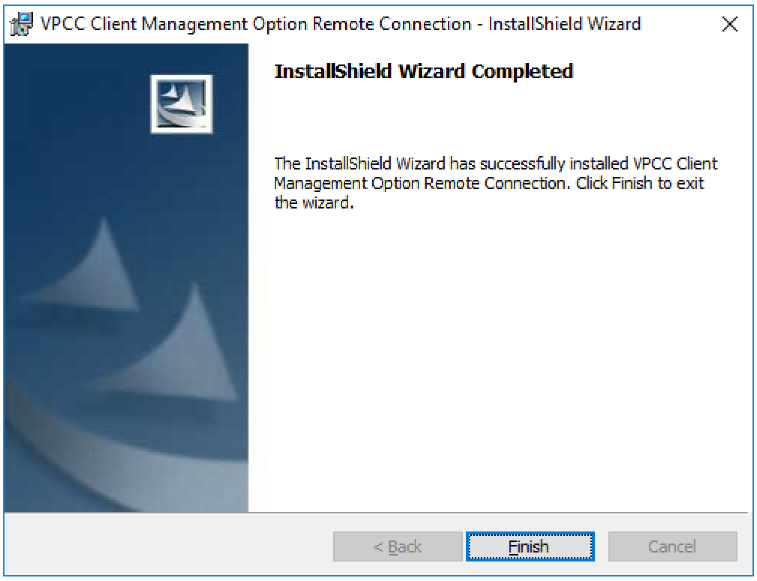
Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

☑ Create shortcut on desktop.

☑ Register to startup.

9. Click **Finish**.



VPCC Client Management Option Remote Connection - InstallShield Wizard

InstallShield Wizard Completed

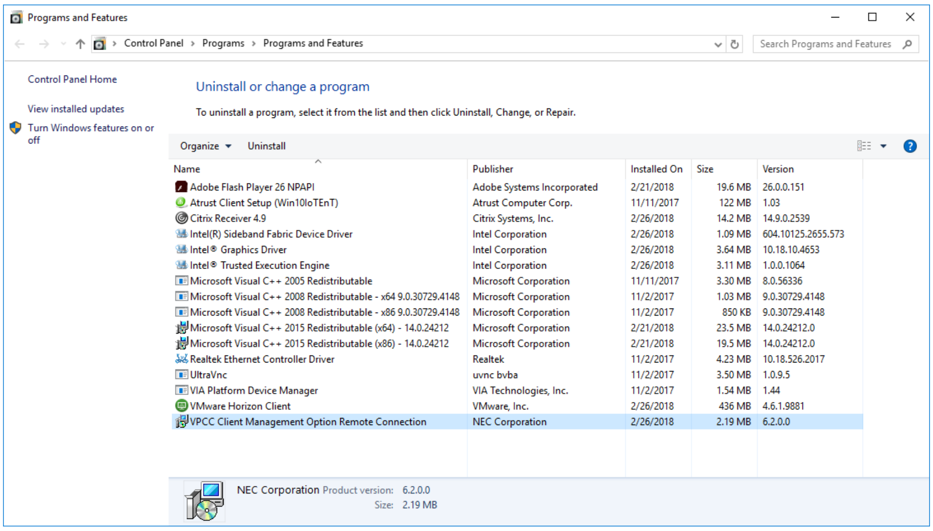
The InstallShield Wizard has successfully installed VPCC Client Management Option Remote Connection. Click Finish to exit the wizard.

10. On the desktop, move the mouse pointer to the bottom-left corner, and then right-click **Start** to open the popup menu.

11. Click **Add or Remove Programs**.

12. Make sure that **VPCC Client Management Option Remote Connection** is displayed in the program list.

   * Also make sure the version of the installed CMO Terminal Agent is correct.



Programs and Features
Control Panel › Programs › Programs and Features
Search Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Organize
Uninstall

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

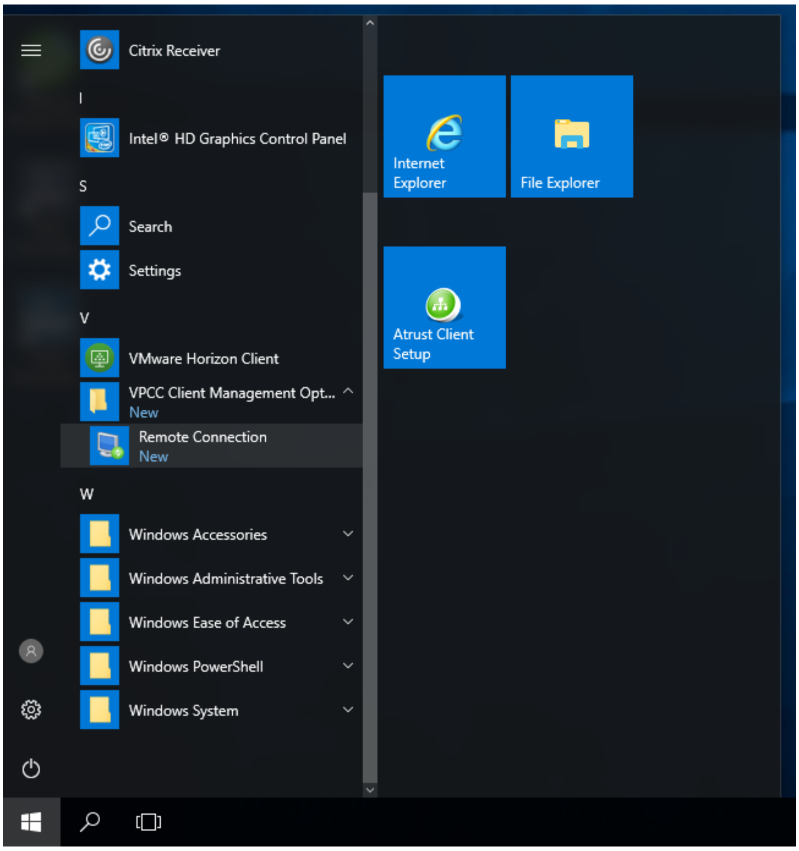
Name	Publisher	Installed On	Size	Version
Adobe Flash Player 26 NPAPI	Adobe Systems Incorporated	2/21/2018	19.6 MB	26.0.0.151
Atrust Client Setup (Win10IoTEnT)	Atrust Computer Corp.	11/11/2017	122 MB	1.03
Citrix Receiver 4.9	Citrix Systems, Inc.	2/26/2018	14.2 MB	14.9.0.2539
Intel(R) Sideband Fabric Device Driver	Intel Corporation	2/26/2018	1.09 MB	604.10125.2655.573
Intel® Graphics Driver	Intel Corporation	2/26/2018	3.64 MB	10.18.10.4653
Intel® Trusted Execution Engine	Intel Corporation	2/26/2018	3.11 MB	1.0.0.1064
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	11/11/2017	3.30 MB	8.0.56336
Microsoft Visual C++ 2008 Redistributable - x64 9.0.30729.4148	Microsoft Corporation	11/2/2017	1.03 MB	9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148	Microsoft Corporation	11/2/2017	850 KB	9.0.30729.4148
Microsoft Visual C++ 2015 Redistributable (x64) - 14.0.24212	Microsoft Corporation	2/21/2018	23.5 MB	14.0.24212.0
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.24212	Microsoft Corporation	2/21/2018	19.5 MB	14.0.24212.0
Realtek Ethernet Controller Driver	Realtek	11/2/2017	4.23 MB	10.18.526.2017
UltraVnc	uvnc bvba	11/2/2017	3.50 MB	1.0.9.5
VIA Platform Device Manager	VIA Technologies, Inc.	11/2/2017	1.54 MB	1.44
VMware Horizon Client	VMware, Inc.	2/26/2018	436 MB	4.6.1.9881
VPCC Client Management Option Remote Connection	NEC Corporation	2/26/2018	2.19 MB	6.2.0.0

NEC Corporation Product version: 6.2.0.0
Size: 2.19 MB

13. Sign out from the Administrator account.

14. Sign in as a User.

15. Wait until the CMO Terminal Agent shortcut appears on the **Start** screen.



Note CMO Terminal Agent is registered in the Startup menu when it is installed, and is automatically launched when you sign in to US320f.

13. Wireless LAN Settings

To communicate with the wireless LAN access point with US320f, it is necessary to connect the optional USB wireless LAN adapter to the main body USB port.

The Windows 10 IoT client can connect to the wireless LAN using the following security and encryption.

- **No authentication (open system) Encryption WEP**
- **Shared key encryption WEP**
- **WPA Personal (WPA - PSK) Encrypted AES and TKIP**
- **WPA 2 Personal (WPA 2 - PSK) Encrypted AES and TKIP**
- **WPA Enterprise (WPA-Enterprise) Encrypted AES and TKIP**
- **WPA2 Enterprise (WPA2-Enterprise) Encrypted AES and TKIP**
- **IEEE 802.1X encrypted WEP**

The following network authentication methods can be used.

- **EAP-PEAP(EAP-MS-CHAP v2, TLS)**
- **EAP-TLS**
- **EAP-TTLS**
- **EAP authentication method other than Microsoft**

Note Use of EAP-MD5 is not supported.

Also, in US320f, changes made when UWF (Unified Write Filter) is enabled are lost after restart. Therefore, in order to retain the wireless LAN profile, it is necessary to set the wireless LAN with UWF disabled (refer to Chapter 4 “2.9 Configuring UWF (Unified Write Filter)") However, since it is necessary to sign in with the Administrator account in order to invalidate UWF, it may be impossible for the user to set up the wireless LAN profile in the operational environment. In that case, you can register the wireless LAN profile in the UWF write protect exception to keep the wireless LAN profile implemented with the User account.

13.1 Maintaining Wireless LAN Profile

To register the wireless LAN profile in the UWF write protection exception, follow the procedure below.

1. Start US320f.
2. After signing in automatically with User account, sign out.
3. Enter the user ID and password for the Administrator account and sign in.
4. Click **Run** from the right-click menu of the start button.
5. Specify the file name and enter **cmd** in the run dialog to start the administrator command prompt.
6. Execute the following UWF command at the command prompt.
   (1) uwfmgr file add-exclusion “C:\ProgramData\Microsoft\wlansvc\Profiles\Interfaces”
   (2) uwfmgr registry add-exclusion HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\wlansvc
   (3) uwfmgr registry add-exclusion HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Wlansvc
   (4) uwfmgr registry add-exclusion HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\WwanSvc
7. Exit the command prompt and restart US320f.

13.2 IEEE 802.1X / EAP authentication

Explanation about wireless LAN authentication using Radius server compliant with IEEE 802.1X / EAP.

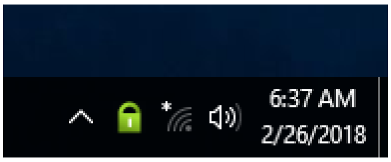
To perform IEEE 802.1X / EAP authentication, "certificate" must be used for client authentication. US320f will lose root certificates and client certificates installed when UWF (Unified Write Filter) is enabled after restart. If you want to keep the certificate after rebooting, you must register the certificate store with the UWF write protection exception. For holding the certificate, refer to Chapter 5 “14 Installing the Certificate”.

EAP-PEAP

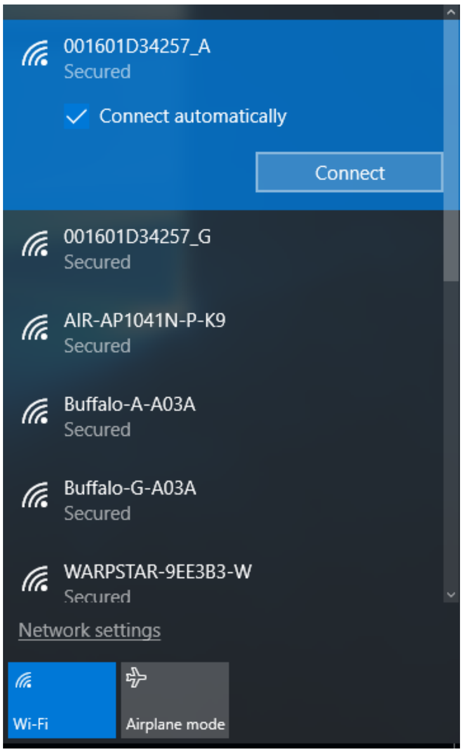
When using EAP-PEAP, it is necessary to install the root certificate in US320f and user authentication by user ID and password is necessary at the same time. To maintain the wireless LAN connection before signing in and after signing out, it is necessary to save the credentials.

Note If you are joining a domain, please set according to the environment such as "Automatically use Windows logon name and password (and domain if there is domain)".

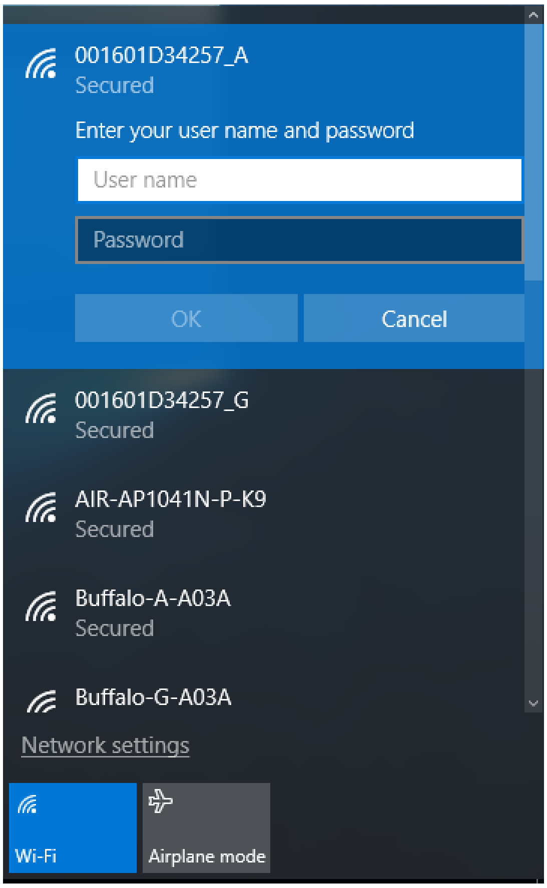
1. Start US320f.
2. Automatically sign in with the User account.
3. Connect the USB wireless LAN adapter to the USB port of US320f.
4. Click the **wireless LAN** icon in the task bar notification area at the bottom right of the screen.



5. Select the network name (SSID) to be connected and click **Connect**.



6. Enter **User name** and **Password** and click **OK**.



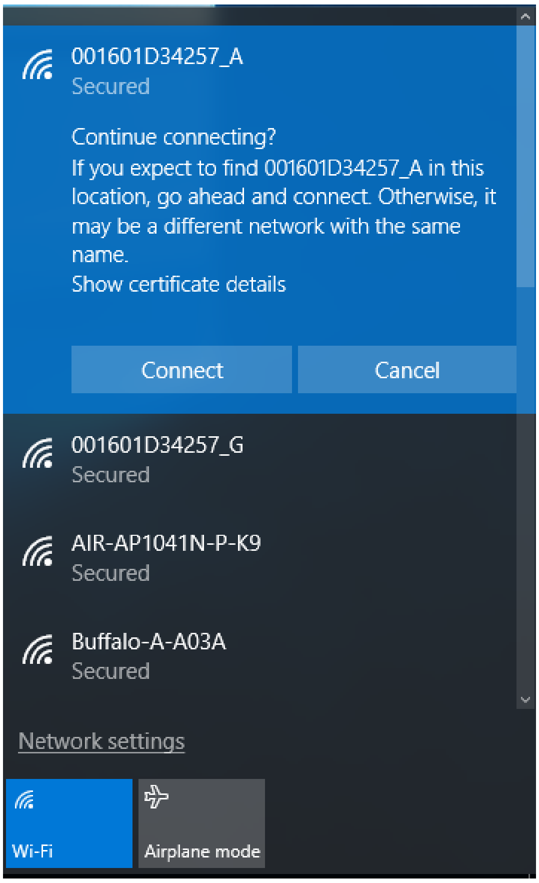
001601D34257_A
Secured

Enter your user name and password

User name

Password

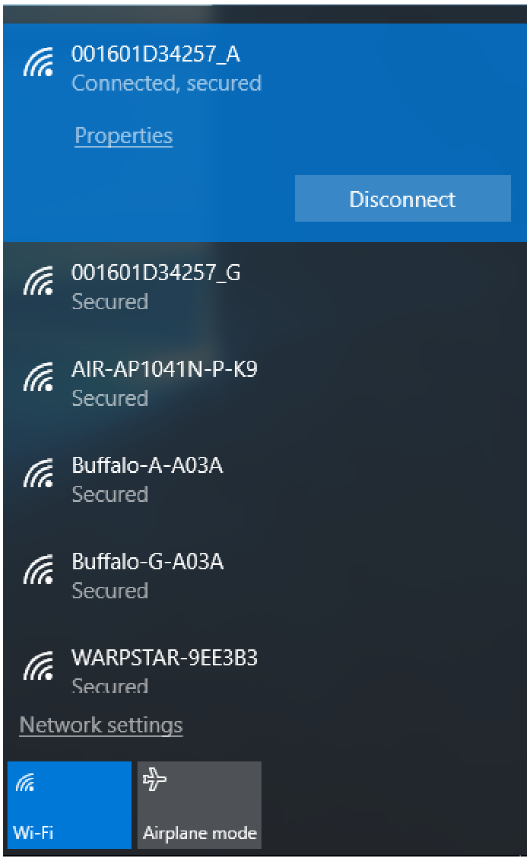
7. If a warning is displayed, click **Connect** to continue.



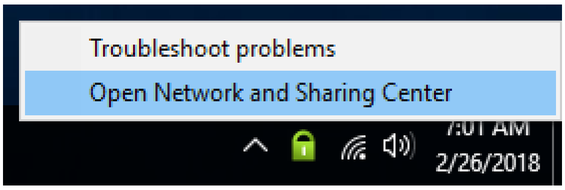
001601D34257_A
Secured

Continue connecting?
If you expect to find 001601D34257_A in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Show certificate details

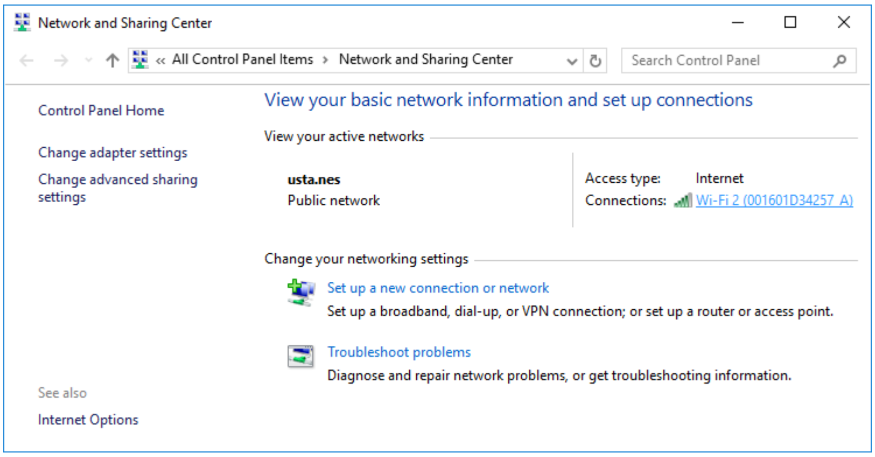
8. Confirm that the status of the network name (SSID) is displayed as **Connected, Secured**.



9. Right-click the wireless LAN icon in the task bar notification area at the bottom right of the screen and select **Open Network and Sharing Center** from the menu.



10. Click **Wi-Fi** from the **active network**.


Network and Sharing Center
« All Control Panel Items › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Internet Options

View your basic network information and set up connections

View your active networks

usta.nes
Public network

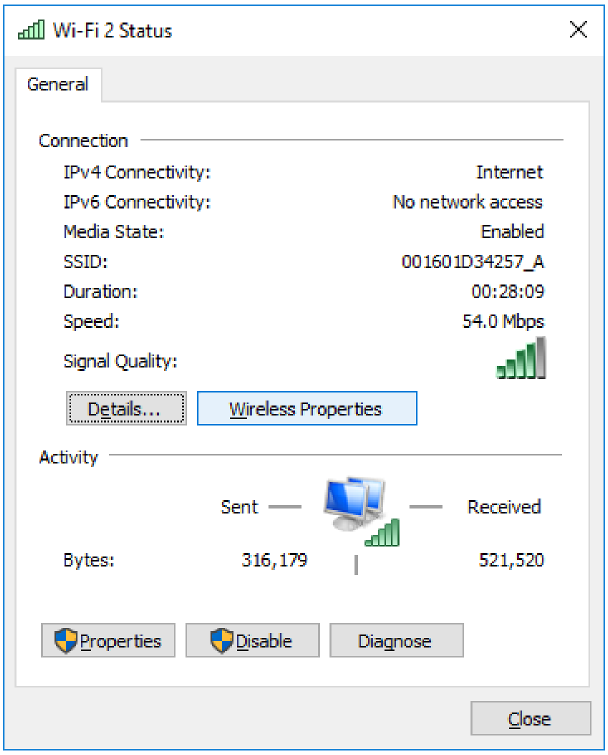
Access type: Internet
Connections: Wi-Fi 2 (001601D34257_A)

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

11. Click the **Wireless Properties** button.



Wi-Fi 2 Status

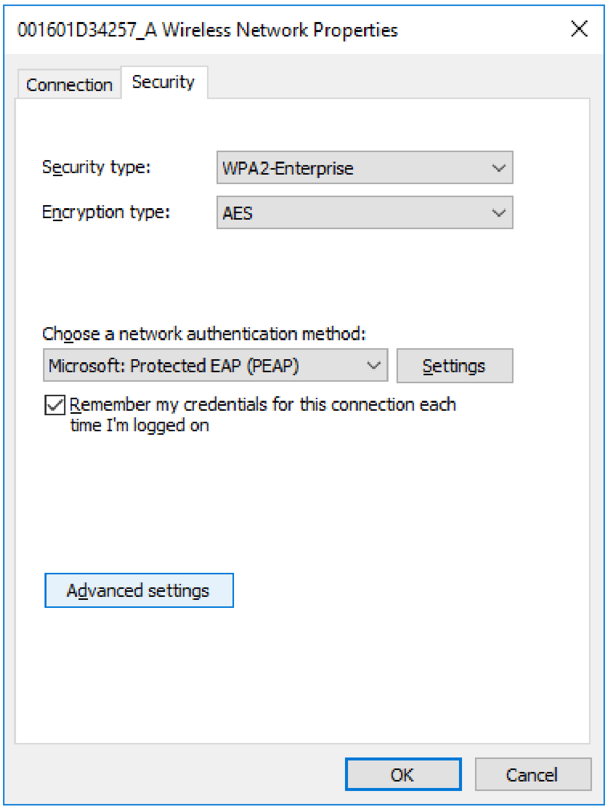
General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No network access
Media State:	Enabled
SSID:	001601D34257_A
Duration:	00:28:09
Speed:	54.0 Mbps
Signal Quality:	

Bytes: 316,179 521,520

12. Select the **Security** tab and click the **Advanced settings** button.



001601D34257_A Wireless Network Properties

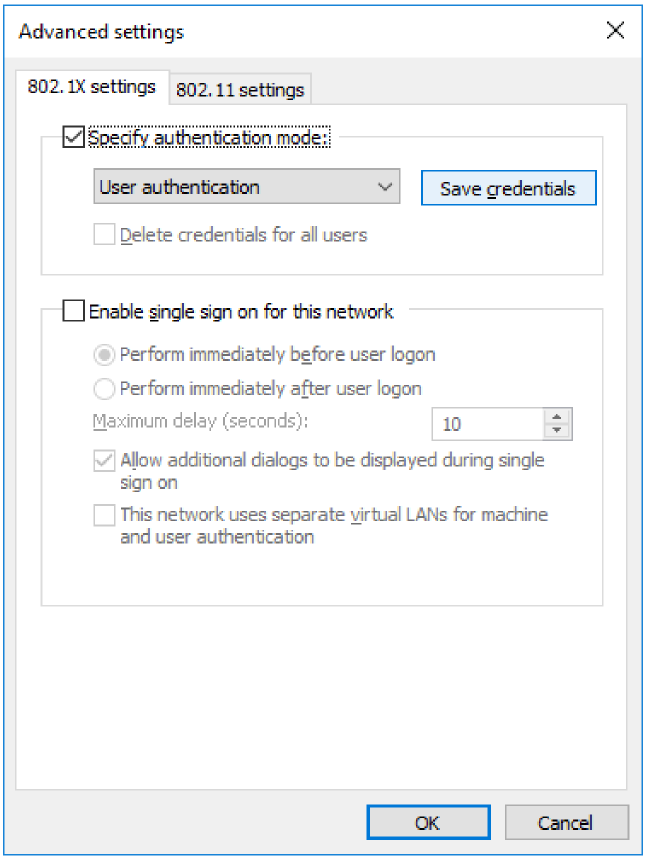
Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

13. Select the **802.1X settings** tab and click the **Save credentials** button.



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User authentication [Save credentials]

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

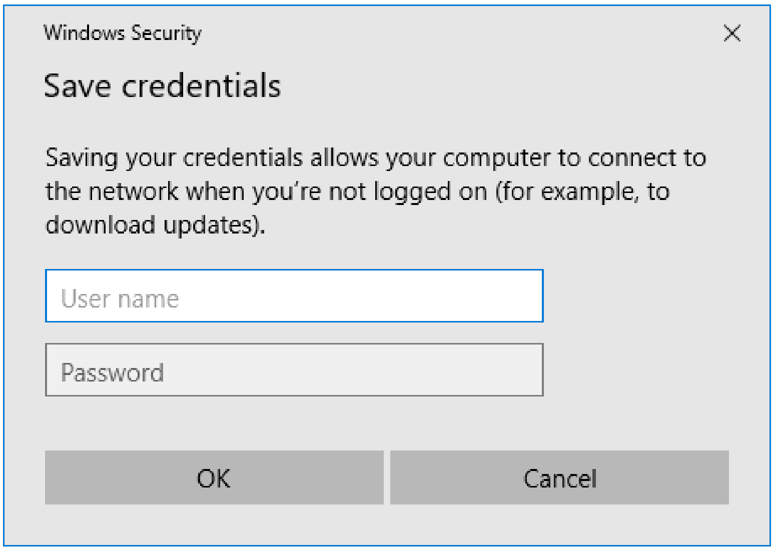
Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

[OK] [Cancel]

14. Enter **User name** and **Password** and click the **OK** button.



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

User name

Password

[OK] [Cancel]

15. Click the **OK** button to close the advanced dialog.
16. Click the **OK** button to close the wireless network properties dialog.
17. Click the **Close** button to close the Wi-Fi dialog.
18. Confirm that the wireless LAN icon in the task bar notification area at the bottom right of the screen is in the connection status.
19. Restart US320f.
20. After the automatic sign-in with the User account, confirm that the wireless LAN icon in the task bar notification area at the lower right of the screen is in the connection status.

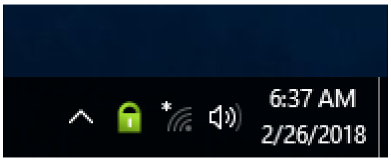
EAP-TLS

When using EAP-TLS, it is necessary to install the root certificate in US320f, and install client certificate at the same time.

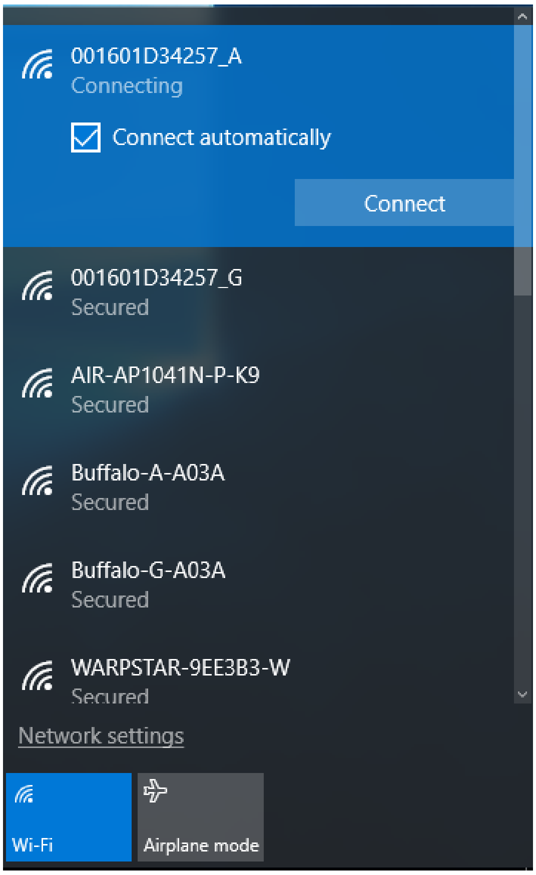
Note

Since EAP-TLS defined in IEEE defines the use of client certificate and either computer certificate or user certificate is not specified, it is also possible to use a user certificate instead of a computer certificate for EAP-TLS authentication. However, it is important to note that if you use a user certificate, you can not establish a wireless LAN connection before signing in and after signing out

1. Start US320f.
2. Automatically sign in with the User account.
3. Connect the USB wireless LAN adapter to the USB port of US320f.
4. Click the **wireless LAN** icon in the task bar notification area at the bottom right of the screen.



5. Select the network name (SSID) to be connected and click **Connect**.



001601D34257_A
Connecting

☑ Connect automatically

001601D34257_G
Secured

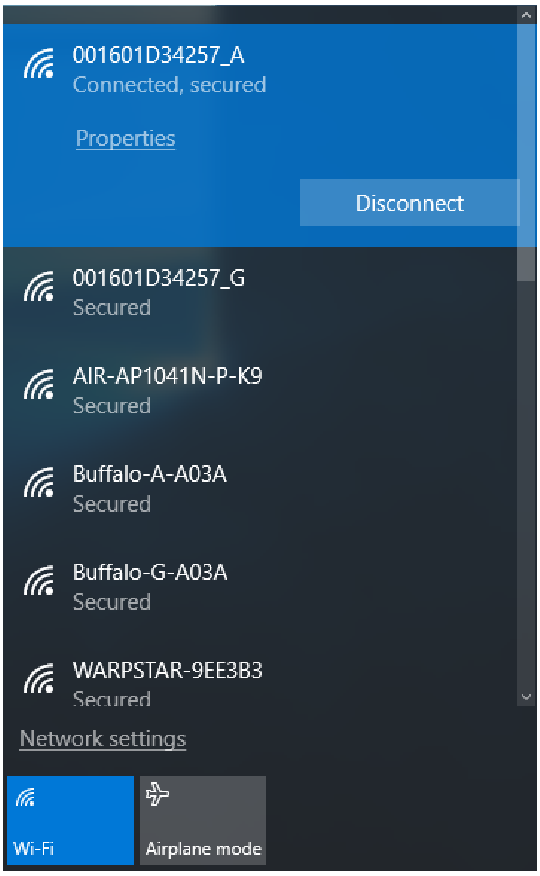
AIR-AP1041N-P-K9
Secured

Buffalo-A-A03A
Secured

Buffalo-G-A03A
Secured

WARPSTAR-9EE3B3-W
Secured

6. Confirm that **Connected, Secured** appears on the status of the network name (SSID).



001601D34257_A
Connected, secured

001601D34257_G
Secured

AIR-AP1041N-P-K9
Secured

Buffalo-A-A03A
Secured

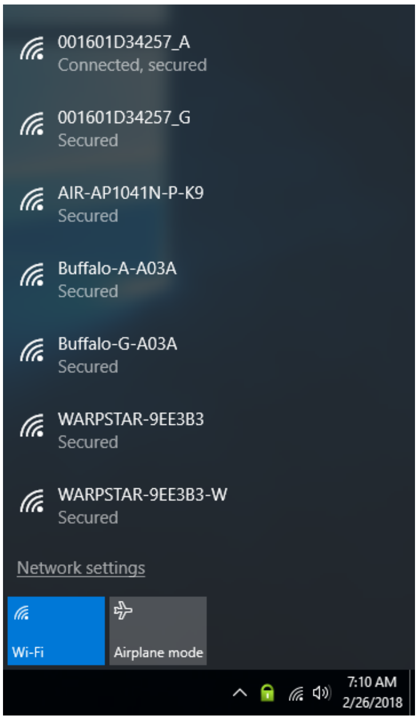
Buffalo-G-A03A
Secured

WARPSTAR-9EE3B3
Secured

13.3 Deleting a Network Profile

To delete a network profile, follow the procedure below.

1. Click the **Wireless** icon (the icon indicating the strength of radio waves) in the lower right corner of the desktop screen.



001601D34257_A
Connected, secured

001601D34257_G
Secured

AIR-AP1041N-P-K9
Secured

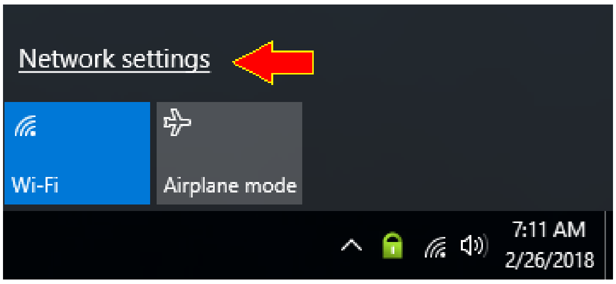
Buffalo-A-A03A
Secured

Buffalo-G-A03A
Secured

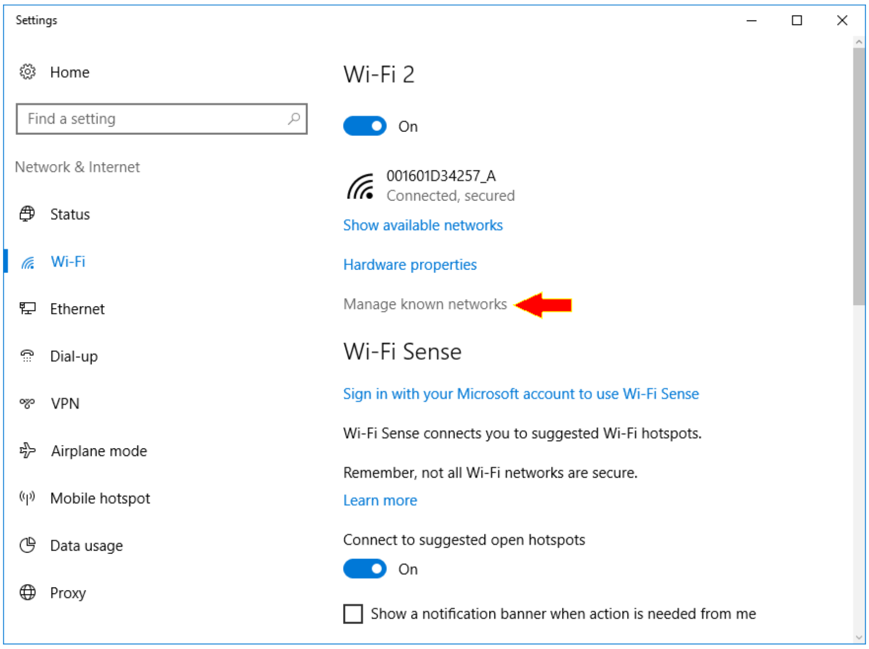
WARPSTAR-9EE3B3
Secured

WARPSTAR-9EE3B3-W
Secured

2. Click **Network Settings**.



3. Click **Manage Known Networks**.



Settings

Home

Find a setting

Network & Internet

Status

Wi-Fi

Ethernet

Dial-up

VPN

Airplane mode

Mobile hotspot

Data usage

Proxy

Wi-Fi 2

On

001601D34257_A
Connected, secured

Show available networks

Hardware properties

Manage known networks

Wi-Fi Sense

Sign in with your Microsoft account to use Wi-Fi Sense

Wi-Fi Sense connects you to suggested Wi-Fi hotspots.

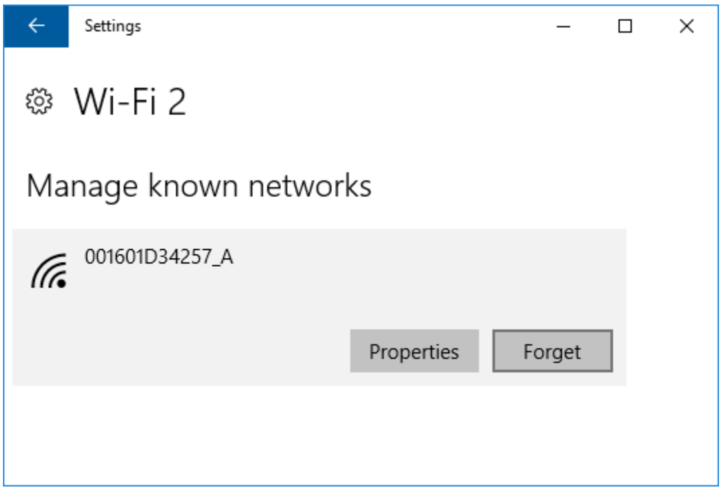
Remember, not all Wi-Fi networks are secure.
Learn more

Connect to suggested open hotspots

On

□ Show a notification banner when action is needed from me

4. When **Network** is displayed, select the network name (SSID) to be deleted and click the **Forget** button.



Settings

Wi-Fi 2

Manage known networks

001601D34257_A

Properties Forget

5. The network profile is deleted.

14. Installing the Certificate

US320f protects the thin client from erroneous writing to the flash memory by UWF (Unified Write Filter). Writing to flash is valid as long as the thin client is active, but it will be lost if the thin client is restarted or shut down. Certificates installing UWF in a valid state are lost when you restart or shut down the thin client.

14.1 Retention of Certificate

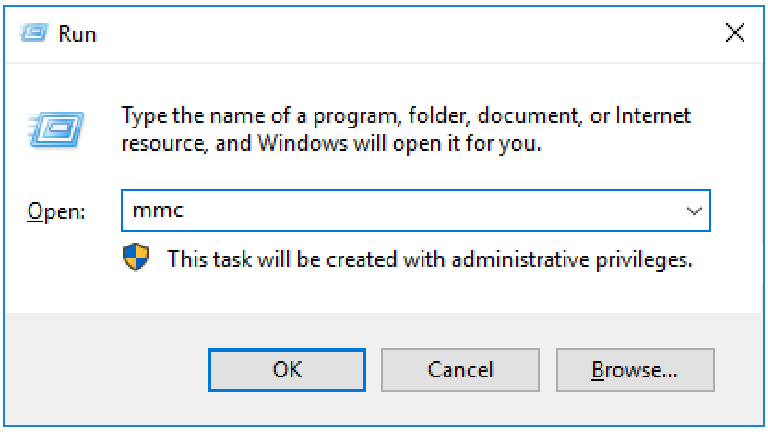
To register the root certificate and computer certificate in the UWF write protect exception, follow the procedure below.

1. Start US320f.
2. After signing in automatically with User account, sign out.
3. Enter the user ID and password for the Administrator account and sign in.
4. Click **Run** from the right-click menu of the start button.
5. Specify the file name and enter **cmd** in the run dialog to start the administrator command prompt.
6. Execute the following UWF command at the command prompt.
   (1) uwfmgr file add-exclusion “C:\Windows\System32\Microsoft\Protect”
   (2) uwfmgr file add-exclusion “C:\ProgramData\Microsoft\Crypto”
   (3) uwfmgr registry add-exclusion HKEY_LOCAL_MACHINE\SOFTWARE \Microsoft\SystemCertificates
7. Exit the command prompt and restart US320f.

14.2 Installing the root certificate

For clients which joined the domain, root certificates are automatically installed in "trusted root certification authorities" when joining a domain. This section describes how to install the root certificate in US320f which does not participate in the domain. If you have not registered the certificate store as a UWF write protection exception, follow the steps below after disabling UWF.

1. Start US320f.
2. After signing in automatically with User account, sign out.
3. Enter the user ID and password for the Administrator account and sign in.
4. Click **Run** from the right-click menu of the start button. Enter **mmc** and click the **OK** button.



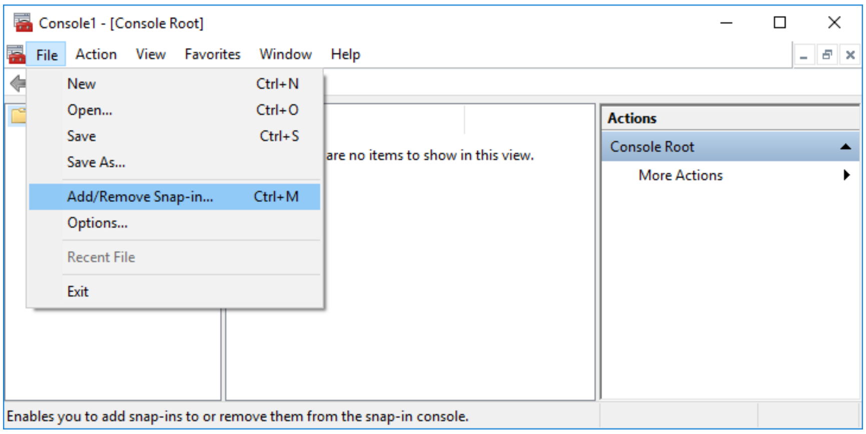
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

This task will be created with administrative privileges.

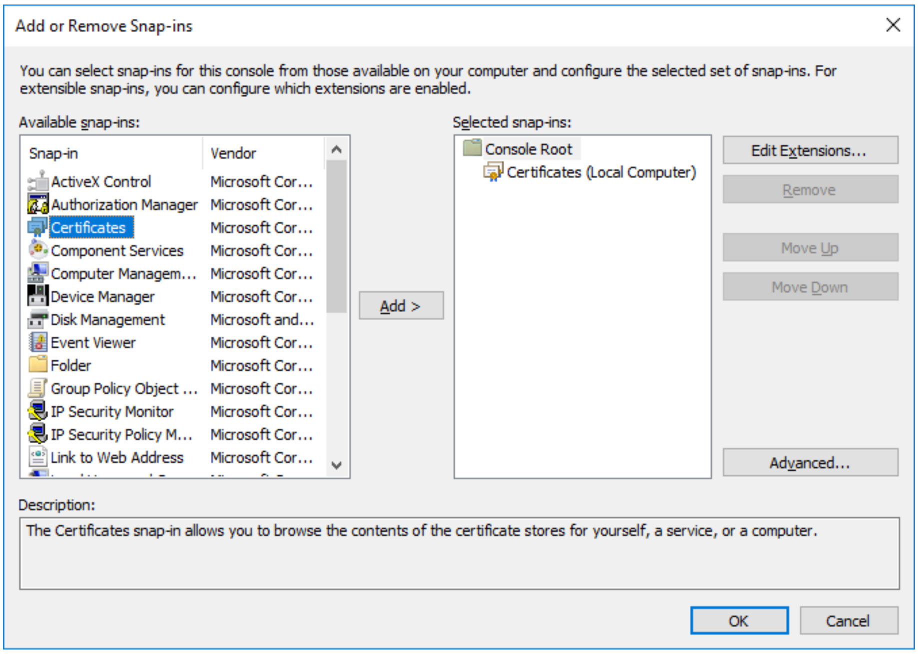
5. On the Console window, click the **File** menu to select **Add/Remove Snap-in**.



are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

6. On the **Add or Remove Snap-ins** window, click **Certificates** > **Add** > **Computer account** > **Local computer** > **Finish** > **OK** to add the Certificates snap-in.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

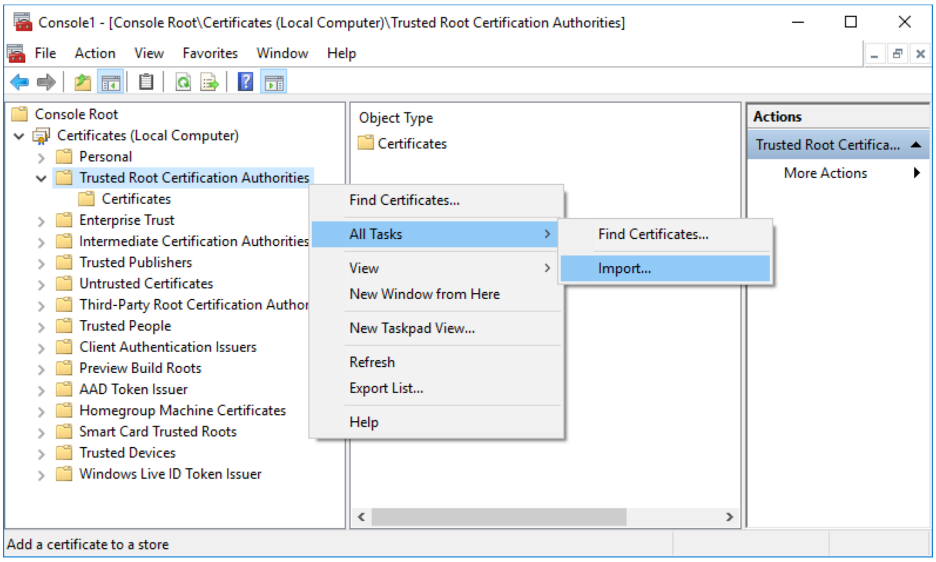
Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

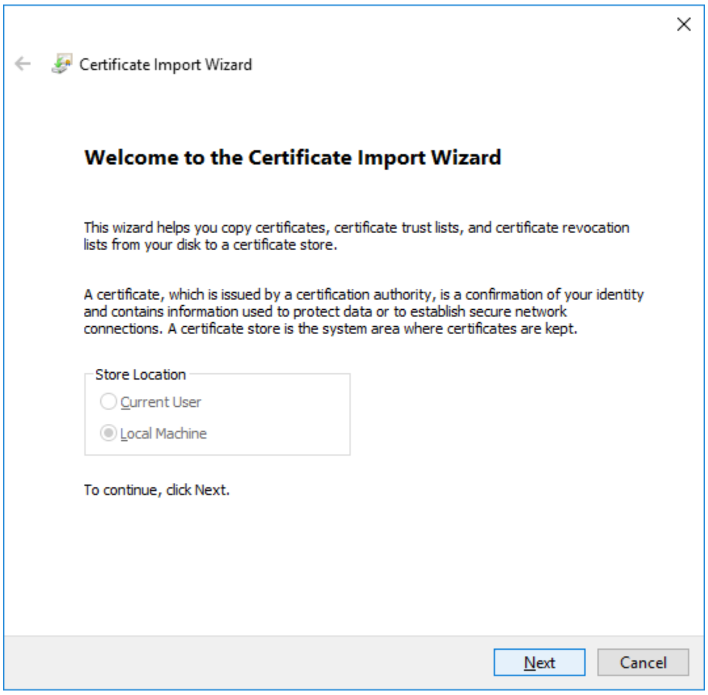
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

7. 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. In the console window, click the **File** menu and select **Add / Remove Snap-in**.


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities]
File Action View Favorites Window Help
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Author
Trusted People
Client Authentication Issuers
Preview Build Roots
AAD Token Issuer
Homegroup Machine Certificates
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer
Object Type
Certificates
Find Certificates...
All Tasks
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Find Certificates...
Import...
Actions
Trusted Root Certifica...
More Actions

Add a certificate to a store

8. The **Certificate Import Wizard** will be launched. Click the **Next** button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

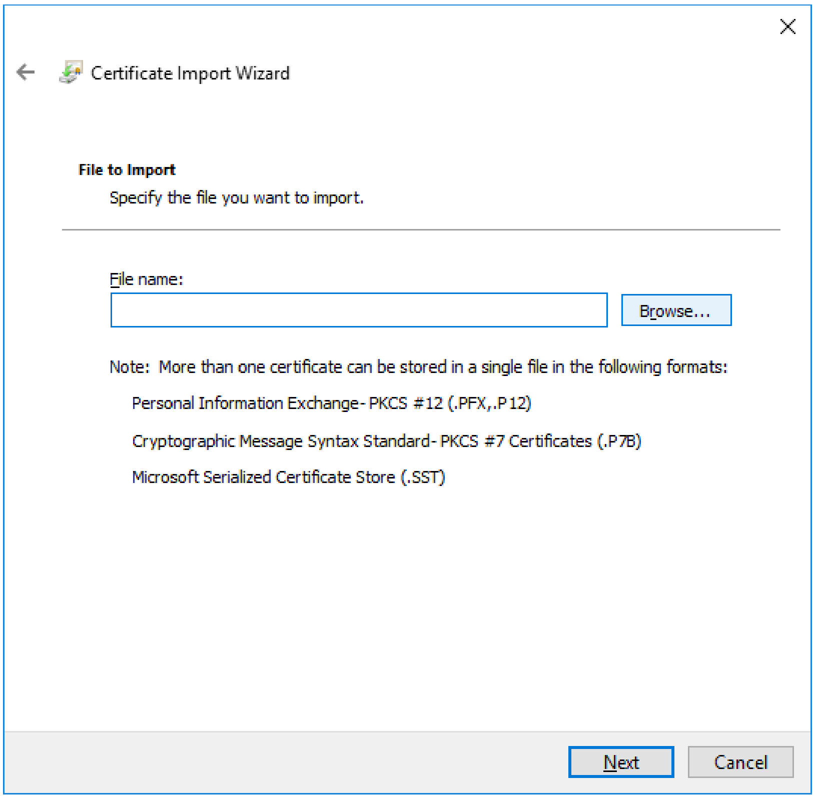
Store Location

○ Current User

● Local Machine

To continue, click Next.

9. Click the **Browse** button.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

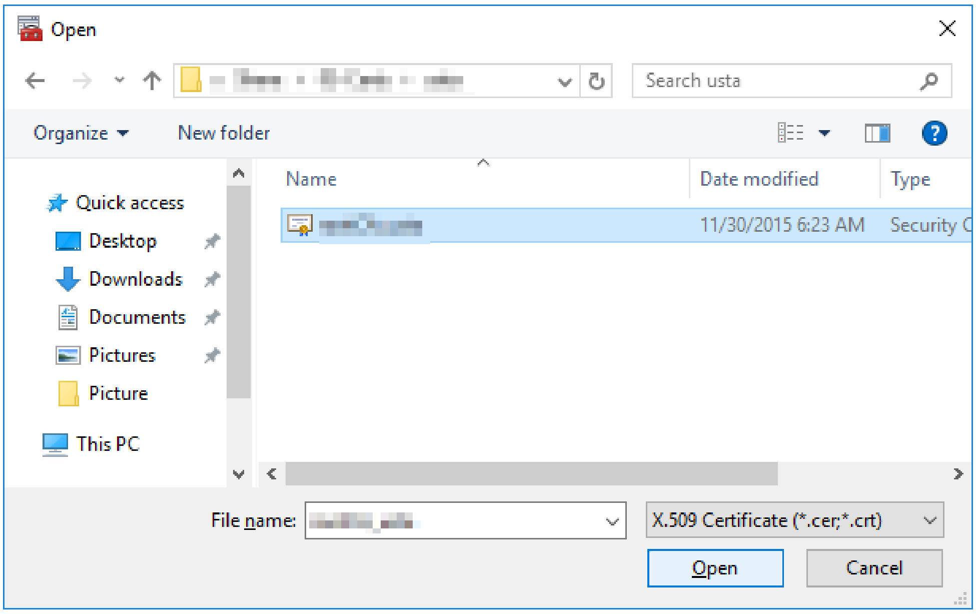
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

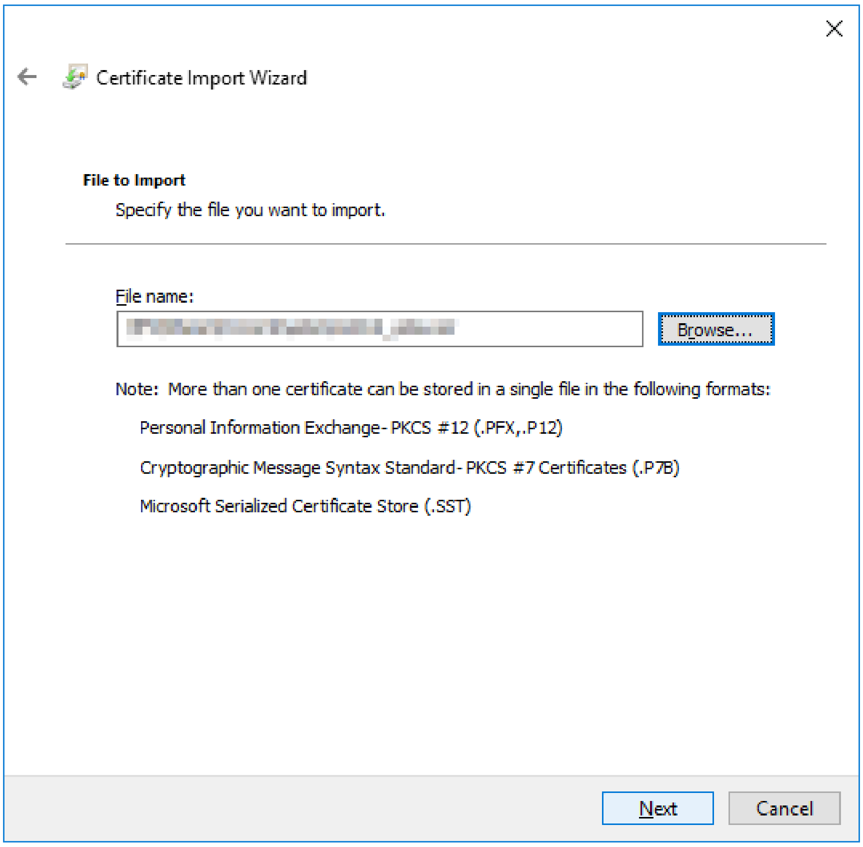
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

10. Select the root certificate file issued by the trusted root certification authority and click the **Open** button.



11. Click the **Next** button.



File to Import

Specify the file you want to import.

File name:

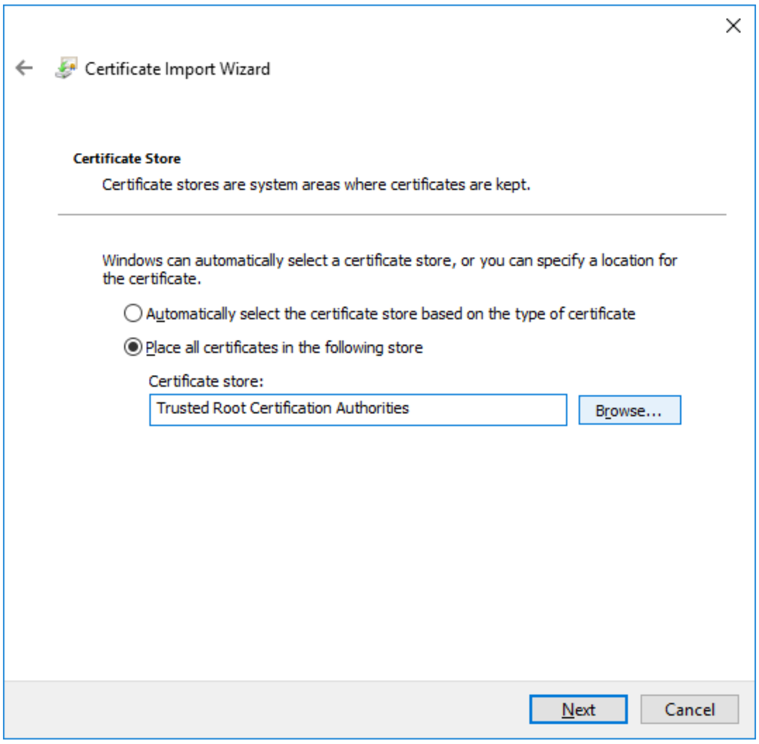
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

12. Click the **Browse** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

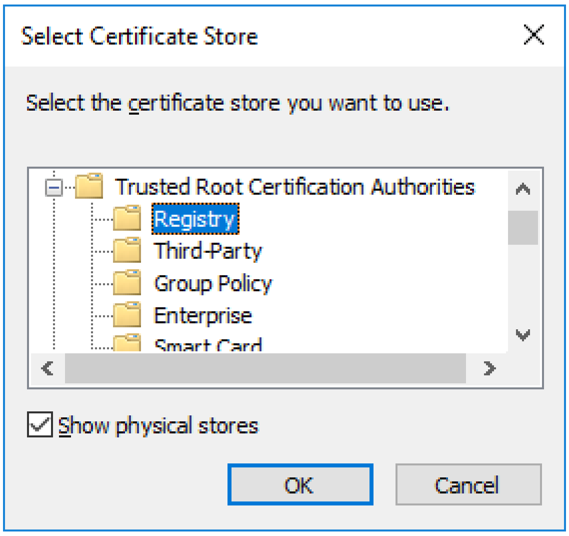
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

13. Activate the **Show physical store** checkbox, select **Trusted Root Certification Authorities** - **Registry** and click the **OK** button.

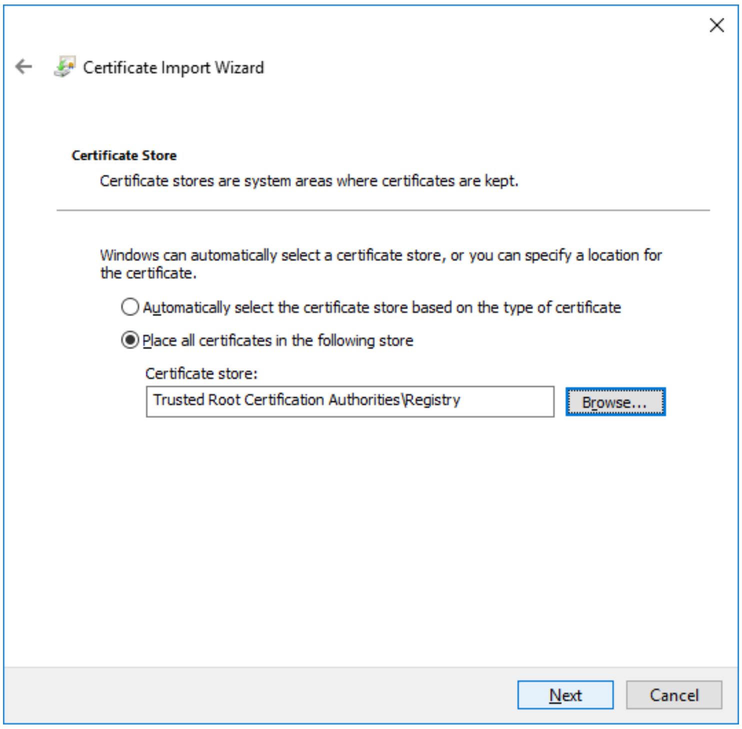


Select Certificate Store

Select the certificate store you want to use.

☑ Show physical stores

14. Click the **Next** button.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

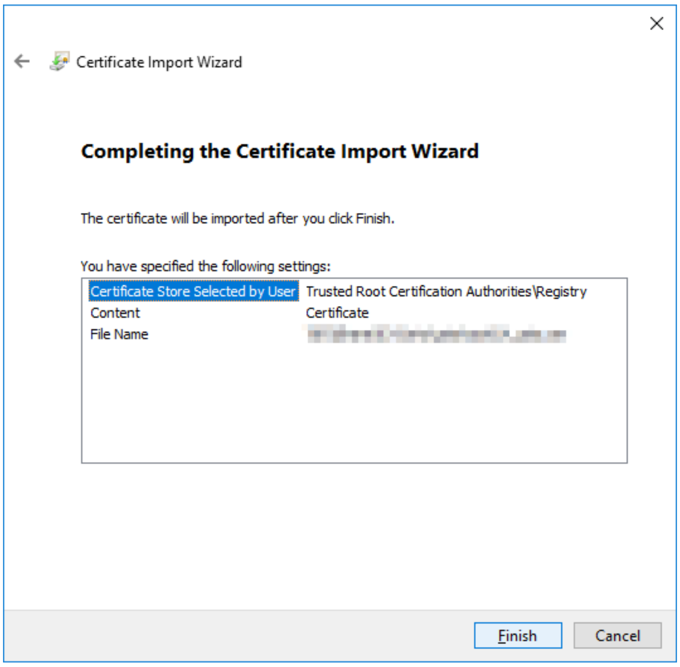
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities\Registry

15. Click the **Finish** button.



Certificate Import Wizard

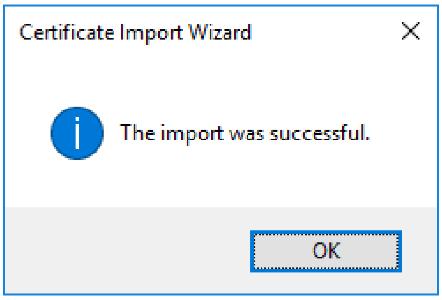
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities\Registry
Content	Certificate
File Name	[redacted]

16. Click the **OK** button to close the dialog.



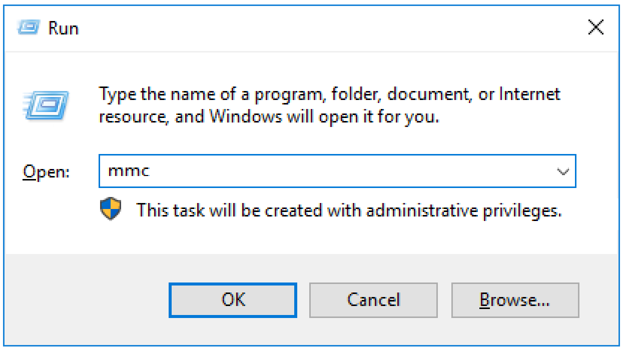
Certificate Import Wizard

The import was successful.

14.3 Installation of Computer Certificate

Below is a description of how to install a computer certificate in US320f. If you have not registered the certificate store as an UWF write protection exception, follow the steps below after disabling UWF.

1. Start US320f.
2. After signing in automatically with User account, sign out.
3. Enter the user ID and password for the Administrator account and sign in.
4. Enter **mmc** and click the **OK** button

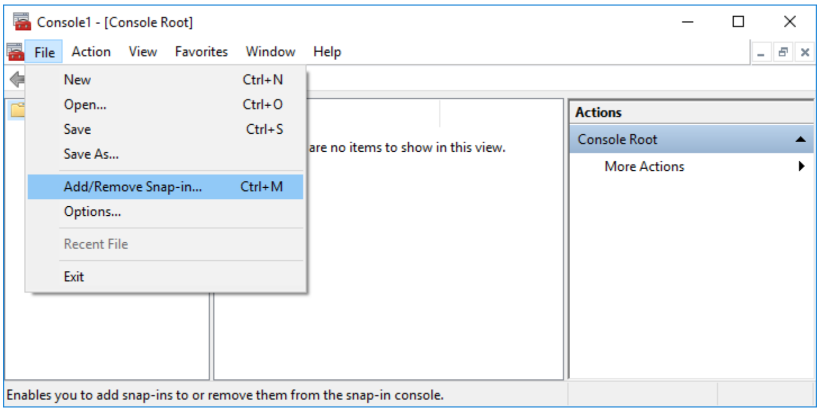


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mmc

This task will be created with administrative privileges.

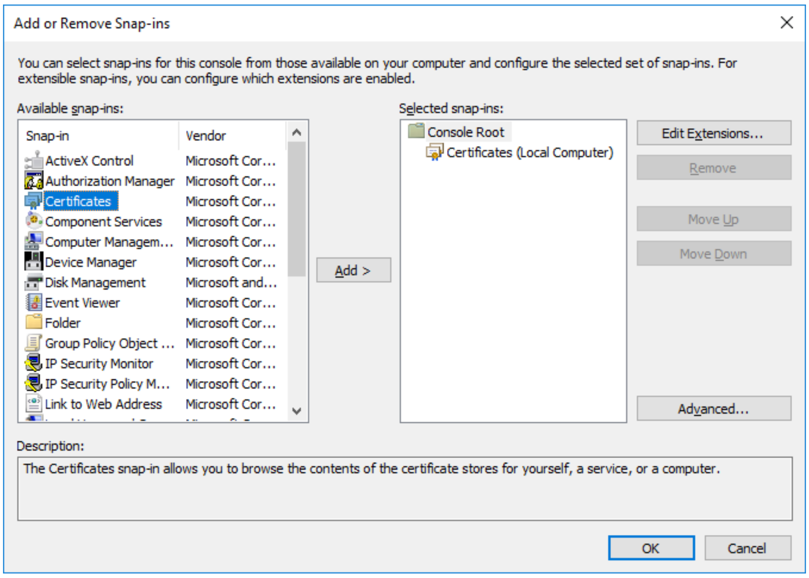
5. In the console window, click the **File** menu and select **Add / Remove Snap-in**.



are no items to show in this view.

Enables you to add snap-ins to or remove them from the snap-in console.

6. In **Add / Remove Snap-in**, click **Certificate** > **Add** > **Computer Account** > **Local Computer** > **Finish** > **OK** to add the **Certificates** snap-in.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates (Local Computer)

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

7. In the console window, click to expand the Certificates group tree, right click on **Person** > **Certificate** and select **All Tasks** > **Import** from the menu.
8. The **Certificate Import Wizard** will be launched. Click the **Next** button.
9. Click the Browse button and select the computer certificate file issued by the Trusted Root Certification Authority.
10. Click the **Next** button.
11. Click the **Browse** button.
12. Activate the **Show physical store** checkbox.
13. Select **Personal** and double click.
14. Select **Registry** and click the **OK** button.
15. Click the **Next** button.
16. Click the **OK** button to close the dialog.

NEC Express5800 Series
US320f

6

Chapter 6 System Administration

This chapter contains local and remote system administration information to help you perform the routine tasks needed to maintain your thin client environment.

1. Using Atrust Device Manager (ADM) Software for Remote Administration

Atrust Device Manager™ (ADM) servers provide network management services to thin clients, allowing complete user-desktop control through features such as shortcut creation, firmware updates, snapshot capture for mass deployment, remote shadow, reboot, shutdown, and Wake-on-LAN). By using ADM, you can manage all of your network devices from one simple-to-use console.

You can download Atrust Device Manager from the following website:

http://www.58support.nec.co.jp/global/download/

If thin clients that have ACS installed are managed and registered on the ADM server, the administrative status becomes effective and it can not be detected from other ADM servers. This is a security specification to make it inaccessible from a malicious server. If a thin client is not registered as an ADM server management target, it may be detected from an unintended malicious server and the setting may be changed. Therefore, make sure that the thin client in the production environment is registered as managed by the ADM server (detected from the ADM server), or if you do not use the ADM server, enable stealth mode of ACS.

Important

Care is required when migrating a thin client in which ACS was configured in the kitting environment to the production environment. In this case, you need to remove this thin client information from the kitting environment ADM server. If this operation is not performed, the production environment ADM server cannot register this thin client.

Note also that in Reset Mode, not only the ACS managed status, but also all ACS settings are initialized. For details about the Reset Mode, see Chapter 6, "2.2 Restoring Atrust Client Setup Settings"

Note with care that the production environment ADM server executes "Pull Settings" after detecting the thin client. As a result, the thin client ACS settings are synchronized to the ADM server and overwrite the settings on the ADM server side.

Note

- The registration information in Thin Client is not removed when the thin client is removed by ADM in the condition that thin client is disconnected from network. In this case you need to execute **Reset Mode** at Thin Client.
- Even if **Reset Mode** is executed at the Thin Client, registration information on ADM side isn't updated. Administrators need to remove the Thin Client at ADM side.

2. Restoring Settings

Depending on the default settings you want to restore on the thin client, you can:

- Use the BIOS to restore default values for all the items in the BIOS setup utility. (See Chapter 6, "2.1 Restoring BIOS Settings".
- Reset the settings made by Atrust Client Setup or Atrust Device Manager to restore the system to its factory defaults. (See Chapter 6, "2.2 Restoring Atrust Client Setup Settings".)
- Re-image the thin client to restore all factory default settings by using the Atrust Recovery USB Disk Creator or Atrust Device Manager. (See Chapter 6, "2.3 Imaging Devices with Atrust Recovery USB Disk Creator" and Chapter 6, "1. Using Atrust Device Manager (ADM) Software for Remote Administration".

Preparing to re-image

The thin client that runs Windows 10 IoT Standard can only be returned to factory defaults by re-imaging the thin client (the same process used when upgrading the firmware). The re-imaging process requires:

- **Imaging software**

  US320f provides two imaging software products to re-image your thin client that runs Windows 10 IoT Standard:

  - Atrust Recovery USB Disk Creator™

    Recommended for smaller environments. (See Chapter 6, "2.3 Imaging Devices with Atrust Recovery USB Disk Creator".)

  - Atrust Device Manager™

    Recommended for larger environments. (See Chapter 6, "1. Using Atrust Device Manager (ADM) Software for Remote Administration".)

Important

Thin client has been activated at the factory. But if, by using Atrust Device Manager (ADM) or Atrust Recovery USB Disk Creator, thin client firmware is updated or snapshot is installed, activation (license activation) is also needed. Please be careful. Please refer to Chapter 6, "4 Activating US320f" for more details about activation.

2.1 Restoring BIOS Settings

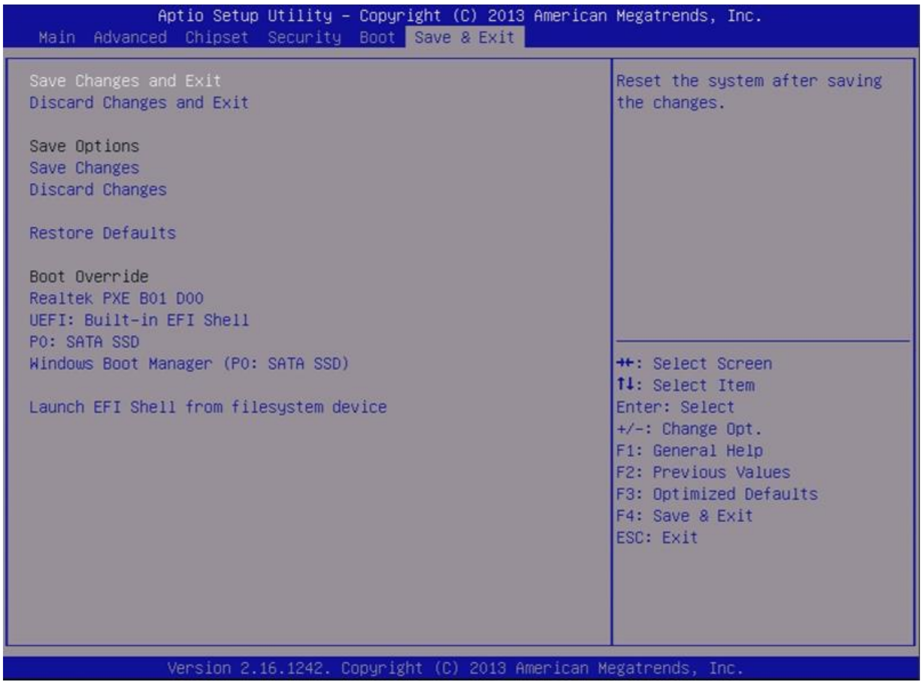
When power is turned on, the NEC logo appears briefly. Press the <DEL> key while this screen is displayed to start SETUP.

Important **The factory-set BIOS settings may differ from the restored settings.**

Restore the BIOS settings as follows:

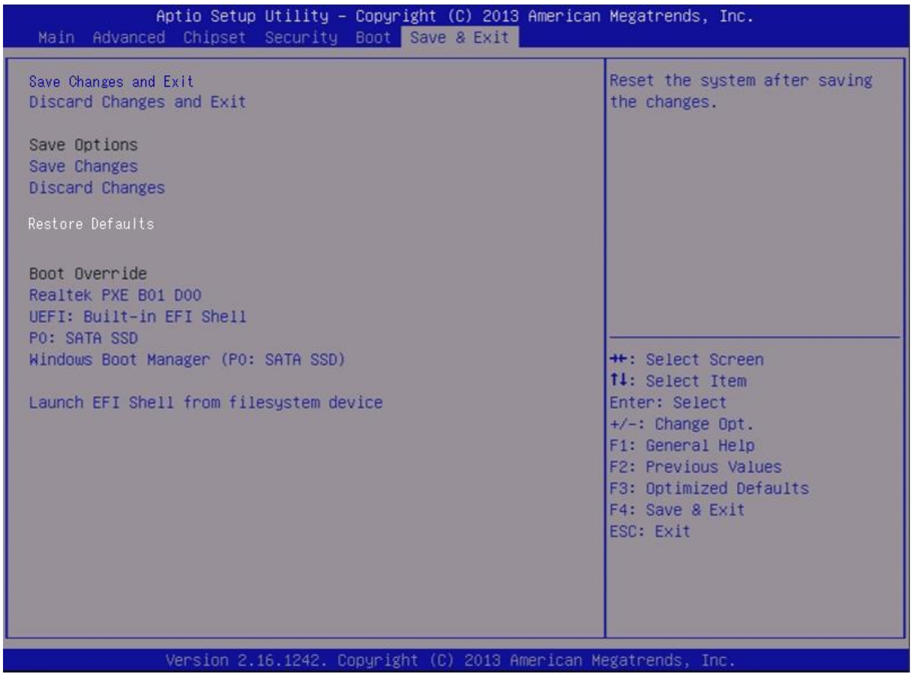
1. Restart your US320f.
2. Press the **<DEL>** key on the keyboard while the NEC logo is displayed on the screen.

3. Move to the **Save & Exit** menu of BIOS Setup.



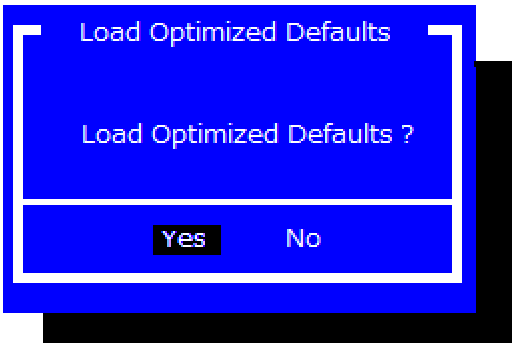
```
              Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

 Save Changes and Exit                              Reset the system after saving
 Discard Changes and Exit                           the changes.

 Save Options
 Save Changes
 Discard Changes

 Restore Defaults

 Boot Override
 Realtek PXE B01 D00
 UEFI: Built-in EFI Shell
 P0: SATA SSD
 Windows Boot Manager (P0: SATA SSD)                →←: Select Screen
                                                    ↑↓: Select Item
 Launch EFI Shell from filesystem device            Enter: Select
                                                    +/-: Change Opt.
                                                    F1: General Help
                                                    F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

               Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

4. Select **Restore Defaults**, and press <**Enter>** key.



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
 Main  Advanced  Chipset  Security  Boot  Save & Exit

Save Changes and Exit                          Reset the system after saving
Discard Changes and Exit                       the changes.

Save Options
Save Changes
Discard Changes

Restore Defaults

Boot Override
Realtek PXE B01 D00
UEFI: Built-in EFI Shell
P0: SATA SSD                                   
Windows Boot Manager (P0: SATA SSD)            →←: Select Screen
                                               ↑↓: Select Item
Launch EFI Shell from filesystem device        Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

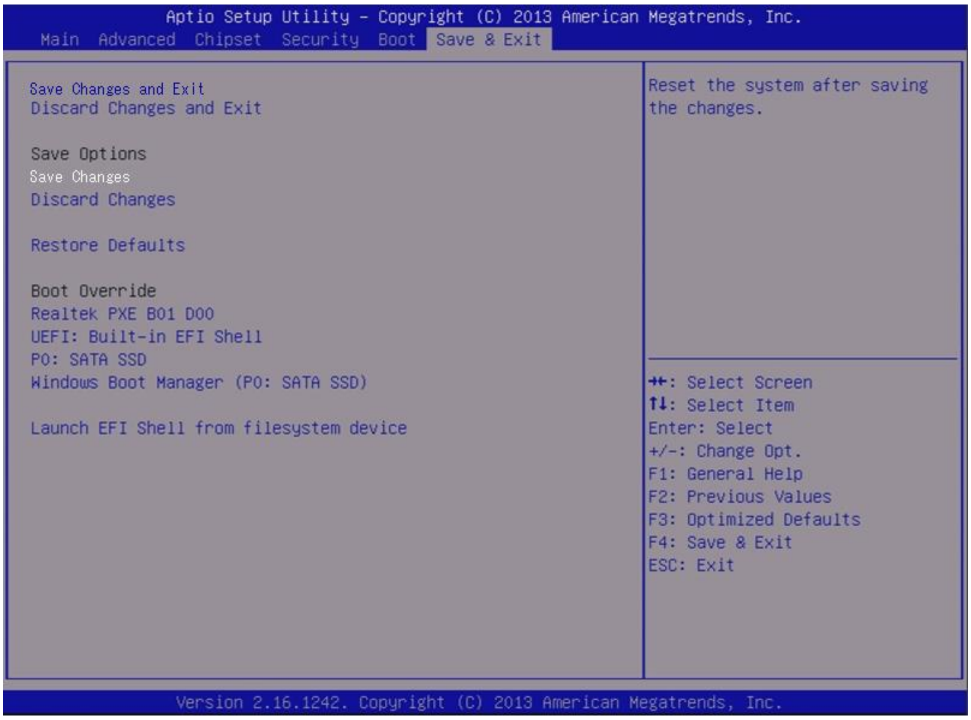
5. A confirmation message "Load Optimized Defaults?" appears. Select **Yes**, and then press <**Enter**> key.



Load Optimized Defaults

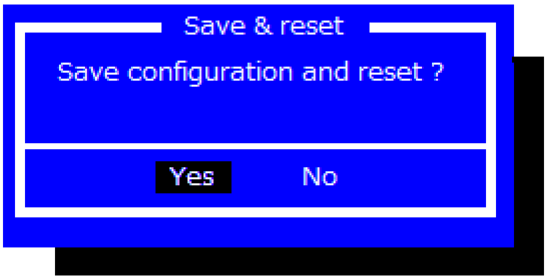
Load Optimized Defaults ?

6. Select **Save Changes and Exit**, and then press <**Enter**> key.



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
 Main  Advanced  Chipset  Security  Boot  Save & Exit

Save Changes and Exit                          Reset the system after saving
Discard Changes and Exit                       the changes.

Save Options
Save Changes
Discard Changes

Restore Defaults

Boot Override
Realtek PXE B01 D00
UEFI: Built-in EFI Shell
P0: SATA SSD                                   
Windows Boot Manager (P0: SATA SSD)            →←: Select Screen
                                               ↑↓: Select Item
Launch EFI Shell from filesystem device        Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
```

7. A confirmation message "Save configuration and reset?" appears. Select **Yes**, and then press <**Enter**> key.



Save & reset

Save configuration and reset ?

8. US320f restarts with the restored BIOS settings.

2.2 Restoring Atrust Client Setup Settings

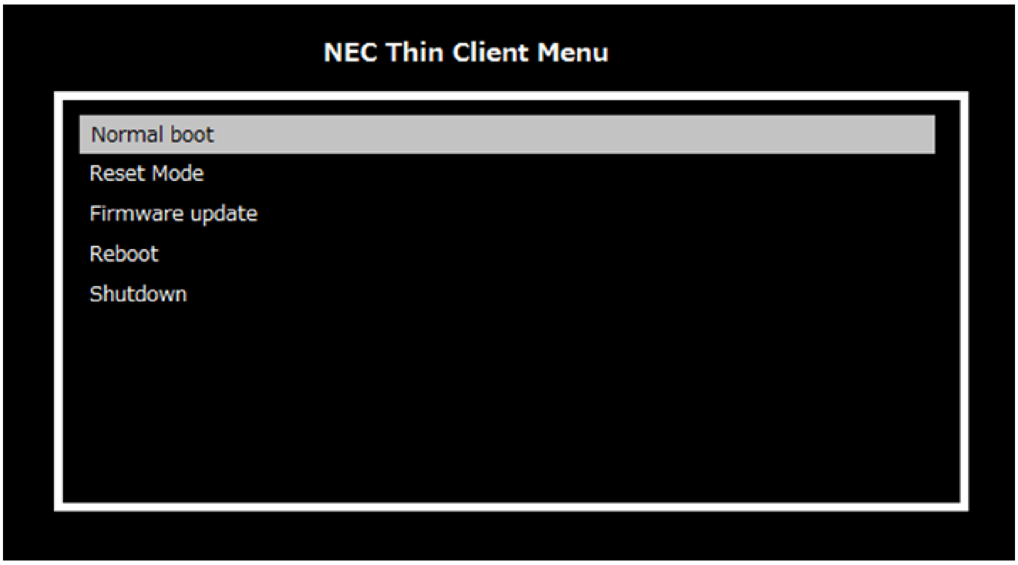
Reset Mode enables you to restore settings under Atrust Client Setup to the factory defaults. Additionally, it also releases a managed US320f from the management of Atrust Device Manager, a management console developed by Atrust for remote and mass client management.

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

Note If your US320f is subject to management by a specified Atrust Device Manager, it cannot be managed from another Atrust Device Manager. If your server environment or other settings have been changed and you want to release your US320f from being managed by Atrust Device Manager, use **Reset Mode** on the NEC Thin Client Menu or Atrust Device Manager. For detailed information, refer to the user's guide of Atrust Device Manager.

To reset Atrust Client Setup settings, do the following:

1. Restart your US320f.
2. During the POST (Power-On Self-Test) period, press <**Esc**> key on the keyboard to enter NEC Thin Client Menu.

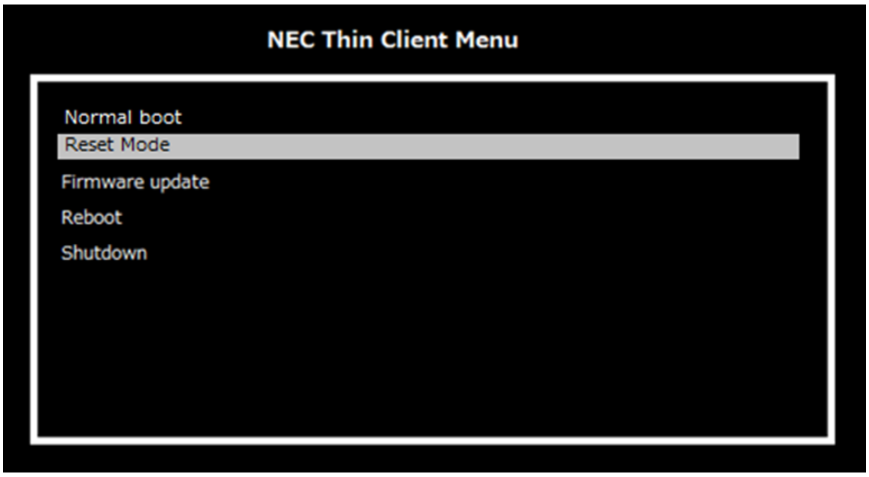


Note Five options are available on NEC Thin Client Menu: **Normal boot**, **Reset Mode**, **Firmware Update**, **Reboot**, and **Shutdown**. See the table below for the description of each option:

Menu option	Description
Normal boot	Powers up your US320f as the normal startup procedure.
Reset Mode	Resets Atrust Client Setup settings and remote management status for your US320f.
Firmware Update	Updates firmware for your US320f through the network.
Reboot	Restarts your US320f.
Shutdown	Powers off your US320f.

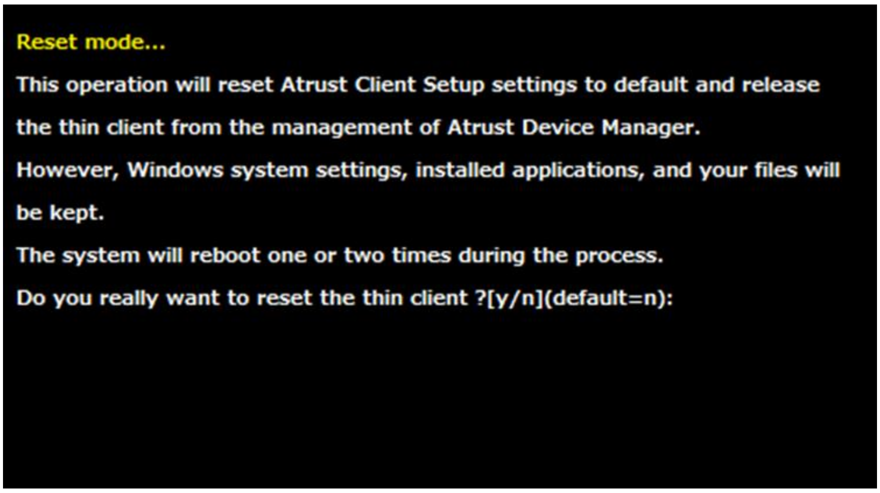
Note To perform **Firmware Update**, an Atrust Device Manager (ADM) server is required. Connect US320f to ADM via the network and use the firmware image stored on ADM to update the thin client. For detailed information, refer to the user's guide of Atrust Device Manager.

3. Use arrow keys to select **Reset Mode**, and then press <**Enter**> key to continue.



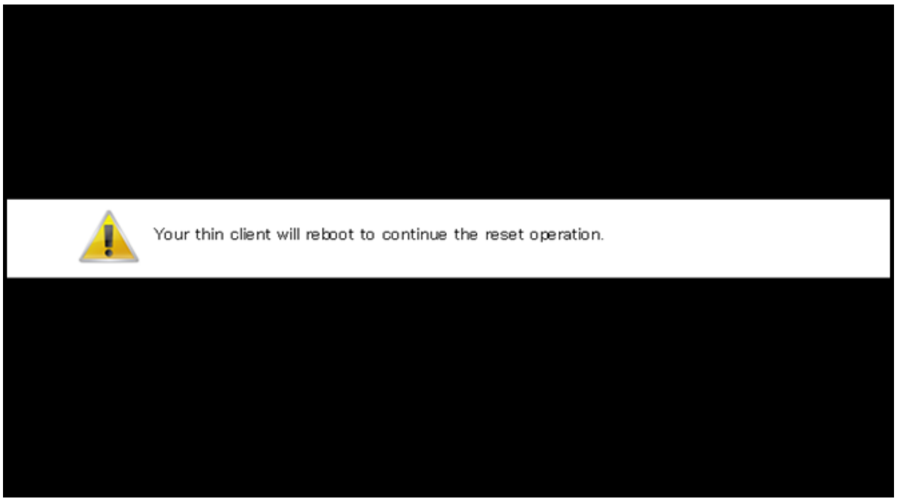
NEC Thin Client Menu

4. A message appears prompting you for confirmation. Type **y** to confirm, then press <**Enter**> key to continue.



```
Reset mode...
This operation will reset Atrust Client Setup settings to default and release
the thin client from the management of Atrust Device Manager.
However, Windows system settings, installed applications, and your files will
be kept.
The system will reboot one or two times during the process.
Do you really want to reset the thin client ?[y/n](default=n):
```

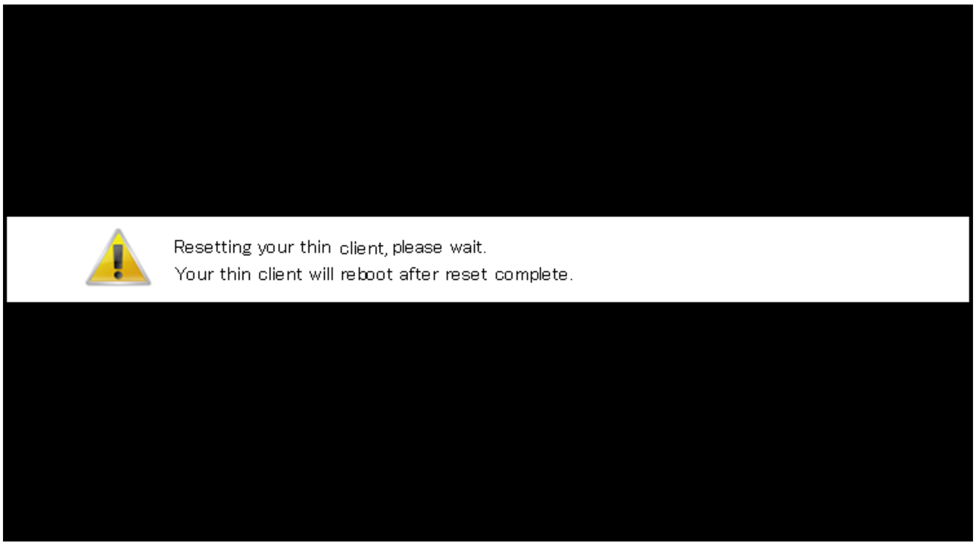
5. US320f will restart automatically.
   After auto sign-in, wait as it is until the message "Your thin client will reboot to continue the reset operation." is displayed. After the auto sign-in, the following message will appear. Wait for a while, or click **Restart Now**.



Your thin client will reboot to continue the reset operation.

6. US320f will restart.

7. After automatic sign-in, "Resetting your thin client, please wait. Your thin client will reboot after reset complete." message will be displayed.



Resetting your thin client, please wait.
Your thin client will reboot after reset complete.

8. When US320f is restarted automatically, the restoration is completed.

2.3 Imaging Devices with Atrust Recovery USB Disk Creator

The Atrust Recovery USB Disk Creator™ provides a simple USB imaging solution to help IT and Customer Service staff quickly and easily image supported devices.

The Atrust Recovery USB Disk Creator is available on the following NEC website:

http://www.58support.nec.co.jp/global/download/

Using the tool's flexible windows utility, users can easily:

- Reference the firmware image on the computer and configure the USB flash drive so as to send the firmware image to the target thin client.

Note USB flash drive of 32 GB (only) is required to deliver the firmware image by using the Atrust Recovery USB Disk Creator.

3. Configuring and Using Peripherals

US320f can be connected to peripheral devices.

NEC only supports the peripheral devices that are connected by using accessories that come with US320f or genuine optional products. Before connecting a non-supported product in the actual operating environment, thoroughly evaluate the operation with the specified settings based on the actual operating environment and confirm that there is no problem in terms of system integration.

4. Activating US320f

This section describes how to activate (authenticate) US320f (Windows 10 IoT Enterprise LTSB). You need to activate US320f to use all the features of Windows 10 IoT.

US320f is activated when shipped from the factory. However, if the firmware image of US320f is upgraded or recovered using ADM (Atrust Device Manger) or Atrust Device USB Disk Creator, US320f must be activated again.

Important

- **US320f supports automatic activation. When US320f is connected to a network connected to the Internet, activation is automatically executed in the background when US320f starts up. This means that you do not have to manually authenticate the license.**
- **In US320f, activation information is registered in the UWF “through” list. The activation status is therefore retained even after US320f restarts, allowing activation with UWF enabled.**

You can activate US320f via the Internet or by phone.

4.1 Via the Internet

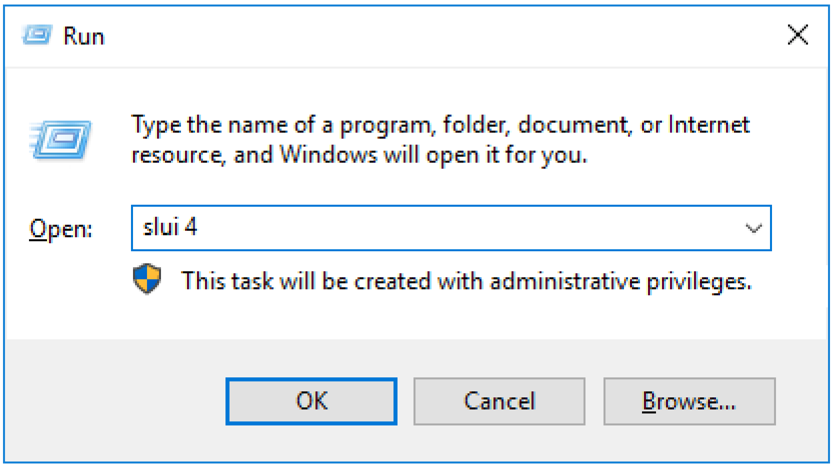
The easiest way is to activate via the Internet. Connect the US320f to the Internet and turn on the power. US320f will automatically activate the license through the internet. US320f supports automatic activation.

1. Connect a LAN cable and start US320f.
2. Confirm that Windows is activated by referring to **Start Menu** > **Settings** > **Update and Security** > **Activation**.

4.2 By phone

If the Internet is unavailable, you can activate your license by calling Microsoft.

1. Restart your US320f.
2. Right-click the **Start** button and click **Run** in the menu. Enter **slui 4** and click the **OK** button.

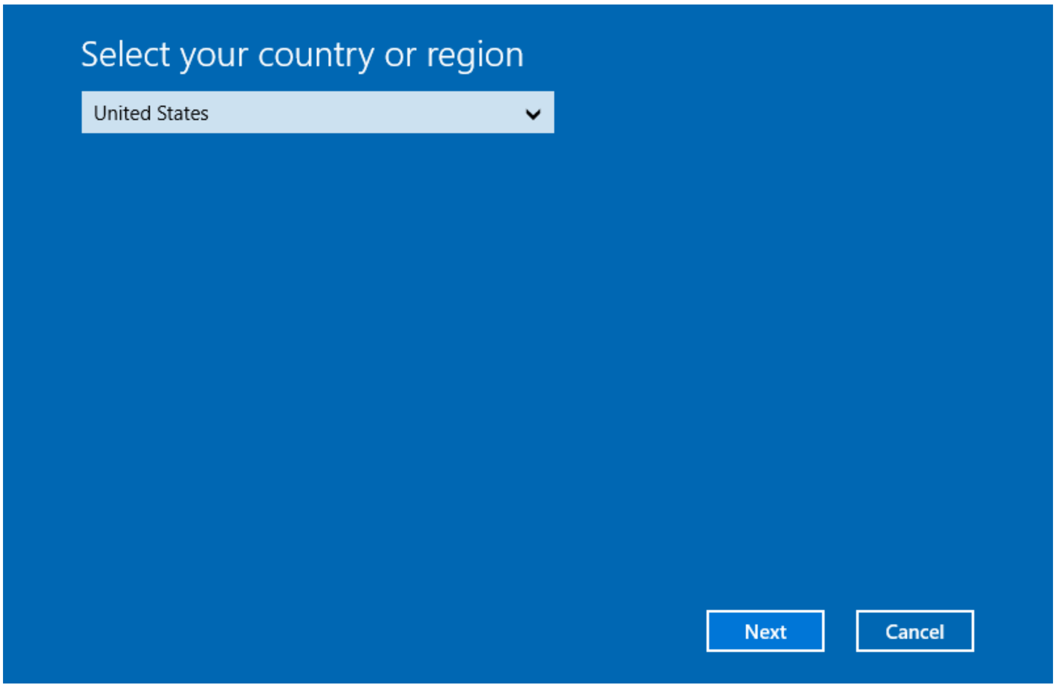


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: slui 4

This task will be created with administrative privileges.

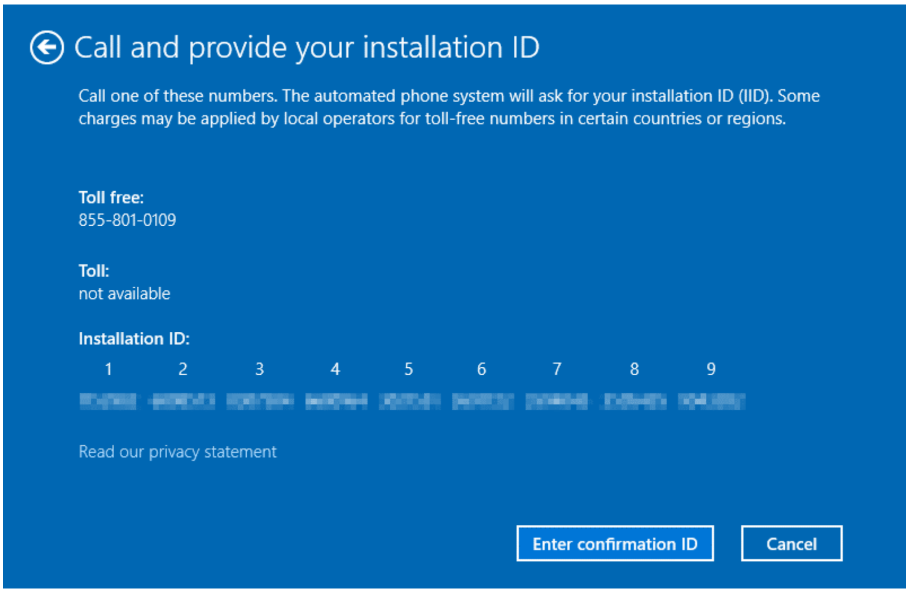
3. Click the down arrow, select the country or region name, and click **Next**.



Select your country or region

United States

4. Call the phone number displayed on the screen. Enter the installation ID by following the instructions from the telephone system.



Call and provide your installation ID

Call one of these numbers. The automated phone system will ask for your installation ID (IID). Some charges may be applied by local operators for toll-free numbers in certain countries or regions.

Toll free:
855-801-0109

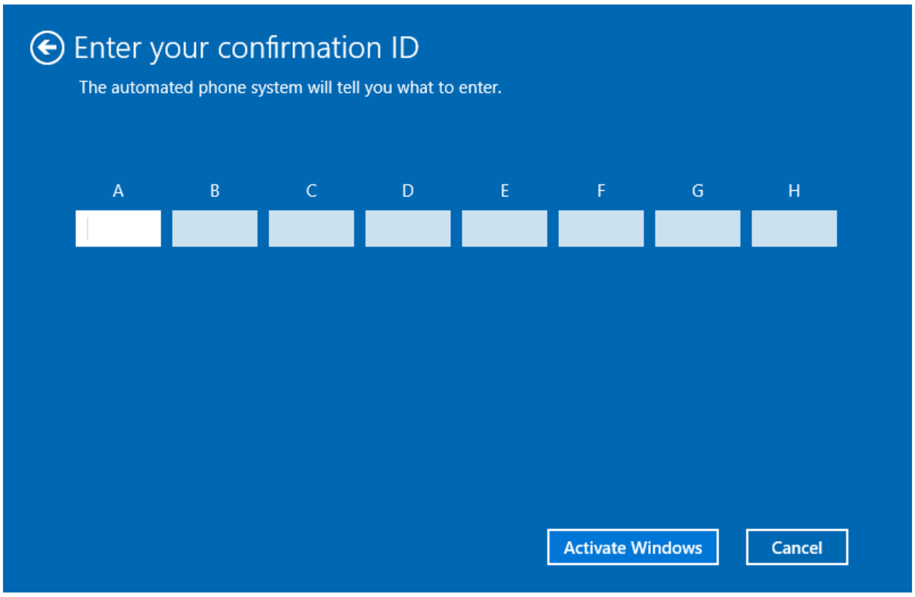
Toll:
not available

Installation ID:

1	2	3	4	5	6	7	8	9
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Read our privacy statement

5. Enter the confirmation ID.



Enter your confirmation ID

The automated phone system will tell you what to enter.

6. Click the **Activate Windows** button.

7. A message window indicating successful completion appears.

4.3 Activating US320f via the Volume Activation Management Tool (VAMT)

You can also activate US320f using VAMT proxy activation. The VAMT host computer distributes a Multiple Activation Key (MAK) to one or more US320f terminals and collects the installation ID (IID) from each US320f terminal. The VAMT host computer sends the IIDs to Microsoft on behalf of the US320f terminals and obtains the corresponding Confirmation IDs (CIDs). Then, the VAMT host computer installs the CIDs on the US320f terminals to complete the activation. To use this activation method, only the VAMT host computer needs to be enabled to access the Internet. For details about the VAMT, see the Microsoft documentation.

To perform VAMT proxy activation, it is necessary to register a firewall exception and set the registry on US320f terminals in advance to allow communication with the VAMT among subnets. Disable UWF to keep the setting also after the restart of US320f, and then perform the following steps:

1. Sign in to US320f as an Administrator.
2. If your device is in a workgroup, you may need to disable Remote UAC. Open a command prompt with administrator user rights and type the following to disable Remote UAC:

   ```
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
   LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
   ```
3. Type the following to enable the Remote Administration exception:

   ```
   netsh advfirewall set service RemoteAdmin enable
   ```
4. Type the following to enable WMI traffic at a command prompt by using a WMI rule:

   ```
   netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
   ```
5. Type the following to establish a firewall exception for DCOM port 135:

   ```
   netsh advfirewall firewall add rule dir=in name="DCOM" program=%systemroot%\system32\svchost.exe
   service=rpcss action=allow protocol=TCP localport=135
   ```
6. Type the following to establish a firewall exception for the WMI service:

   ```
   netsh advfirewall firewall add rule dir=in name ="WMI" program=%systemroot%\system32\svchost.exe
   service=winmgmt action = allow protocol=TCP localport=any
   ```
7. Type the following to establish a firewall exception for the sink that receives callbacks from a remote device:

   ```
   netsh advfirewall firewall add rule dir=in name ="UnsecApp"
   program=%systemroot%\system32\wbem\unsecapp.exe action=allow
   ```
8. Type the following to establish a firewall exception for outgoing connections to a remote device that the local computer is communicating with asynchronously:

   ```
   netsh advfirewall firewall add rule dir=out name ="WMI_OUT" program=%systemroot%\system32\svchost.exe
   service=winmgmt action=allow protocol=TCP localport=any
   ```

NEC Express5800 Series
US320f

7

Chapter 7 Establishing a Server Environment

This chapter contains information about the network architecture and enterprise server environment needed to provide network and session services for your thin clients.

It includes:

1. **Understanding How to Configure Your Network Services**
   Describes the network services available for your US320f.

2. **Understanding Session Services**
   Describes the server environment of the session services available for your US320f.

1. Understanding How to Configure Your Network Services

Network services used by the thin client can include DHCP and DNS. How you configure your network services depends on what you have available in your environment and how you want to design and manage it.

The following topics in this section provide important information to help you configure your network services:

- Using Dynamic Host Configuration Protocol (DHCP)
- Using Domain Name System (DNS)

1.1 Using Dynamic Host Configuration Protocol (DHCP)

A thin client is initially configured to obtain its IP address and network configurations from a DHCP server (new thin client or a thin client reset to default configurations). Using DHCP to configure and upgrade thin clients is recommended and saves you the time and effort needed to complete these processes locally on multiple thin clients. If a DHCP server is not available, fixed IP addresses can be assigned and must be entered locally for each device.

For more information about configuring a DHCP server, see documentation on the Microsoft website at: http://www.microsoft.com.

1.2 Using Domain Name System (DNS)

Thin clients accept valid DNS names registered on a DNS server available to the enterprise intranet. The thin client will query a DNS server on the network for name to IP resolution. In most cases DNS is not required but may be used to allow hosts to be accessed by their registered DNS names rather than their IP addresses. Every Windows DNS server in Windows 2000 and later includes Dynamic DNS (DDNS) and every server registers dynamically with the DNS server.

2. Understanding Session Services

Before you use the information in this section to configure your Citrix ICA, Microsoft RDP, VMware Horizon, and NEC Client Management Option (CMO) session services, be sure you understand and use the following guidelines:

- General guidelines

  The Thin-client session services are made available by servers hosting Citrix ICA, Microsoft RDP, VMware Horizon, and NEC Client Management Option (CMO) software products.

Tips

- You must purchase enough client licenses to support the total concurrent thin client load placed on the server farm. A failure to connect when all client seats are occupied does not represent a failure of equipment.
- If session services are used on a Windows Server OS, a Remote Desktop Services Client Access License (RDS-CAL) server must also reside somewhere accessible on the network. The server will grant a temporary (120-day) license on an individual device basis. Beyond the temporary (120-day) license, you must purchase RDSCALs and install them on the RD license server (you will not be able to make a connection without a temporary or permanent license).

- Citrix ICA guidelines

  Independent Computing Architecture (ICA) is a three-tier, server-based computing technology that separates the logic of an application from its user interface. The ICA client software installed on the thin client allows the user to interact with the application GUI, while all of the application processes are executed on the server. For information about configuring ICA, see Chapter 7*,* "2.1 Configuring Citrix ICA Session Services".

- Microsoft RDP guidelines

  Remote Desktop Protocol (RDP) is a network protocol that allows a thin client to communicate with the remote desktop service running on Windows Server 2008 or 2012 over the network. For information about configuring RDP, see Chapter 7*,* "2.2 Configuring Microsoft RDP Session Services".

- VMware Horizon guidelines

  VMware Horizon is a desktop management solution that allows the system administrator to configure the desktop and control user access. Client software securely connects users to centralized virtual desktops, back-end physical systems, or terminal servers through the PCoIP (PC over IP) or RDP protocol. For information about configuring VMware Horizon, see Chapter 7, "2.3 Configuring VMware Horizon Session Services".

- NEC Client Management Option (CMO) guidelines

  NEC Client Management Option (CMO) consists of components such as CMO Manager, CMO Configuration Console, CMO Virtual PC Agent, and CMO Terminal Agent.

  For information about configuring NEC Client Management Option (CMO), see Chapter 7, "2.4 Configuring NEC Client Management Option (CMO) Services".

2.1 Configuring Citrix ICA Session Services

ICA session services can be made available on the network using either Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016 with Terminal Services (remote desktop service) and one of the following installed:

- Citrix XenApp
- Citrix XenDekstop
- Citrix VDI-in-a-Box

Use the instructions accompanying these products to install them and make sessions and applications available to the thin clients sharing the server environment.

2.2 Configuring Microsoft RDP Session Services

RDP Session Services is used when remotely connecting to terminals running the following operating systems:

- Windows 7 (Supported versions only)
- Windows 8 (Supported version s only)
- Windows 8.1 (Supported versions only)
- Windows 10 (Supported versions only)
- Windows Server 2008 (R2)
- Windows Server 2012 (R2)
- Windows Server 2016

Thin clients can run Windows applications in a Windows GUI environment by using Remote Desktop Protocol. However, in actuality, these Windows applications are run on the connected computer.

Install one of the operating systems listed above according to the guidelines provided with the product, and provide sessions and applications on the thin clients that share the server environment.

US320f supports Microsoft VDI (Virtual Desktop Infrastructure). MS VDI consists of the following major components:

- RD connection broker server

  A software service that acts as a broker for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server.

- RD Web access server

  Works as a connection point for virtual desktops. Users can use RD Web access and connect to a virtual desktop pool or personal virtual desktop in addition to RemoteApp programs provided by RD sessions.

- RD gateway server

  A Remote Desktop (RD) gateway can be used for external connection via the Internet.

- RD license server

  Manages the Remote Desktop Services Client Access Licenses (RDS CALs) required for devices or users to use remote desktop services.

- RD virtualized host server

  Manages startup and maintenance of virtual machines via an RD virtualized host component that resides between Hyper-V and the RD connector broker.

2.3 Configuring VMware Horizon Session Services

VMware Horizon is a desktop management solution that allows the system administrator to configure the desktop and control user access. Client software securely connects users to centralized virtual desktops, back-end physical systems, or terminal servers.

Tip

> Information about installing and configuring VMware Horizon can be found on the VMware website at http://www.vmware.com.

VMware Horizon consists of the following major components:

- View Connection Server

  A software service that acts as a broker for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server.

- View Agent

  A software service that is installed on all guest virtual machines, physical systems, or terminal servers in order to allow them to be managed by View Manager. The agent provides features such as RDP connection monitoring, virtual printing, remote USB support, and single sign on.

- View Client

  A locally installed software application that communicates with View Connection Server in order to allow users to connect to their desktops using Blast protocol, PCoIP protocol or Microsoft Remote Desktop Protocol (RDP).

- View Portal

  A Web-based version of View Client supported by multiple operating systems and browsers.

- View Administrator

  A Web application that allows View Manager administrators to configure View Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.

- View Composer

  A software service that is installed on the VirtualCenter server in order to allow View Manager to rapidly deploy multiple linked clone desktops from a single centralized base image.

2.4 Configuring NEC Client Management Option (CMO) Services

Tip

Information about installing and configuring NEC Client Management Option (CMO) can be found on the NEC website at http://www.nec.com/.

NEC Client Management Option (CMO) consists of the following major components:

- SigmaSystemCenter (SSC)

  A suite of integrated virtualization platform management software that enables unified management of servers, virtual PCs, storage, and networks.

- CMO

  CMO Manager performs auto connections to virtual PCs, power management, and log output.

- CMO Configuration Console

  Used to configure auto connections to virtual PCs and power management by CMO. Settings for connections (between thin clients or users and virtual PCs) are configured based on thin client, user, and virtual PC information obtained from the system or entered by users. If a request for connecting to virtual PC is issued from a thin client to CMO, CMO makes a list of available virtual PCs based on the configured information, and sends that list to the user.

- CMO Terminal Agent

  CMO Terminal Agent runs on a thin client. When a thin client is started, CMO Terminal Agent communicates with CMO Manager, and automatically connects US320f to the virtual PC best suited to the user. If several virtual PCs are assigned to the user, CMO Terminal Agent displays a list of candidates. If a candidate virtual PC is powered off, CMO Terminal Agent can turn it on and connect to it. CMO Terminal Agent can also restart a connected virtual PC.

Tip

CMO Terminal Agent is not installed on US320f by default. Use the installer bundled with US320f to install it separately. For how to install CMO Terminal Agent, see Chapter 5, "12. Installing CMO Terminal Agent".

- CMO Virtual PC Agent

  CMO Virtual PC Agent runs on a virtual PC. It detects RDP connection/disconnection and sign-in/sign-out of virtual PCs, and sends a report to CMO.

NEC Express5800 Series
US320f

8

Chapter 8 Software Information, Notes, and Restrictions

This chapter describes US320f software information, and notes and restrictions on using US320f.

1. **Software Information**
   Describes software incorporated in and used with US320f.

2. **Notes and restrictions**
   Describes notes and restrictions on using US320f.

1. Software Information

This section describes software incorporated in and used with US320f.

1.1 Disk Configuration

The GUID Partition Table (GPT) of disk consists of the following three partitions to support UEFI.

- EFI system partition (FAT32) 100 MB
- Microsoft reserved partition (None) 128 MB
- OS partition (NTFS)

Note The NTFS file system used for Windows is compressed to reduce occupied space on the disk.

1.2 OS Build

Item	Description
Platform	US320f
Build version of English OS	Windows 10 IoT Enterprise LTSB v1.04-INTL
Build version of Japanese OS	Windows 10 IoT Enterprise LTSB v1.04-INTL

* This product release supports Atrust Device Manager (ADM) 2.09.001 or later. If you are using an older version of ADM, upgrade ADM before upgrading the firmware.

1.3 BIOS

Item	Description
Platform	US320f
BIOS version	US320f v2.04

1.4 Applications

Application	Version
Adobe Flash Player 26 NPAPI	26.0.0.151
Atrust Client Setup (Win10IoTEnT)	1.01
Citrix Receiver	4.9.0.2539(14.9.0.2539)
Intel (R) Sideband Fabric Device Driver	604.10125.2655.573
Microsoft Visual C++ 2005 Redistributable	8.0.56336
Microsoft Visual C++ 2008 Redistributable (x64)	9.0.30729.4148
Microsoft Visual C++ 2008 Redistributable (x86)	9.0.30729.4148
Microsoft Visual C++ 2015 Redistributable (x64)	14.0.2412.0
Microsoft Visual C++ 2015 Redistributable (x86)	14.0.2412.0
Realtek Ethernet Controller Driver	10.18.526.2017
UltraVNC	1.0.9.5
VIA Platform Device Manager	1.44
VMware Horizon Client	4.6.1.9881
Windows Media Player	12.0.9200.16578
Intel® Graphics Driver	10.18.10.4653
Intel® Trusted Execution Engine	1.0.0.1064
Internet Explorer	11.1770.14393.0
Remote Desktop Client (RDP8.0)	10.0.14393
Microsoft .NET Framework 4.6.2	4.6.01586

1.5 Media Codecs

Your US320f contains the following codecs:

Audio

- WMA
- 2ch Dolby Digital (AC-3)
- AAC
- MP3

Video

- WMV
- MPEG-4 Visual (MPEG-4 Part 2)
- AVC.H.264 (MPEG-4 Part 10)

2. Notes and Restrictions

This section describes notes and restrictions on using US320f.

2.1 Features and Software Not Supported

NEC does not provide support for the features below.

- US320f (Windows 10 IoT Enterprise LTSB) does not include Microsoft Edge, Cortana, Windows Store, Mail / Calendar application etc).
- Windows Update should be performed by upgrading the firmware. OS updates cannot be applied by using Windows Update or Windows Server Update Services (WSUS).
- UWF (Unified Write Filter) Servicing Mode cannot be used. OS updates cannot be applied by using Windows Update or Windows Server Update Services (WSUS).
- The UWF HORM (Hibernate Once/Resume Many) mode cannot be used.
- The Disk Cleanup utility cannot be used.
- BitLocker drive encryption cannot be used in the system drive (C). It can be used on removable media such as USB flash drives by using BitLocker To Go.
- A Microsoft account cannot be used.
- Currently, USB 3.0 host controllers are not yet supported. The USB mode of BIOS is EHCI (USB 2.0) by default. Use this default EHCI as the USB mode of the BIOS. Do not switch to XHCI (USB 3.0).
- The file encryption credential management function cannot be used.

2.2 Notes and Restrictions

- Failure of the software built into this product and related software published on the support page can no longer be corrected after the relevant software developer discontinues support. In this case, only limited support such as actions based on known cases is provided and you must basically operate the system by working around the failure (the failure remains “as-is”). To avoid such a situation, promptly conduct verification in all the operation scenarios to confirm that the product operates normally while building the system and after starting operation.
- The thin client terminal equipped with Windows OS is putting into effect the basic security measure for restricting part of operation to the User account in the factory shipment state, but it isn't guaranteed that there are no problems for security. According to the practical environment and the security for the customer, it's necessary to customize function restriction for User account and the blockade of the network port which isn't used, and so on. After confirming the no problem thing sufficiently beforehand, please use it.
- Like other IT systems, the thin client system might not operate correctly or it might not work sufficiently due to factors such as network configuration, policy settings, and the specifications of the connected peripheral devices. Some features require installation of third party software. NEC does not guarantee the use of this thin client in any environment under any conditions. Before using the thin client, thoroughly evaluate the operation in the actual operating environment and confirm that there is no problem.
- Hotfixes of thin client are published by support page. It is recommended to configure ADM server for deploying the Hotfixes to a thin client over the network and register the thin client as a management target of the ADM server. You need install the Hotfixes to each thin client manually if ADM is not used.
- OS to be equipped with this product is renewed for functional enhancement and quality improvement. Because of the timing of OS renewal at the production plant, there is a possibility that old and new OS is mixed in the case of additional purchase or two or more purchase. When needing unification of the OS version by the whole system, please use system image delivery by ADM and USB flash memory.
- If you copy a file whose size exceeds the pre-set maximum memory size (1024 MB by default) of UWF to C drive of US320f while the UWF is enabled, US320f becomes extremely unstable.
- ACS supports VMWare Horizon Client pre-installed on US320f. If you upgrade VMWare Horizon Client, connection entries created by Atrust Client Setup may not work correctly.
- When installing or uninstalling an application, you need to apply the shortcuts of the application displayed on Start screen of the User account before enabling UWF (Unified Writer Filter). It takes some time (about 4 to 5 seconds) before the shortcuts are displayed on the **Start** screen of a user account other than Administrator after sign-in. If you enable UWF without applying the shortcuts when using a User account, the settings will be discarded every time the system restarts and the shortcuts will take a long time to appear. (In the case of uninstallation, the deleted shortcuts remain and take time to disappear.)

  To permenantly apply the shortcuts on the **Start** screen, disable UWF first, and follow the steps below to install or uninstall an application, and then enable UWF.

  When installing an application

  1. Sign in to US320f as an Administrator.
  2. Install the application.
  3. Sign out from the Administrator account.
  4. Sign in as a User.
  5. Wait until the shortcut of the installed application appears on the **Start** screen.

  When uninstalling an application

  1. Sign in to US320f as an Administrator.
  2. Uninstall the application.

3. Sign out from the Administrator account.

4. Sign in as a User.

5. Wait until the shortcut of the uninstalled application disappears from the **Start** screen.

- In US320f local environment, the shortcut keys combined with Windows logo key are disabled.
- Only Japanese and English (U.S.) are supported as keyboard languages.

  If using another language, be sure to verify in advance that it will not cause any problems when the system is integrated.
- When performing port-level redirection for a mass storage device in a Citrix ICA or VMware Horizon session by using HDX USB redirection or USB redirection, redirection will enable a locally connected USB storage device to be used even if **Disable USB storage** is selected via Atrust Client Setup. To completely prevent a USB storage device from being used in a virtual desktop session, a setting must be configured in each service delivery environment.
- US320f is set to not use the virtual memory (page file) (0 MB). To use the virtual memory (page file), you must set the page file on a volume not protected by UWF. The virtual memory (page file) cannot be used in US320f because US320f consists of a single volume protected by UWF.
- Although Recycle Bin is displayed when you sign in with a domain user account, the recycle function is not provided. When you delete a folder or file, it is completely deleted.
- You may fail to sign in with a domain user account. In this case, "There are currently no logon servers available to service the logon request." appears and Event ID 5719 is recorded in the log.
  With the Windows fast logon function, US320f starts up without waiting for initialization of the network. So if the network connection is not yet established when you sign in with a domain user account, this phenomenon will occur because the domain server cannot be found.
  If you have already initially signed in with a domain user account (created a domain user profile), you can sign in using the domain cache the next time even if the network connection is not established. (Group policies are asynchronously applied by the fast logon optimization function.) However, changes to US320f are discarded by UWF after restart. Therefore, unless you initially sign in with a domain user account with UWF disabled, the created domain user profile is discarded at every restart and this phenomenon occurs.
  There are many possible scenarios where it takes time to establish a network connection. For example, the DHCP relay agent may need a long time to acquire the IP address or the 802.1X authentication process may take a long time. If it is difficult to solve the problem due to a variety of factors, you may be able to avoid this phenomenon by enabling **Computer configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon** under the group policies. If this setting is enabled, Windows displays the sign-in screen after the network connection is established. (Startup takes more time.) Although Event ID5719 may not be avoided and recorded in the log, you can ignore it as long as you can normally sign in to the domain.
- If you enable **Computer configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of removable devices** under the group policies, a blue screen error occurs after you restart US320f, so do not enable this policy.
- Windows KB files cannot be used to upgrade the built-in IE Flash Player.
- If the snapshot image contains setting information configured in **Profile Group** in ADM, you may not be able to properly acquire or distribute setting information from ADM in US320f after the snapshot image is distributed if you delete setting information for the profile group.
- When a thin client installing ACS is managed and registered in the ADM server, the administrative status becomes valid and it can not be detected from other ADM servers. This is a security specification to make it inaccessible from a malicious server. If a thin client is not registered as an ADM server management target, it may be detected from an unintended malicious server and the setting may be changed. Please use the thin client in a state registered as the management target of the ADM server (state detected from the ADM server) or secured with stealth mode.
- When ADM is built on the virtual machine of VMware ESXi and an update of firmware or a snapshot is installed in US320f from ADM, delay of a network occurs, and it sometimes fail in download of an image file. There is a possibility that it's improved by invalidating a flow control of a virtual NIC of VMware ESXi in setting in this case. Please refer to the following knowledge base about the way to invalidate a flow control of a virtual NIC of VMware ESXi in setting.

  Configuring Flow Control on VMware ESXi and VMware ESX
  http://kb.vmware.com/kb/1013413

- When starting a virtual desktop session from a Remote Desktop Connection shortcut with a standard user (User) account, you can not enter the character of the user name and password, because the focus is lost from the credential information input dialog. To enable keyboard input, it is necessary to activate the dialog by clicking on the credential information input dialog once with a mouse. There is currently no way to avoid this phenomenon.

- When starting a virtual desktop session from a Remote Desktop Connection shortcut with a standard user (User) account, you can not enter the character of the user name and password, because the focus is lost from the credential information input dialog. To enable keyboard input, it is necessary to activate the dialog by clicking on the credential information input dialog once with a mouse. There is currently no way to avoid this phenomenon.

- For US320f, SmartScreen filter function of Internet Explorer is enabled. SmartScreen matches files downloaded from the web against a list of reported malicious software sites and known unsafe programs. If a match is found, SmartScreen warns you that the download was blocked for security. If the network to which the US320f is connected is a local intranet or other environment where you can not connect to the Internet, the SmartScreen Filter function may block file downloads or add-ons' execution. Therefore, if you connect to a site that starts virtual desktop via RD Web access, browser such as StoreFront's Receiver for Web or Horizon HTML Access, it prevents configuration file download and add-on's execution. To avoid it, register the site you want to connect to the Internet option trusted site or intranet zone and connect to it with the appropriate security level.

- In US320f, execution of command prompt of standard user (User) account is restricted. Therefore, the "Support data collection" function of VMware Horizon Client can not be used with the standard user (User) account.

- With the standard user (User) account, the Intel® HD Graphics Control Panel hotkey does not work.

- In US320f, automatic redirect setting of Citrix Receiver's general USB redirect is enabled by default.
  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB\Devices]

  "AutoRedirectAudio"=dword:00000001

  "AutoRedirectPrinters"=dword:00000001

  "AutoRedirectVideo"=dword:00000001

  "AutoRedirectStorage"=dword:00000001

  "AutoRedirectImage"=dword:00000001

  * When controlling automatic redirection of devices other than audio (AutoRedirectAudio), printer (AutoRedirectPrinters), Web camera (AutoRedirectVideo), mass storage (AutoRedirectStorage), scanner, digital camera (AutoRedirectImage), it is necessary to add a registry to specify the vendor ID and product ID of the device as described below. Please also refer to the Citrix document for details.

  (example)

  [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB\Devices\VID12AB PID5678]

  "AutoRedirect"=dword:00000001

NEC Express5800 Series
US320f

9

Chapter 9 Operation and Maintenance

This chapter describes troubleshooting and how to maintain US320f to keep it running smoothly.

1. **Cleaning of US320f**
   Describes how to clean US320f to keep it in good shape.

2. **Troubleshooting**
   See this section when you suspect failure. This section provides helpful information for solving problems that might occur in your system.

3. **Relocation and Storage**
   Describes how to relocate or store US320f.

4. **User Support**
   Describes user support related to US320f.

1. Cleaning

Clean US320f on a regular basis to keep it in good shape.

⚠WARNING

Observe the following instructions to use US320f safely. Failure to follow these instructions may result in loss of life or serious personal injury.

- **Do not disassemble, repair, or alter US320f.**

1.1 Cleaning of US320f

Wipe off dirt on the surface of US320f with a soft cloth. If dirt is hard to remove, US320f can be cleaned as described below.

Important

- **Do not use a volatile solvent such as thinner and benzene for cleaning. Using these may damage or discolor US320f.**
- **Do not allow US320f, plugs, cables, rear connectors or the surrounding area to become wet.**

1. Confirm that the power of US320f is off.
2. Pull out the power cord of US320f from the outlet.
3. Wipe off any dust on the power cord and plugs with a dry cloth.
4. Soak a soft cloth in mild detergent diluted with cold or lukewarm water and wring out the cloth thoroughly.
5. Rub the dirty areas of US320f firmly with the cloth described in step 4 above to remove the dirt.
6. Wipe off again with a cloth soaked in fresh water and wring out thoroughly again.
7. Wipe US320f with a dry cloth.

2. Troubleshooting

Any of the problems listed in this section might be resolved by updating the US320f firmware. For how to update the firmware, see Chapter 6, "2. Restoring Settings".

2.1 Problems When Connecting to Virtual PCs

[?] Failed to connect to a virtual PC:

→ If the date and time are not set on the virtual PC and US320f, RDP connection to the virtual PC might fail. Set the correct date and time. The date and time are not set immediately after US320f is started. Acquire the correct date and time from the time server.

[?] [New] does not appear on the right-click menu on a mapped USB storage device:

→ This error may occur depending on the environment of the virtual PC to be connected. In this case, create a file or a folder in a place other than the USB storage device, and copy it to the USB storage device.

2.2 Other Problems with Using US320f

[?] There are problems with the way the equipment is operating, such as screens freezing or the system responding very slowly:

→ It might seem as if US320f is malfunctioning, depending on the conditions under which it is being used.
Wait for a while, and if the problem is not resolved, restart US320f.
If the OS is unresponsive, hold down the power switch for at least five seconds to forcibly turn off the power, then press the power switch again.

[?] The screen will not display the maximum resolution:

→ Check that the DVI-VGA adapter that you are using is the one supplied with US320f.
The screen will not display properly if an adapter other than the one supplied is used.

3. Relocation and Storage

For how to relocate or store US320f, contact your service representative.

⚠WARNING

Observe the following instructions to use US320f safely. Failure to follow these instructions may result in loss of life or serious personal injury. For details, see *Precautions for Use*.

- **Do not disassemble, repair, or alter US320f.**
- **Do not remove the lithium battery.**
- **Do not handle US320f with the power cord of US320f connected to a power source.**

⚠CAUTION

Observe the following instructions to use US320f safely. Failure to follow these instructions may cause a fire, personal injury, or property damage.

- **Do not drop US320f.**

Important

- **When carrying out major work such as changing the floor layout, contact your sales or service representative.**
- **To enable US320f and built-in devices to operate properly following relocation or storage, it is recommended to keep US320f in a place where standard room temperature can be maintained.**
- **Observe the storage conditions (temperature: –10°C to 55°C, humidity: 10% to 95% and no condensation) when storing US320f.**

1. Turn off US320f. (The Power status LED goes off.)
2. Pull out the power cord connected to US320f from the inlet.
3. Remove all cables connected to US320f.
4. Pack US320f securely so as to avoid damage, shock and vibration.

Important

Before operating US320f again after transportation or storage, first check and adjust the system clock. If the system clock gains or loses a significant amount of time as time passes even if you adjust the time, contact your service representative and request maintenance. When US320f and built-in optional devices are moved from a cold site to a warm site, condensation may occur and using them without any adjustment may cause a malfunction or fault to occur. Before the devices are operated again after transportation or storage, they should be suitably prepared for the usage environment.

4. User Support

4.1 Before Requesting Repairs

Before requesting repairs, do the following if the server appears to have failed:

1. Check if the power cord and the cables to other devices are properly connected.
2. See "Troubleshooting" to see if your problem fits one of the descriptions. If it does, take the recommended action.
3. Check if the software required for operation of the server is properly installed.
4. Run anti-virus software on the servers.

If the server still appears to have failed after you have taken the above actions, contact your service representative immediately. Before contacting your service representative, take a note of the LED indications of the server and the alarm indications on the display unit, as these may provide significant help to your service representative.

Go to **Support information** on the NEC Corporate website (http://www.nec.com/) for more information.

4.2 When Requesting Repairs

When requesting repairs, prepare the following documents:

□ Memo of the message shown on the screen display when the failure occurred

□ Failure information (if requested by your service representative)

□ Record of the equipment and peripheral devices

4.3 About Repair Parts

Repair parts for this equipment will be available for up to 5 years after manufacture is discontinued.

NEC Express5800 Series
US320f

10

Chapter 10 Appendix

Appendix A Specifications

Item	Specification
Processor	Intel® Celeron® N2930 1.83 GHz Quad-core processor
Memory	32GB flash memory / 4GB RAM DDR3
I/O ports and peripherals	USB 2.0 port ×3, USB 3.0 port ×1 (operates in USB 2.0 mode) DVI-I port ×1 DVI-D port ×1
Networking	RJ45 (10/100/1000Mbps)
Display	Single: Max. 1920x1200@32 bpp Dual: Max. 1920x1200@32 bpp
Audio	Output: ϕ3.5 mini-jack Input: ϕ3.5 mini-jack
Mounting	Mount upright by using the stand, or mount on the back of monitor.
Device security	Kensington security slot (cable: separately priced)
Physical characteristics	Height: 143 mm (5.63 inch) Width: 39.5 mm (1.56 inch) Depth: 103 mm (4.06 inch)
Power supply	Auto detect (for all countries) 100-240 VAC, 50/60 Hz Mean power consumption (with connected keyboard ×1, PS/2 mouse ×1 and monitor ×1: Approx. 12.2 watts
Temperature range	Operating: 10°C to 35°C (50°F to 95°F) Storage: –10°C to 55°C (14°F to 131°F)
Humidity	Operating: 20% to 80% Storage: 10% to 95% (non-condensing)
Certificates	US 60950-1, EN 60950-1, CSA60950-1 FCC, CE, VCCI WEEE, RoHS compliant

US320f
User's Guide
FW Win10IoTEnt LTSB v1.04-INTL

Second Edition, JUNE 2018

NEC Corporation
7-1 Shiba 5-Chome, Minato-Ku
Tokyo 108-8001, Japan