Express5800

NEC

Express5800 **Series**

US310e User's Guide

Documents for US310e

Documents for this product are provided as booklets (📖), which are supplied with the product, and as digital manuals (📄) available on the NEC website.

	Getting Started	Describes how to use this product, from unpacking to operations. Read this guide first for confirm an overview of US310e.

PDF	User's Guide	
	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 US310e.
	Chapter 1: About US310e	Describes the names and features of US310e 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 US310e.
	Chapter 3: Using US310e	Describes the basics of how to use your US310e.
	Chapter 4: Configuring Client Settings with Atrust Client Setup	Describes the client setting tools useful for US310e.
	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 US310e.
	Chapter 8: Software Information, Notes, and Restrictions	Describes US310e software information, and notes and restrictions on using US310e.
	Chapter 9: Operation and Maintenance	Describes troubleshooting and how to keep US310e 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 US310e 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 US310e or its software.
Tip	Indicates information that is helpful to keep in mind when using US310e.

Abbreviations of Operation Systems

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

Notations in this document	Official names of Windows
Windows 8.1 *1	Windows 8.1 Enterprise Edition
Windows 8 *1	Windows 8 Enterprise Edition
Windows 7	Windows 7 Enterprise 64-bit (x64) Edition
	Windows 7 Enterprise 32-bit (x86) 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

*1 *Windows 8* indicates the 64-bit edition unless otherwise stated.

Trademarks

Microsoft, Windows, Windows Server, Windows Vista, and MS-DOS are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Intel, XEON, Intel Core, Pentium, Celeron, and Intel vPro are trademarks or registered trademarks of Intel Corporation in the United States and/or other countries.

ATI, ATI logo, FirePro, and combinations thereof are trademarks of Advanced Micro Devices, Inc.

Adaptec and the Adaptec logo are registered trademarks of Adaptec, Inc.

SCSISelect is a trademark of Adaptec, Inc.

LSI and the LSI logo design are registered trademarks or trademarks of LSI Corporation.

Adobe, the Adobe logo, and Acrobat are trademarks of Adobe Systems Incorporated.

Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.

NVIDIA, the NVIDIA logo, and Quadro are trademarks or registered trademarks of NVIDIA Corporation in the United States and other countries.

Atrust is a registered trademark of Atrust Computer Corporation.

Symantec Norton Ghost

(c) 1999 Symantec Corporation. All Rights Reserved.

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.nec.com/

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 US310e 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 US310e.

Disposal

Dispose of US310e, the battery, and all the optional devices according to national laws and regulations. Also dispose of the power cord provided with US310e to prevent it being used for other devices.

Shipping

A lithium metal battery or a lithium ion battery is used for US310e 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 US310e.

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 US310e as the external power supply unit.

Important	**Use only the AC adapter that comes with US310e. Using an AC adapter that does not meet the required electrical specifications may cause a fire, malfunction, or fault to occur.**

FCC Statement

This equipment has been tested and found to comply with the limits for either Class A or Class B digital devices, 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 the 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.

Shielded interconnect cables and shielded AC power cable must be employed with this equipment to insure compliance with the pertinent RF emission limits governing this device. Changes or modifications not expressly approved by the system's manufacturer could void the user's authority to operate the equipment.

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 or DVDs.
When disposing of used products, you should comply with applicable legislation or agreements you may have. The mark on the electrical and electronic products only applies 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.

台灣電池規制 (廢棄物清理法)

警告:
如果更換錯誤電池會產生爆炸請以相同或同型電池更換使用

廢電池請回收

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"

⚠ 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 US310e.

This User's Guide describes hazardous parts of US310e, 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

Symbol to draw attention   Description of warming   Term indicating a degree of danger

WARNING

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 US310e 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 US310e near the fire. This can result in a fire.
	Do not touch US310e 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 US310e. 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 US310e safely. Read this section carefully to ensure proper and safe use of US310e. For symbols, refer to *Safety Precautions*.

General

	WARNING	
🚫	**Do not use US310e for services which may directly affect human lives and for which critically high reliability is required.** US310e 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 US310e has been used for the above applications.	
⚠️🔥 🔌 🚫	**Do not use US310e if any smoke, odor, or noise is present.** If smoke, odor, or noise is present, immediately turn off US310e and disconnect the power plug from the outlet. Then contact the store where you purchased the product or your maintenance service company. Using US310e 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 US310e.** Do not let any liquid such as water or foreign materials including pins or paper clips enter US310e. Failure to follow this warning may cause an electric shock, a fire, or failure of US310e. If liquid or foreign matter accidentally enter US310e, immediately turn off the power and disconnect the power plug from the outlet. Do not disassemble US310e. 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 US310e in any environment that requires an extension cord. Connecting to a cord that does not conform to the power supply specifications of US310e 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.
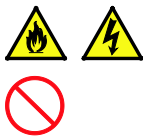
Insert the power plug into the outlet as far as it goes.

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 US310e. 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.
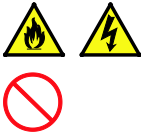
- Do not stretch the cord harness.
- Do not bend the power cord.
- Do not twist the power cord.
- Do not step on the power cord.
- Uncoil the power cord before use.
- Do not secure the power cord with staples or equivalent objects.

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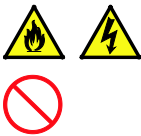
Do not use the attached power cord for any other device or usage.

The power cord that comes with US310e is designed to connect with US310e and to be used with US310e, 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 US310e in other than the specified location.

Do not install US310e 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 US310e in an environment where corrosive gases exist

Do not install US310e in a place subject to corrosive gases including sodium chloride, sulfur dioxide, hydrogen sulfide, nitrogen dioxide, chlorine, ammonia, or ozone. Do not install US310e 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 US310e 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 US310e including the cables. Failure to follow this warning may cause a fire or an electric shock.	
⚠ ⚡ 🚫	**Keep animals away from US310e.** Keep animals such as pets away from US310e. Pet hair or other waste can enter US310e, 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 US310e 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.	

Wireless features (when using N8120-118 (option)

<table>
<tr><td colspan="2" align="center">**CAUTION**</td></tr>
<tr>
<td>⚠</td>
<td>

Keep US310e at least 30 cm away from an internal artificial cardiac pacemaker.

Use US310e at least 30 cm away from an internal artificial cardiac pacemaker. Internal artificial cardiac pacemakers may be affected by radio waves.

</td>
</tr>
<tr>
<td>⚠</td>
<td>

Turn off the power or wireless communication features of US310e in places where use of US310e is prohibited.
Turn off the power or wireless communication features of US310e in places where use of US310e is prohibited (such as medical treatment facilities).
If any medical equipment is being used near US310e, turn off the power or wireless communication features of US310e regardless of whether the use of US310e is prohibited. The medical equipment may be affected, causing an accident. For more information, consult with the relevant medical treatment facility.

</td>
</tr>
<tr>
<td>⚠</td>
<td>

Turn off the wireless communication features of US310e if US310e cause radio interference.

If your US310e causes radio interference with any other equipment, immediately turn off the power or wireless communication features of US310e. The equipment may be affected and cause an accident due to malfunction.

</td>
</tr>
</table>

Cleaning and working with internal devices

<table>
<tr><td colspan="2" align="center">**CAUTION**</td></tr>
<tr>
<td>⚠ ⚡ 🚫</td>
<td>

Do not disassemble, repair, or alter US310e.

Never attempt to disassemble, repair, or alter US310e under any circumstances. Failure to follow this instruction may cause an electric shock or fire as well as malfunction of US310e.

</td>
</tr>
<tr>
<td>⚠ ⚡ 🔌</td>
<td>

Disconnect the power plug before opening US310e.

Make sure to power off US310e and disconnect the power plug from the power outlet before cleaning the unit or attaching and detaching cables. Touching the inside of US310e with its power cord connected to a power source may cause an electric shock even if US310e 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.

</td>
</tr>
</table>

For Proper Operation

Observe the following notes for successful operation of US310e. Ignoring these notes can cause malfunction or failure of US310e.

- When you have just turned off US310e, wait at least 10 seconds before turning it back on. If US310e 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 US310e and unplug the power cord from the outlet before relocating US310e.

- Clean US310e 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 US310e should be stored in a place where a stable room temperature is able to be maintained. It is preferable to store US310e 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 US310e. Radio interference may cause malfunction of US310e.

- Observe the following notes on using and connecting an interface cable.

  - Do not use a damaged cable connector.
  - Do not step on the cable.
  - Do not place any object on the cable.
  - Do not use US310e with loose cable connections.
  - Do not use a damaged cable.

- If US310e or the option devices (add-ons) connected inside US310e are moved suddenly from a cold environment to a warm environment, condensation might form inside US310e or its add-ons, causing malfunction or damage if US310e is used in this state. To protect your important data and assets, be sure to consider the environment carefully before using US310e.

- Make sure that all add-ons and peripherals are able to be attached or connected to US310e. Note, however, that even if add-ons or peripherals can be physically attached or connected, they might damage US310e 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 US310e, but if these add-ons cause US310e 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.
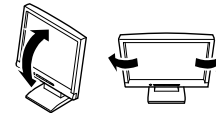
Adjustment of Screen Brightness and Contrast
The display unit has brightness and contrast adjustment functions. The most suitable brightness and contrast depend on the individual and the working environment (well-lit room versus insufficient light). Adjust brightness and contrast so that the screen will be easy to see. An extremely bright or dark screen will have a bad effect on your eyes.
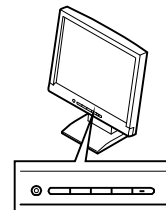
Adjustment of Keyboard Angle
The angle of the keyboard provided with the server can be adjusted. Adjust the keyboard to an angle at which it is easy to operate. Adjustment assists in reducing strain on your shoulders, arms, and fingers.

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
US310e**

About US310e

This chapter describes the features of US310e and the names of the components.

1. **Introduction**

   Provides an overview of US310e.

2. **Names and Functions of Components**

   Describes the names and functions of US310e components.

3. **Installation and Connection**

   Describes how to install and connect US310e.

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 US310e.

US310e is a desktop thin client terminal that is designed to configure a virtual PC thin client system.

US310e 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 US310e to fully understand the handling of US310e, and appreciate its functions to the maximum extent.

2. Names and Functions of Components

This section describes the names and functions of US310e components.

2.1 Front View
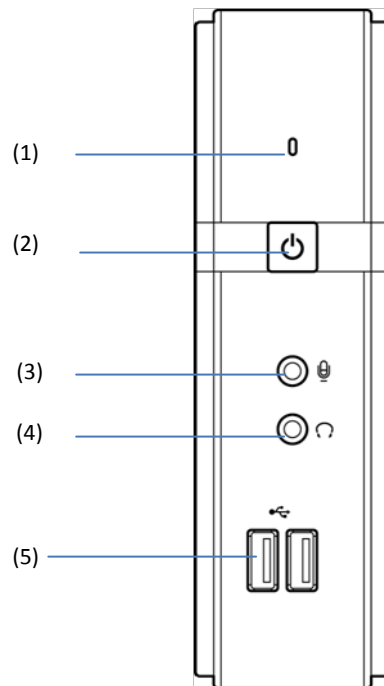
(1) Status LED (Blue: normal state, Orange: standby state) (*1)   (4) Headphone connector

(2) Power switch   (5) USB 2.0 ports (2 ports)

(3) Microphone connector

*1 US310e does not support standby operations.

2.2 Rear View
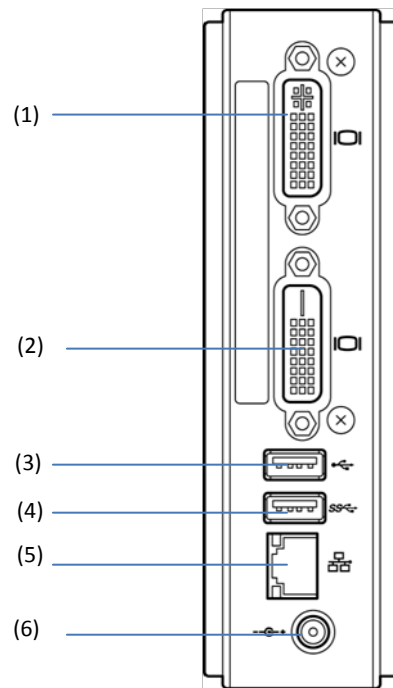
(1) DVI-I port   (4) USB 3.0 port (*1)

(2) DVI-D port   (5) LAN connector

(3) USB 2.0 port   (6) Power connector

*1 The USB 3.0 port on US310e 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 US310e 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 US310e to connect peripherals conforming to the USB 2.0 standard (such as keyboard, mouse, and HDDs) to US310e.

Note	US310e cannot be woken up from a USB 2.0 port.

2.2.4   USB 3.0 port

One USB port is located on US310e to connect peripherals conforming to the USB 2.0 standard (such as USB flash drives and HDDs) to US310e.

Note	• US310e cannot be woken up from a USB 3.0 port. • The USB 3.0 port on US310e 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 US310e.

Important	**Be sure to use the AC adapter and power cord that comes with US310e. 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 US310e.**

2.3   Top View
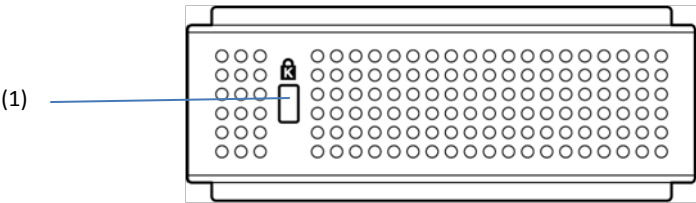
(1) Security slot

3. Installation and Connection

This section describes how to install and connect US310e.

3.1 Installation

Install US310e by using the stand that comes with US310e.

3.1.1 Placing on a desk

Place US310e (with its stand) on a desk or similar place in an upright position.
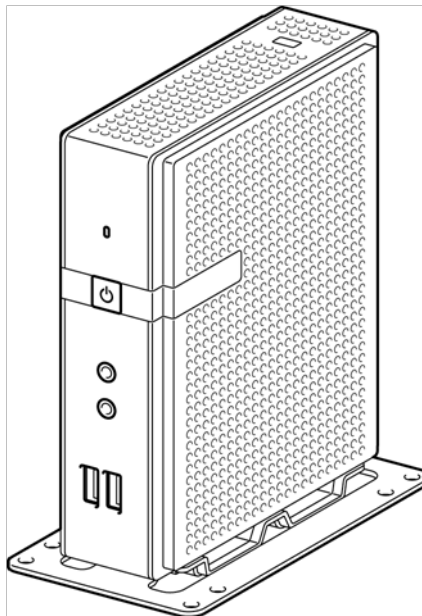
3.1.2   **Mounting on the back of a monitor**

Mount US310e on the back of a monitor by using the stand.

You can mount your US310e on a monitor conforming to VESA.

1. Place your US310e with its bottom facing up, and remove the screw located in the center.
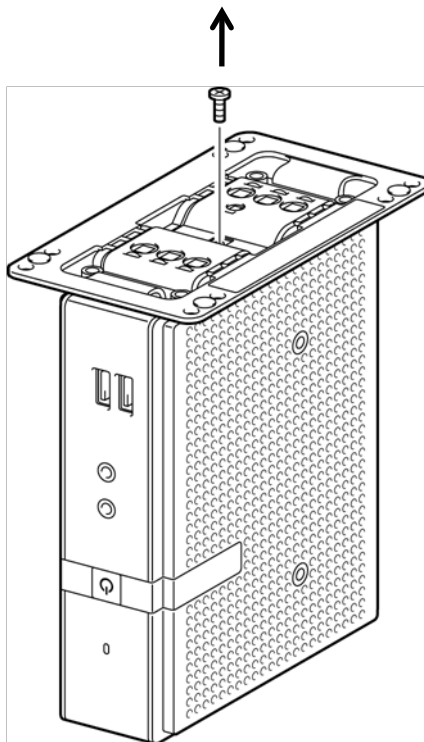
Store the removed screw inside the stand.
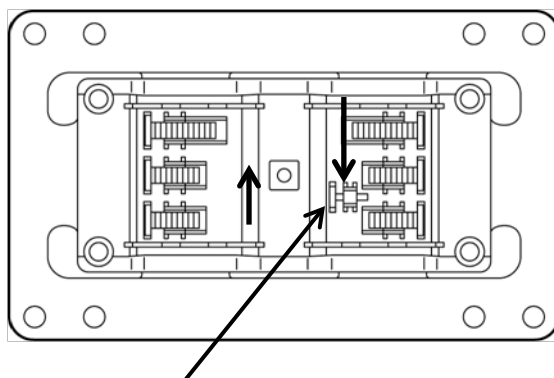
The screw head must face inside.

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)

(2)

(3)
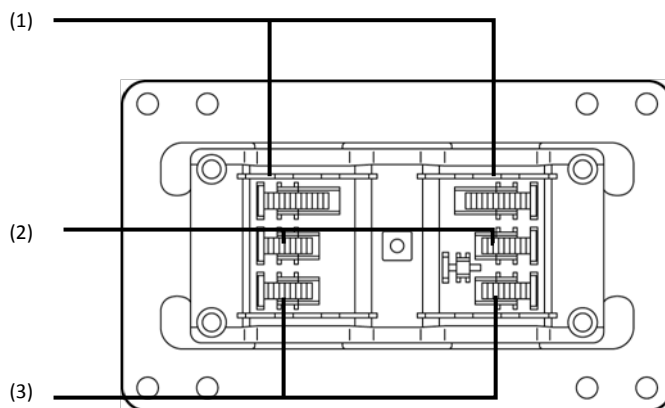
(1) Fixing screw for monitor (long) (Approx. 13 mm)   (3) Fixing screw for body

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

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.

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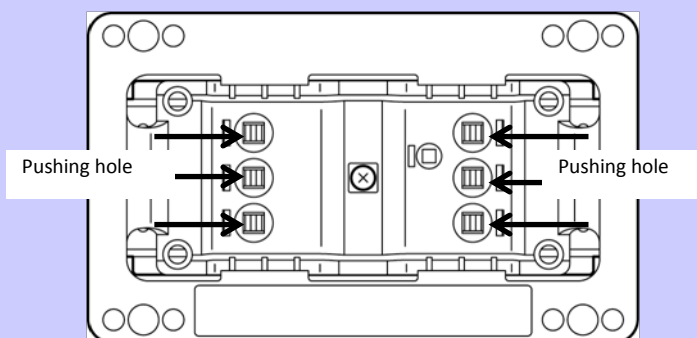
- If the screwdriver is too thin (or too thick) for the screw, the screw thread may be damaged. Use the proper screwdriver.

3. Mount the stand on US310e by using the screws for the body.
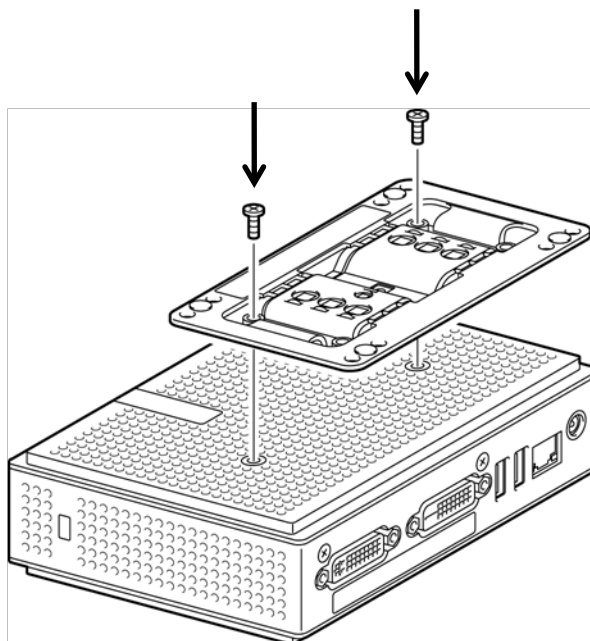
4. Use the screws for the monitor to mount US310e on the mounting holes on the monitor so that the front of US310e faces left. See the figure below.
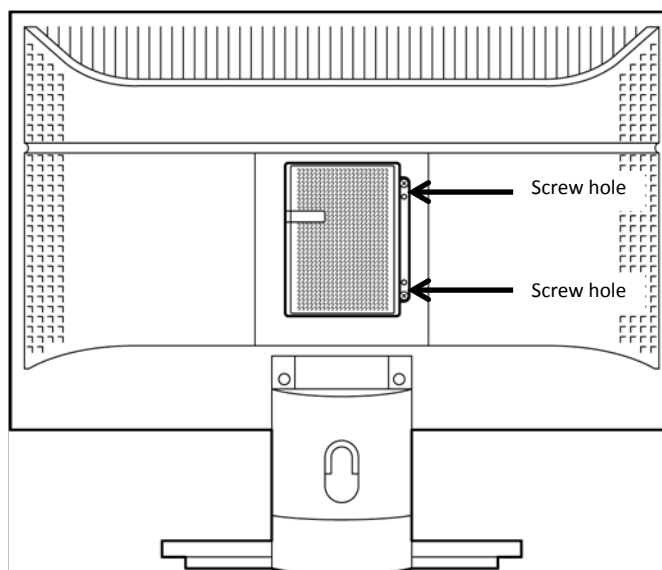
Tips	• Use two screws to mount US310e on the monitor.
	• The location of the mounting holes depends on the monitor size. Refer to the manual that comes with your monitor.
	• To remove US310e from the monitor, reverse the steps (1) through (4) in "3.1.2 Mounting on the back of a monitor" to remove US310e and mount the stand.

Important	• **Do not use US310e with the stand being removed.**
	• **Do not change combination of US310e and the stand.**

⚠ **CAUTION**

Observe the following instructions to use US310e safely. Failure to follow these instructions may cause a fire, personal injury, or property damage. For details, see *Precautions for Use*.
- **Do not install US310e in other than the specified locations.**

Environmental requirements:
- Operating
  Temperature: 10 to 35⁰C
  Humidity: 20 to 80%
- Storage
  Temperature: −10 to 55⁰C
  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
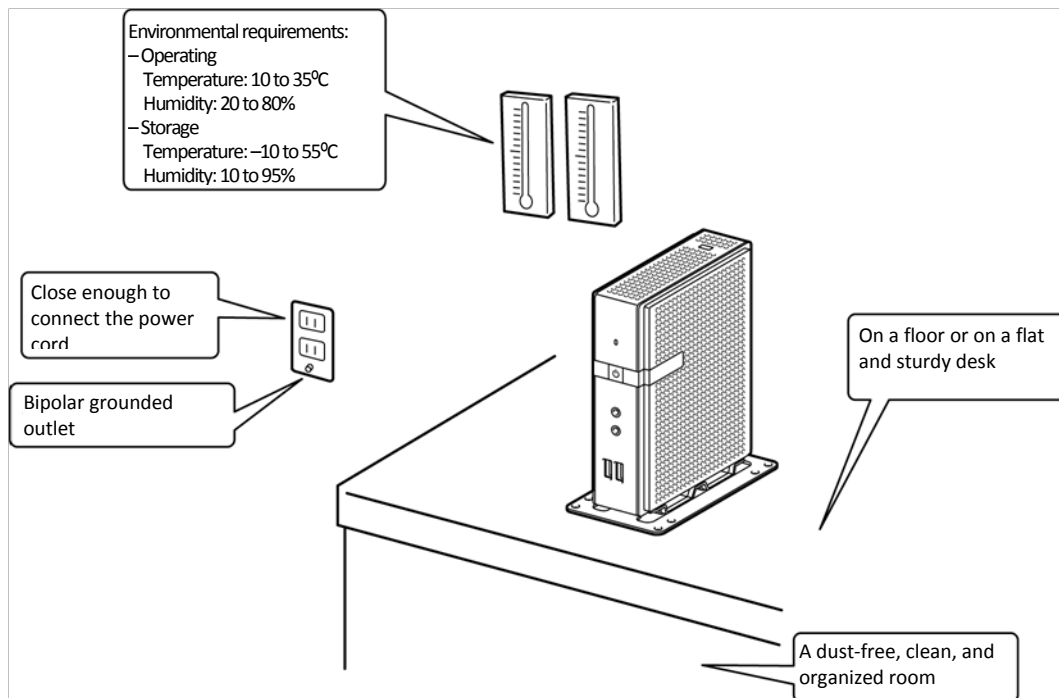
Do not place US310e in the following places. Otherwise, US310e might malfunction.

- 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 US310e

- Places near equipment that generates power noise (e.g., contact sparks when powering-on or powering-off a commercial power supply via a relay). (To install US310e near equipment that generates power noise, ask your service representative to separate the power wiring or install a noise filter.)

3.2   Connection

Connect US310e to your network.

After connecting the network cable, connect the power cord of the AC adapter that comes with US310e to US310e and plug the power cord into the wall socket.

⚠ WARNING

Observe the following instructions to use US310e 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 US310e 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 US310e with any loose interface connection.
- Use the authorized power cord only.
- Do not connect any interface cable with the power cord of US310e being connected to a power source.
- Do not use any unauthorized interface cable.

Important
- **Before connecting US310e, turn off US310e and peripherals to be connected. Failure to follow this may cause malfunction or failure.**
- **Before connecting a third-party peripheral or interface cable to US310e, ask the dealer whether the device or cable can be used for US310e. Some third-party devices cannot be used for US310e. 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 US310e.

Front view

Microphone

Headphone or
computer speaker

USB devices

Rear view

Display (DVI or VGA)*1

Display (DVI)

USB devices

*2

AC adapter

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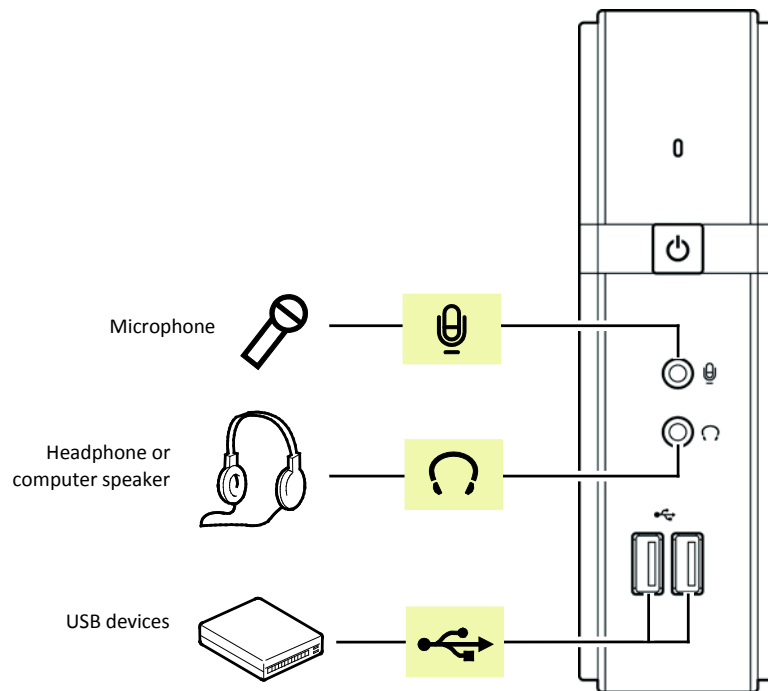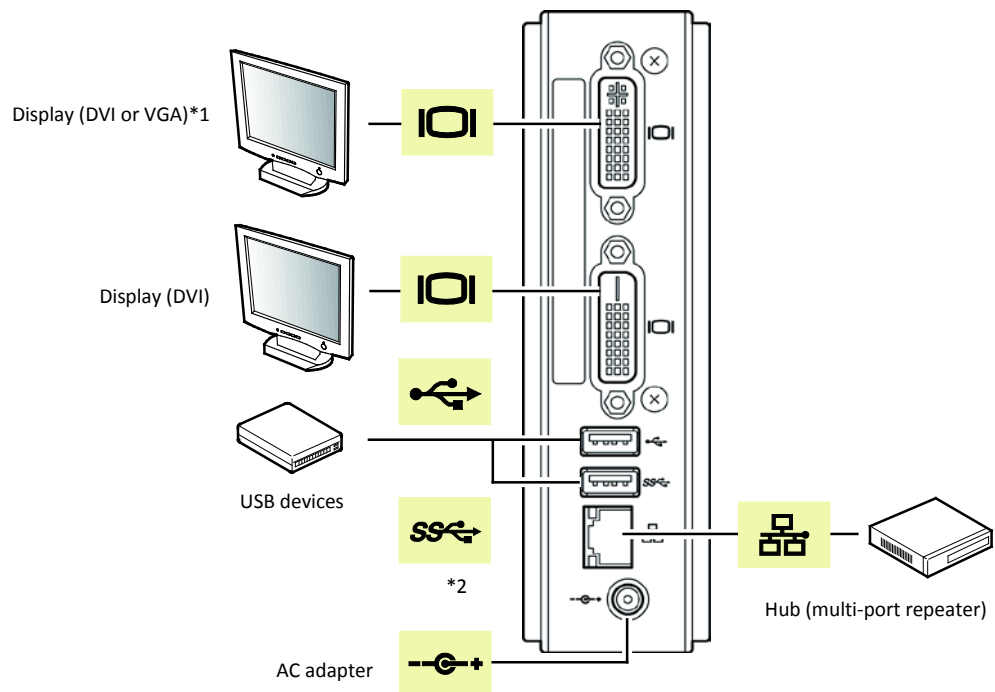
*1 Use the supplied DVI-VGA adapter to connect a display that uses a VGA interface.
*2 The USB 3.0 port is disabled by the factory default settings.

4. Setting up the System BIOS

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

Read this section before installing US310e 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 US310e.

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 US310e. 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 or F4.
	• Turning off the power of US310e or resetting US310e 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.

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.)

Currently displayed menu

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

         NEC US310e Series                                        Set the Date. Use Tab to
         BIOS Version              US310e v1.49                    switch between Date elements.
         Build Date and Time       11/07/2014 15:49:32

         Memory Information
         Total Memory              2048 MB

         TXE Information
         TXE FW Version            01.01.00.1089

         System Date               [Fri 12/12/2014]
         System Time               [12:14:43]                     ↔: Select Screen
                                                                  ↑↓: Select Item
         Access Level              Administrator                   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.
```

Setting item

Description of key functions

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.
+ /–	Used to change the value (parameter) of the selected item.
+	Changes the current value of the selected item to the next value (increment).
–	Changes the current value of the selected item to the previous value (decrement).
F1	Displays the help of the key operations on the SETUP screen.
F2	Returns all the settings (except for *1 below) to the values before the change.
F3	Returns all the settings (except for *1 below) to their default values.
F4	Used to save the set parameters and exit from SETUP.
Esc	Used to return to the previous screen. If you press this key continuously, the cursor advances to the **Save & Exit** menu.
Enter	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

                                                       Set the Date. Use Tab to
         NEC US310e Series                             switch between Date elements.
         BIOS Version                US310e v1.49
         Build Date and Time         11/07/2014 15:49:32

         Memory Information
         Total Memory                2048 MB

         TXE Information
         TXE FW Version              01.01.00.1089

         System Date                 [Fri 12/12/2014]
         System Time                 [12:14:43]
                                                       ++: 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 US310e in any of the following circumstances: • **After transportation of US310e** • **After storage of US310e** 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**, 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.
```
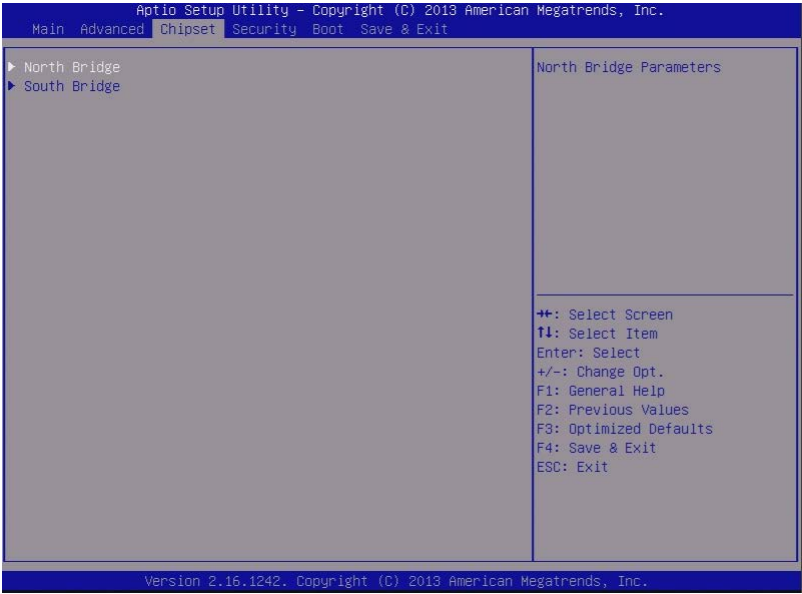
4.4.4   Intel IGD Configuration

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.
```
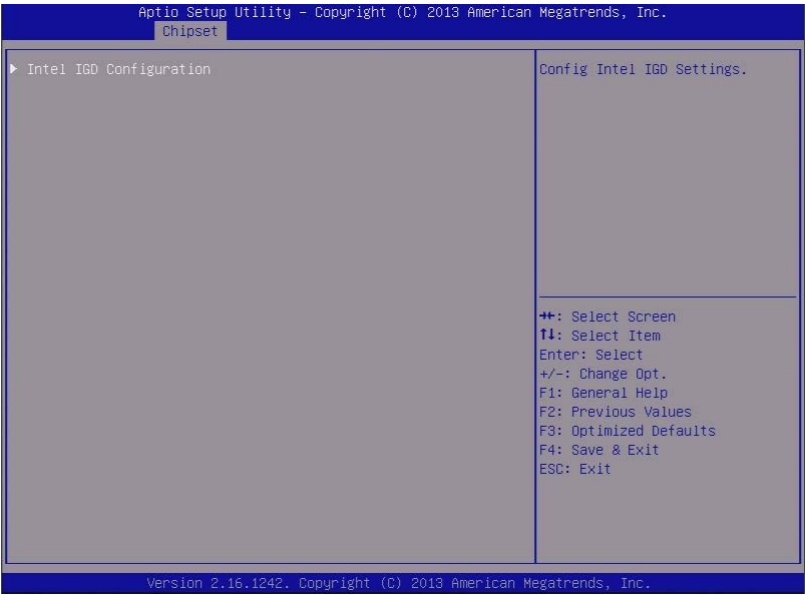
See the table below for each item.

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.
```
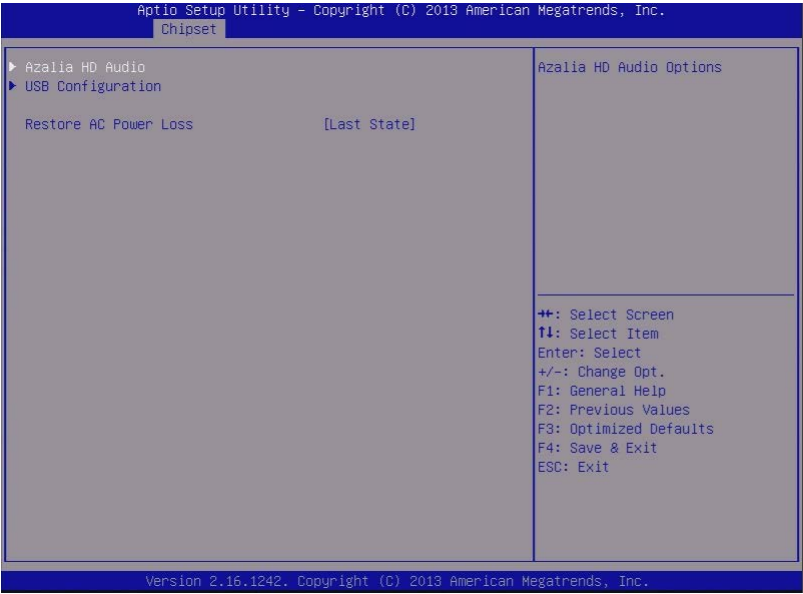
See the table below for each item.

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's password is set,
    then this only limits access to Setup and is
    only asked for when entering Setup.
    If ONLY the User's password is set, then this
    is a power on password and must be entered to
    boot or enter Setup. In Setup the User will
    have Administrator rights.
    The password is not case-sensitive and its
    length must be in the following range:
    Minimum length                3
    Maximum length                20
                                                     ←→: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
    Administrator Password                           +/-: Change Opt.
    User Password                                    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 **Security** menu screen and their functions are described below.

Item	Parameter	Description
Administrator Password	–	Set the Administrator password.
User Password	–	Set the User password.

4.4.7   Boot

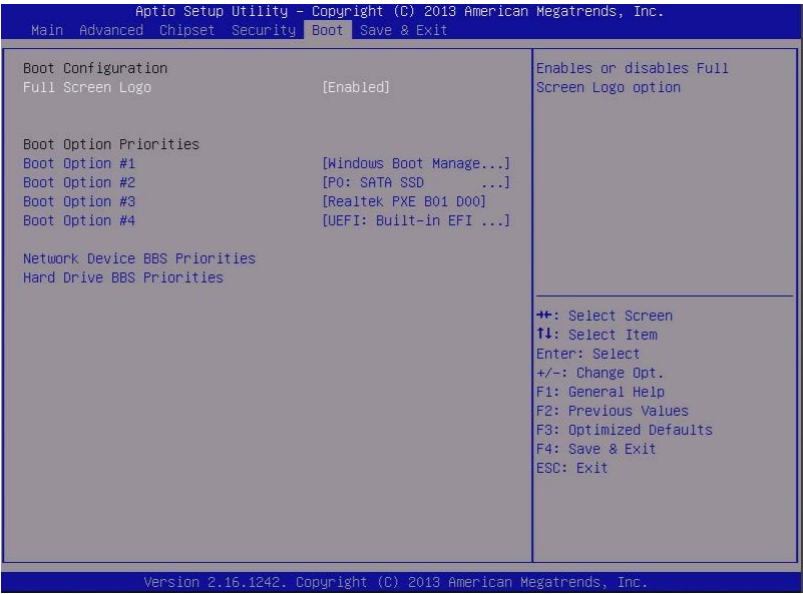If you move the cursor to **Boot**, the **Boot** menu appears.

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
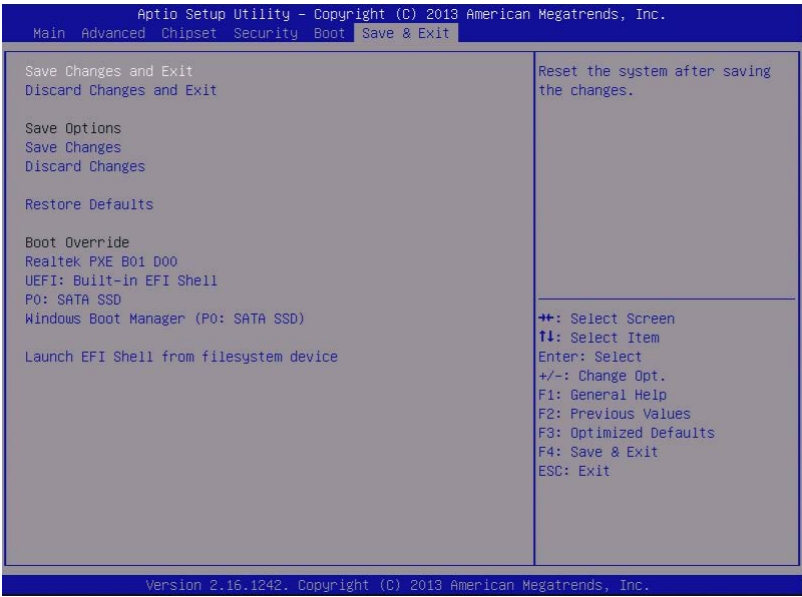
4. UEFI device

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

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                                        →←: Select Screen
  Windows Boot Manager (P0: SATA SSD)                 ↑↓: Select Item
                                                      Enter: Select
  Launch EFI Shell from filesystem device             +/-: 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
US310e**

Before Getting Started

Read this section before starting work on US310e.

1. **About UWF (Unified Write Filter)**

    Describes UWF (Unified Writer Filter).

2. **About Default User Accounts**

    Describes the default user accounts.

3. **About 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 US310e to a printer.

6. **Connecting to a Monitor**

    Describes how to connect US310e to a monitor.

1. About UWF (Unified Write Filter)

Before getting started on client configuration through the Atrust Client Setup console or through the Windows Embedded Standard 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 Embedded-based system.

By default, your US310e 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 US310e 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 US310e. 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. About Default User Accounts

There are two default user accounts for your US310e: 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

Note	The passwords are case sensitive.

Each user account belongs to the groups shown below.

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

US310e 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 Embedded 8 Standard OS, US310e imposes the following access restrictions on the default accounts to provide a more secure environment.

Access restrictions by user (○: Not restricted, ×: Restricted)		
Item	Administrator	User
Use of Windows Update	×	×
Enabling Windows Defender	×	×
Enabling or disabling Windows features	×	×
Displaying recycle bin	×	×
Recycling feature of recycle bin	×	×
Simple switchover of sign-in user	×	×
Sign-in option	×	×
Change of account picture	×	×
Use of disk cleanup tool	×	×
Performance information and tools	×	×
Use of BitLocker drive encryption	○	×
Accessing local drive	○	×
Redirecting to C drive	○	×
Displaying context menu (right-click menu)	○	×
Locking workstation	○	×
Use of Explorer	○	×
Use of Windows logo shortcut key	○	×
Auto replay of USB device	○	×
Relocation of taskbar	○	×
Run command	○	×
Change of Start menu	○	×
Use of Help	○	×
Saving recent files	○	×
Saving jump list	○	×
Changing desktop background	○	×
Windows firewall	○	×
Task Manager	○	×
Action Center	○	×
System	○	×
Device Manager	○	×
Add or Remove Programs	○	×
User account	○	×
Administrative tools	○	×
Credential Manager	○	×
Sync Center	○	×
Windows Fax and Scan	○	×
Steps Recorder	○	×
Paint	○	×
Notepad	○	×
Character codes	○	×
Wordpad	○	×
Command Prompt	○	×
Windows PowerShell	○	×
Computer	○	×
Use of Atrust Client Setup	○	×

3. About the Behavior of System Startup

Every time US310e is started up, you will automatically log in to the Windows Embedded operating system using the default standard user account.

Note	You will also log in using the default user account after signing out.

3.1 Switching the Sign-In User

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

1. Restart your US310e.

2. When the NEC logo appears at OS bootup, press and hold the **Shift** key on the keyboard until the screen to select the sign-in user appears.
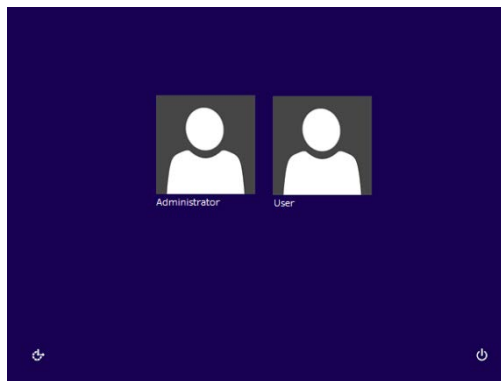
Note	If the **Shift** key is not pressed in time, the screen to select the sign-in user may not be displayed, and you will be automatically signed in to a standard user account. In this case, sign out from the user account while pressing the **Shift** key to move to the screen to select the user.

3. Select the user account to sign in with, enter your password, and then click **OK**.
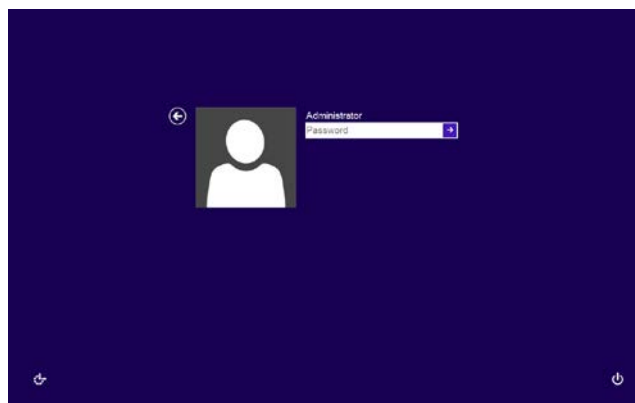
You can change the user account after you have signed out.

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

4. Sign out from the system while pressing the **Shift** key on the keyboard.

5. The screen to select the sign-in user appears.
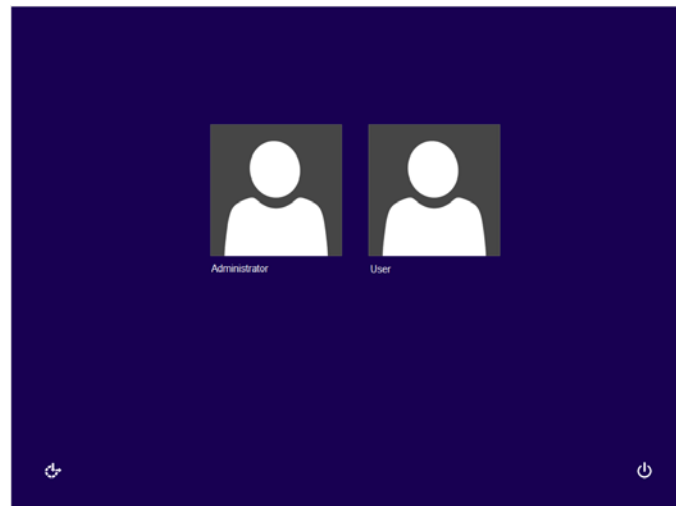
| Note | If the **Shift** key is not pressed in time, the screen to select the sign-in user may not be displayed. In this case, repeat the procedure from step 1. |

6. Select the user account to sign in with, enter your password, and then click **OK**.
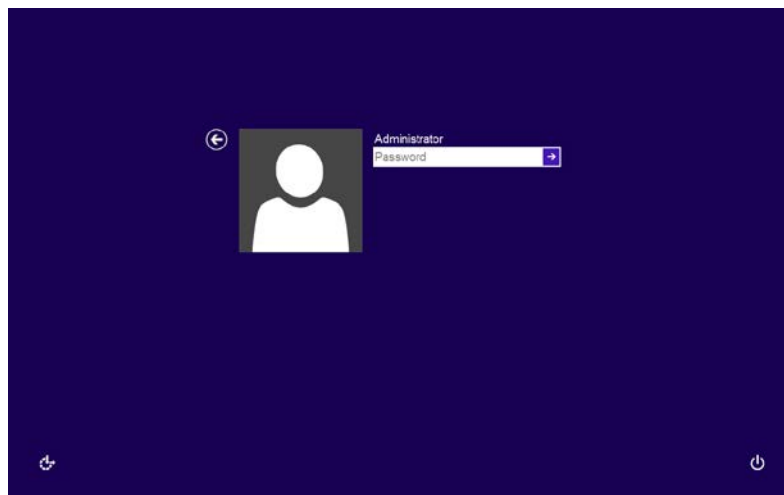
4. Standard / Customized Desktop Shortcuts

With US310e, 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 Embedded 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 US310e".

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 US310e.

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 US310e.
	• If you want to connect a parallel printer to US310e, you need to prepare a USB-parallel printer cable (not supplied with US310e).

𝟔. Connecting to a Monitor

US310e 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, "12. 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 US310e

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.

3

NEC Express5800 Series
US310e

Using US310e

This chapter provides the basics of how to use your US310e.

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 View Services

Describes how to access VMware View and Horizon View 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	VMware Horizon View Client	Double click to access VMware View and VMware Horizon View services.
3	Remote Desktop Connection	Double click to access Microsoft Remote Desktop 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 screen or the desktop taskbar.

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.
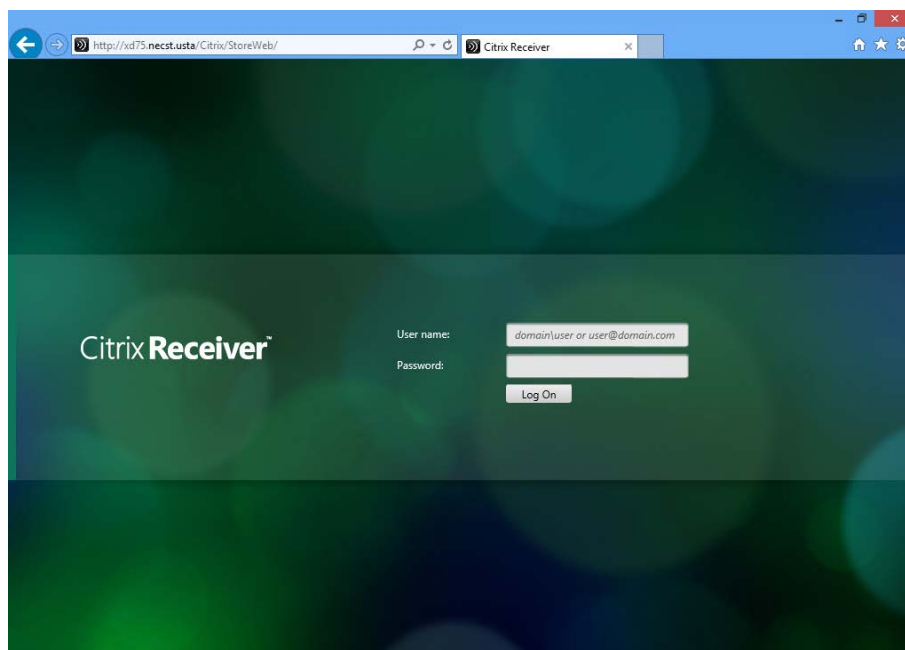
Logon Screen Example (XenDesktop 7.6 Platinum)
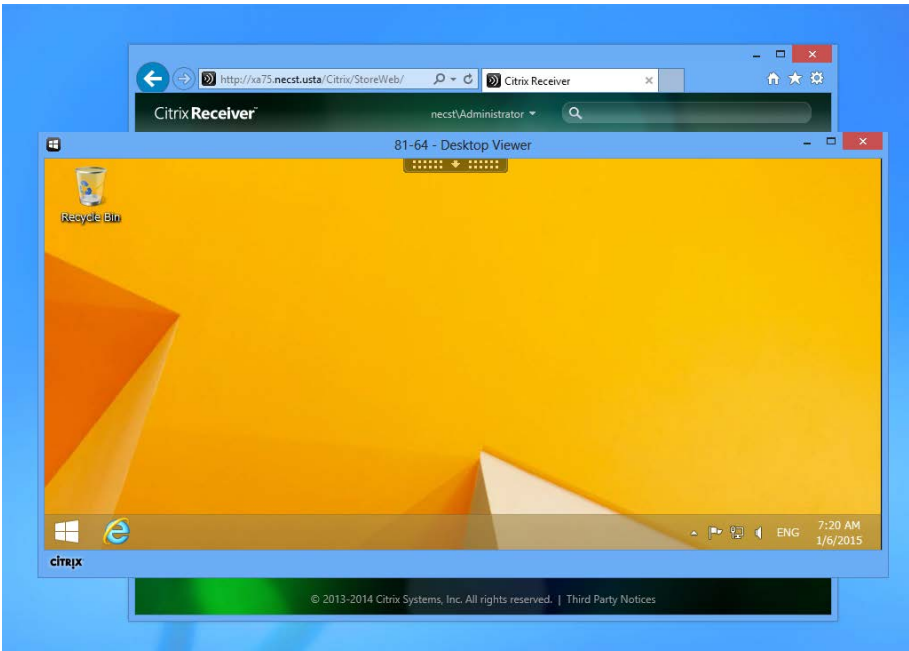
Virtual Desktop Example (Windows 8.1 Enterprise)
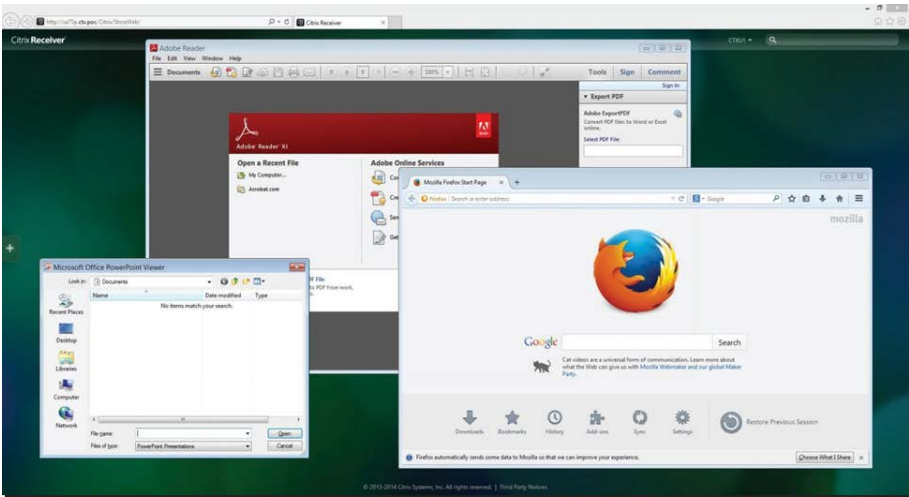
Virtual Application Examples

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 import a certificate.

Note   For how to import a certificate, see Chapter 5, "16. Saving 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 **Next** to continue.
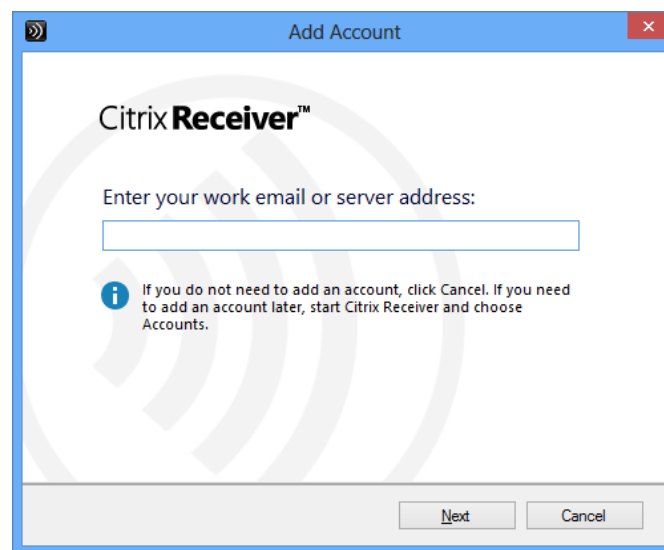
4. Log on with the credentials for your Citrix services.
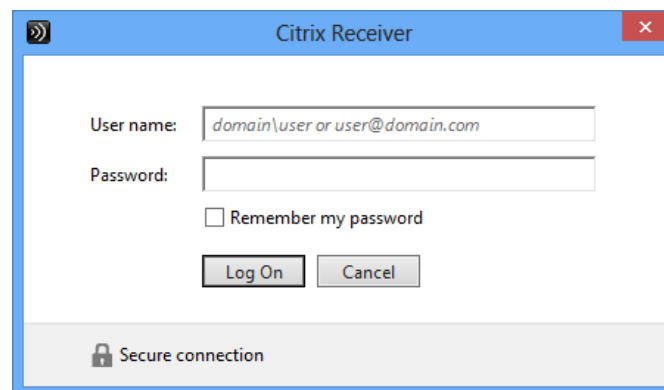
5. Click **Yes** to optimize your Citrix access.

6. When access has been optimized, a success message appears. Click **Finish** to continue.

7. 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.
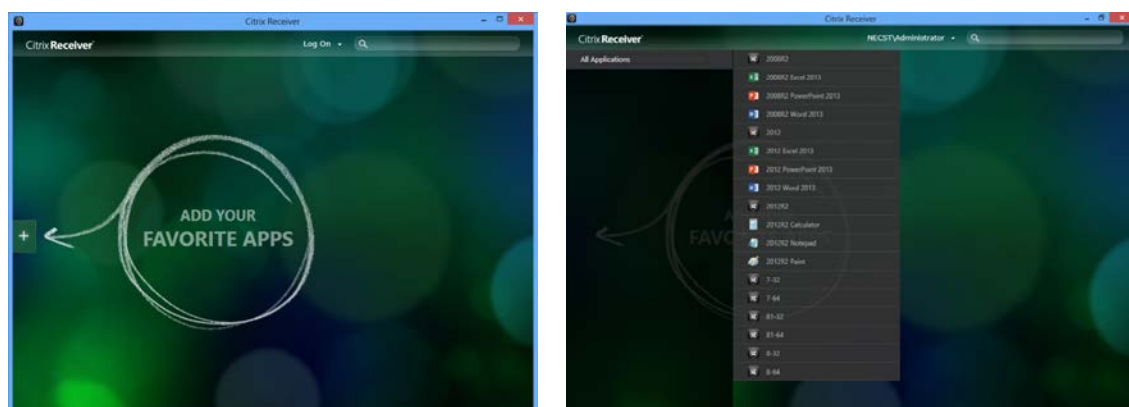
8. Now you can launch the desired application. The virtual desktop or application will be displayed on the screen.

3. Accessing Microsoft Remote Desktop Services

You can access Microsoft Remote Desktop Services:

- By using Remote Desktop Connection
- By 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**.
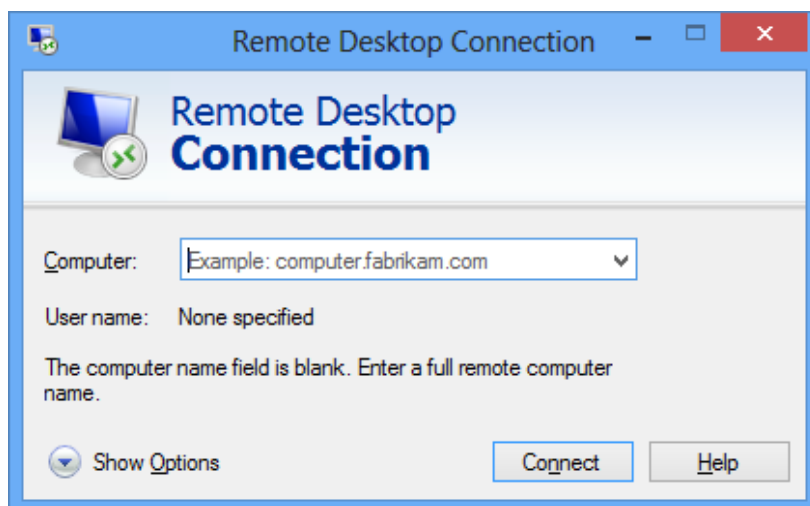
3. Enter your credentials, and then click **OK**.
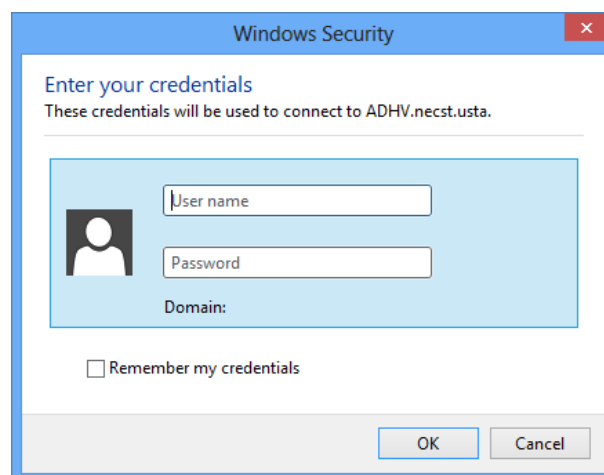
4. A window may appear with a certificate message about the remote computer. Consult your system administrator for details. To bypass, click **Yes** to continue.
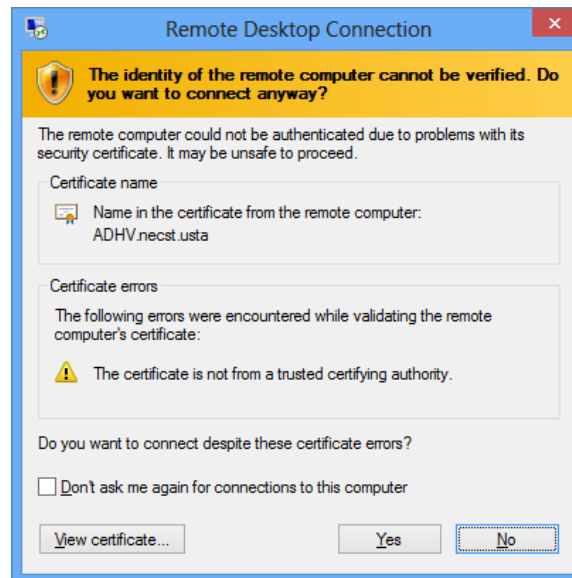
5. US310e is connected to the remote desktop, and the virtual desktop will be displayed on the screen.

3.2　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 import a certificate.

Note	For how to import a certificate, see Chapter 5, "16. Saving the Certificate".
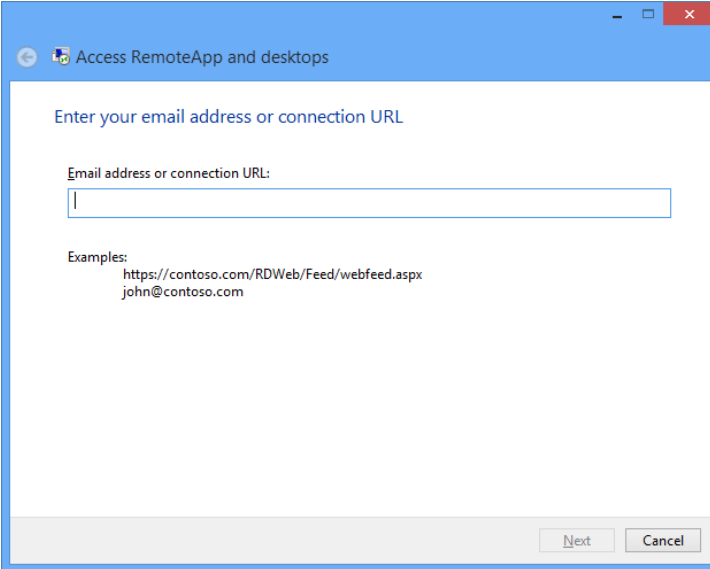
2. On your desktop, move the mouse pointer to the bottom-left corner, and right-click **Start** to open the popup menu.

3. Click **Control Panel**.

4. Select **RemoteApp and Desktop Connections**.
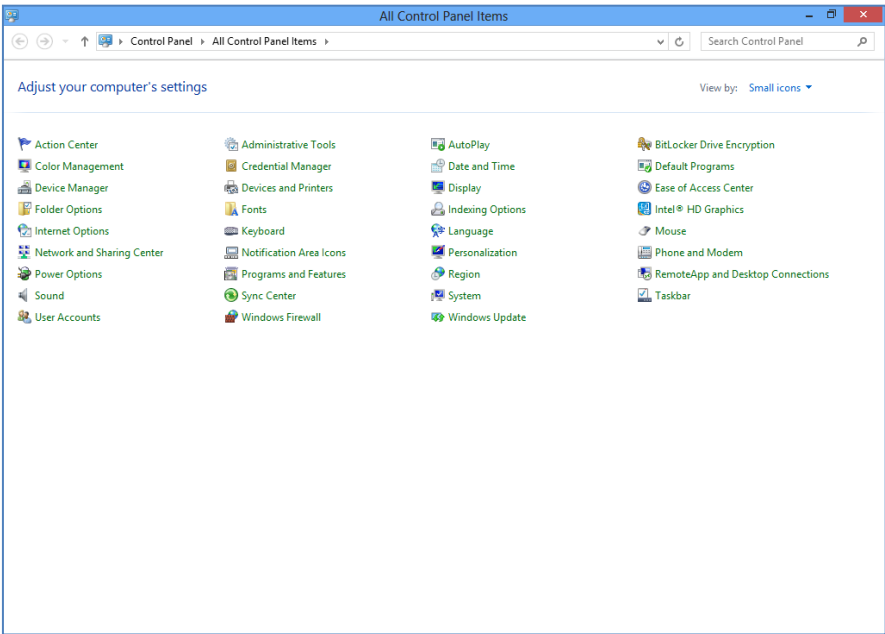
5. Click **Access RemoteApp and Desktops** on the left pane.
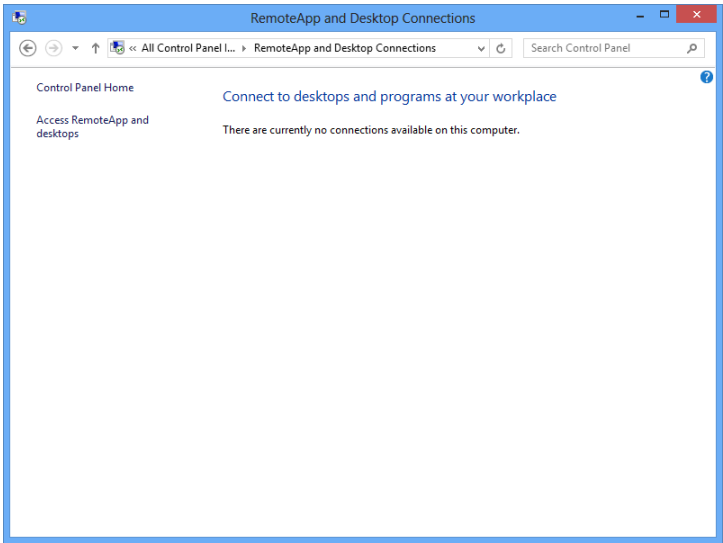
6. A window appears prompting your to enter your email address or connection URL. Consult your system administrator for the proper information to provide here, enter the required data, and then click **Next** to continue.

7. A window indicating that you are ready to set up the connection appears. Click **Next**.
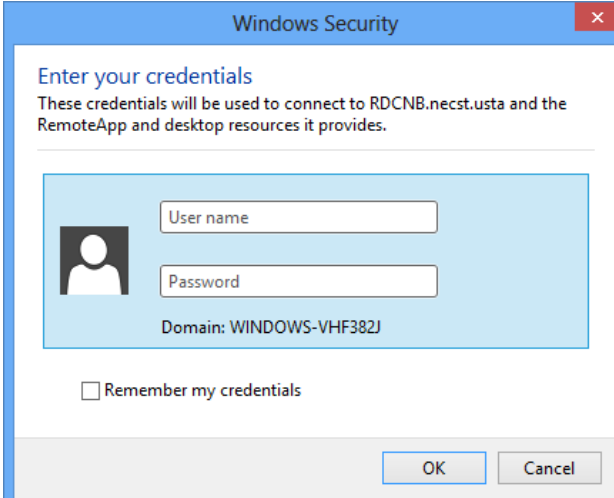
8. Type in your credentials, and then click **OK**.

9. A window indicating that connection is properly set up appears. Click **Finish**.
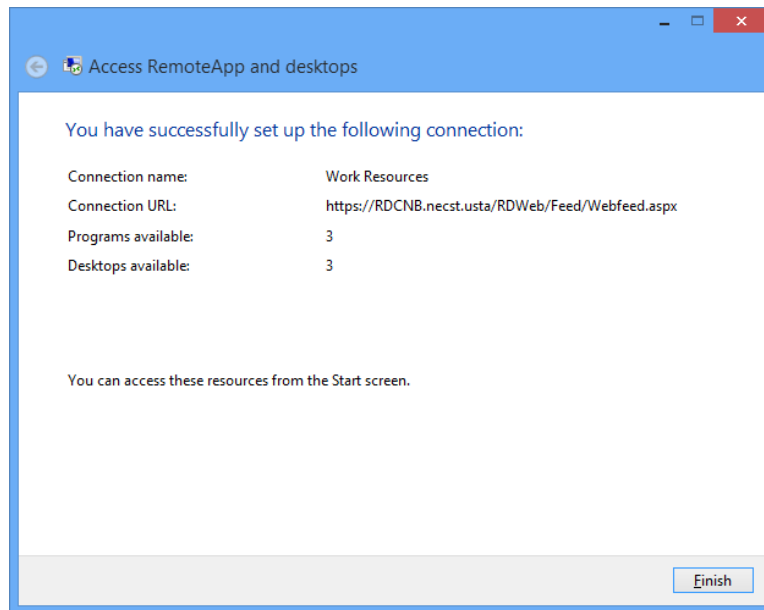
10. When the information you have specified in the steps above is displayed in **RemoteApp and Desktop Connections**, close the **RemoteApp and Desktop Connections** window.
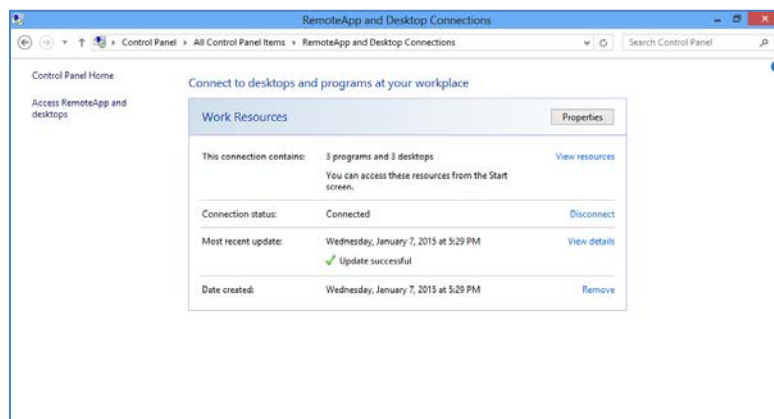
11. Icons for published applications and desktops for remote desktop services are displayed on the **Start** screen.
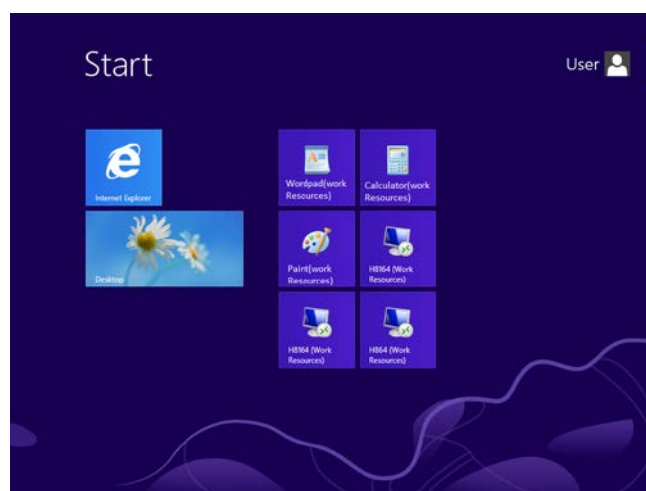
12. Click an icon on the **Start** screen to connect to a desktop or application.

3.3   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 import a certificate.

Note   For how to import a certificate, see Chapter 5, "16. Saving 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**.
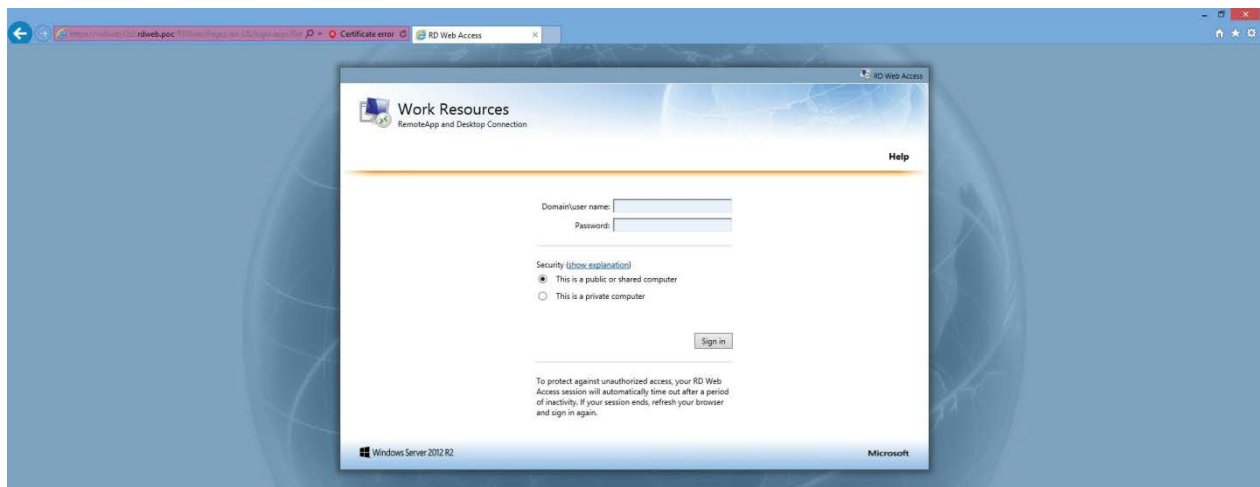
Note   A message window may appear prompting you to permit the execution of "Microsoft Remote Desktop Services Web Access Control" add-ons. Select "Permit" in this case.

5. Icons for connecting to desktops and applications published by Remote Desktop Services are displayed.
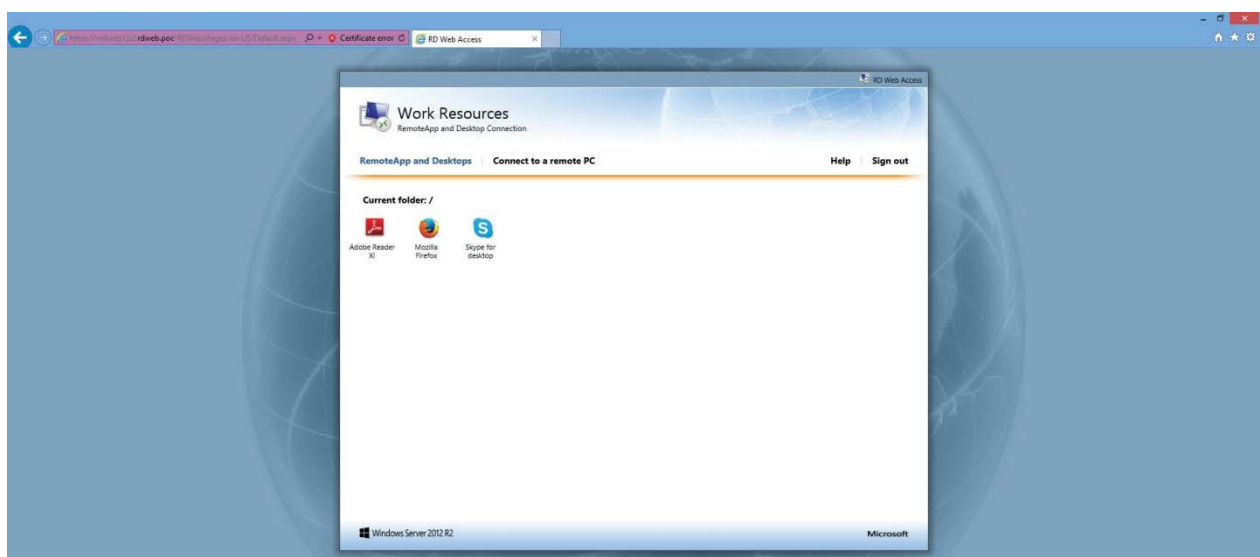
6. Select an icon to connect with a desktop or application.

4. Accessing VMware View and Horizon View Services

You can access VMware View and Horizon View Services:

- By using VMware Horizon View Client

- From your Web browser (Internet Explorer)

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

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

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

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

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

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

Note	For how to import a certificate, see Chapter 5, "16. Saving 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**.

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 View Services by Using Internet Explorer

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

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

Note	For how to import a certificate, see Chapter 5, "16. Saving 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 View Services will be accessed.

4. Enter your credentials, and then click **Sign In**.
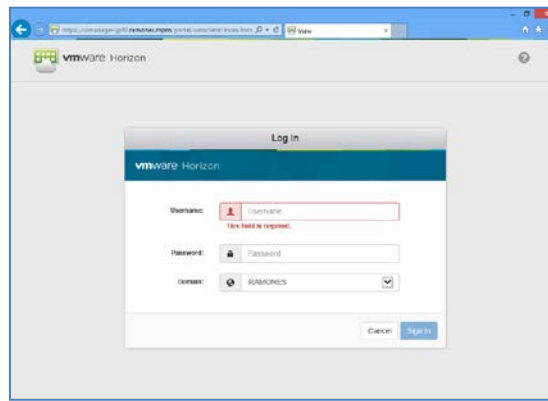
5. Icons for connecting to virtual desktops registered in VMware View and Horizon View Services are displayed.
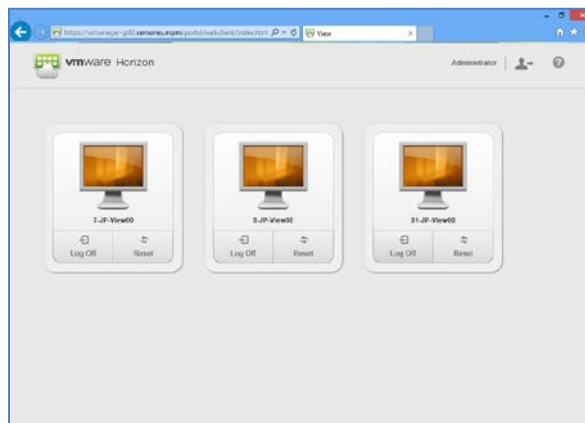
6. Select an icon to connect with a virtual desktop.

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 US310e (it is not installed by default).
	Your US310e contains a CMO Terminal Agent installer. See Chapter 5, "13. 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**.

3. A list of virtual desktops registered in NEC Client Management Option (CMO) Services is displayed.
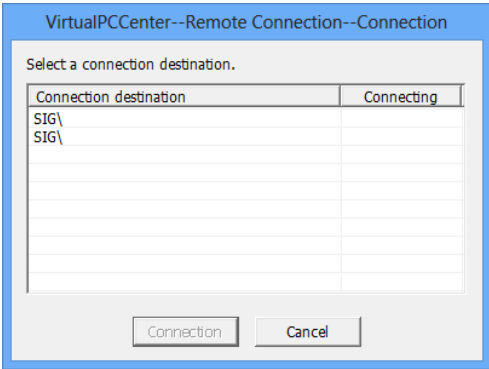
4. Select the virtual desktop you want to connect to, and then click **Connection**.
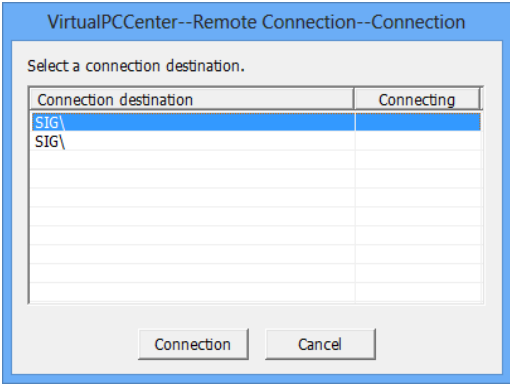
5. The client is connected to the selected virtual desktop.

❻. Browsing the Internet by Using Internet Explorer

Use Microsoft Internet Explorer 10 to browse the Internet. To launch the browser, click **Start** > **Internet Explorer**.

NEC Express5800 Series
US310e

4
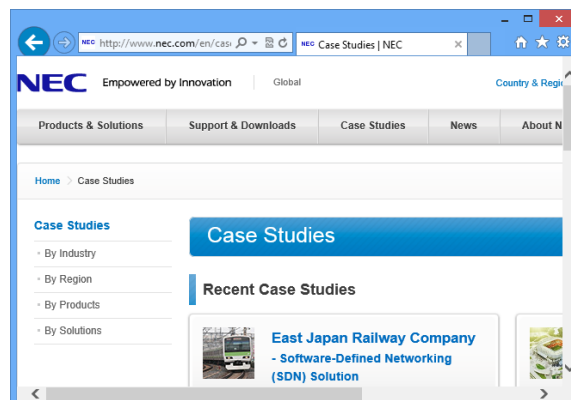
Configuring Client Settings with Atrust Client Setup

This chapter provides instructions on how to configure your US310e 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

1.1   Interface Overview

To access Atrust Client Setup on your US310e thin client, do the following:

1. Log in to your US310e with an administrator account (see Chapter 2 "2. About Default User Accounts" for the default account).

2. Click **Atrust Client Setup** on the Start screen.

3. The Atrust Client Setup window appears.
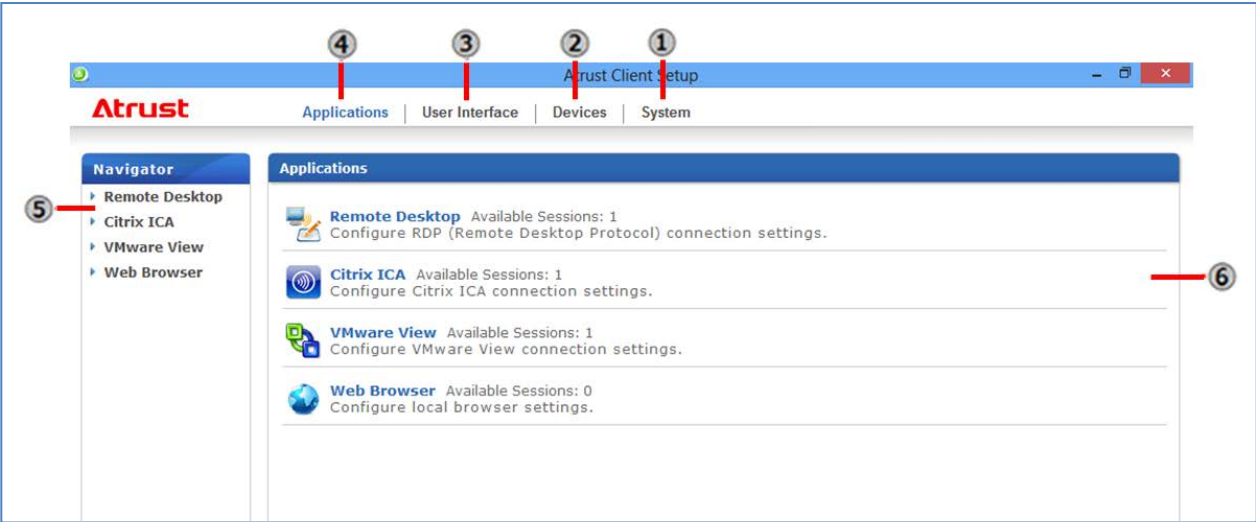
No.	Name	Description
1	System tab	Click to configure settings for the operation and maintenance of the client.
2	Devices tab	Click to configure settings for external devices of the client.
3	User Interface tab	Click to configure the user interface of the client.
4	Applications tab	Click to configure 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 passwords • Configuring remote assistance settings • Updating firmware • Taking snapshots for mass deployment • Enabling/Disabling the Appliance mode • Configuring UWF (Unified Write Filter) settings	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 the display of service access shortcuts	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.
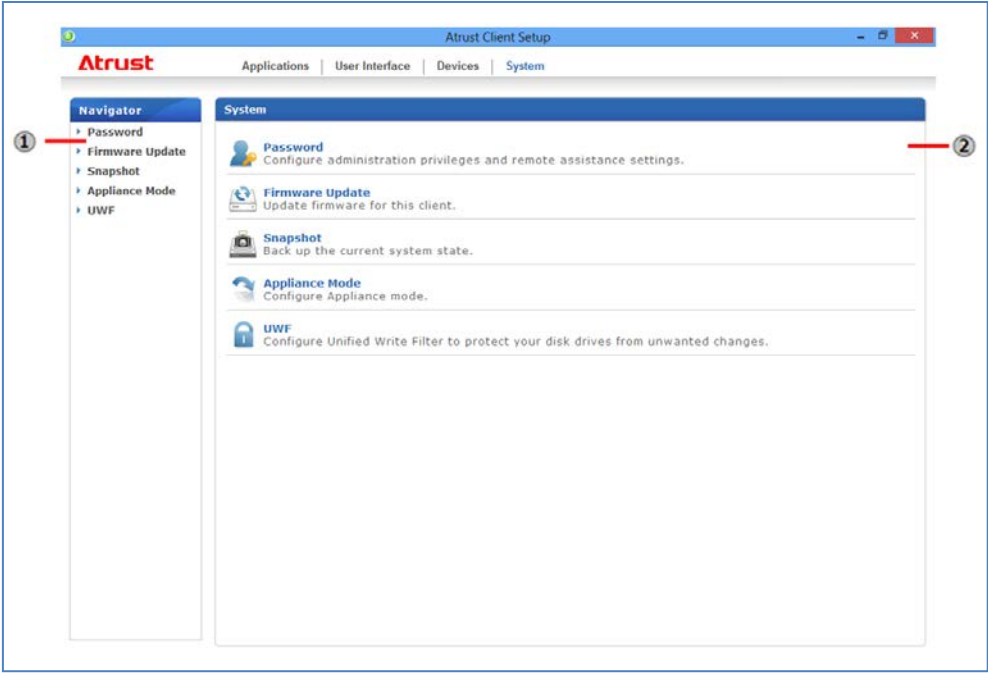
No.	Name	Description
1	Navigation area	Click to select a setting item under **System** tab.
2	Configuration area	Configures setting values when a setting item is selected.

2.2 Available Settings

Tab	Setting	Icon	Description	Section page
System	Password		Click to configure the access privileges of Atrust Client Setup for client users. Click to configure settings for remote assistance.	• Chapter 4, "2.3 Configuring the Access Privileges and Password of 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)".

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   Configuring the Access Privileges and Password of Atrust Client Setup

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

2.3.1   Setting Access Privileges and Password Only for Administrators

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

Note	System administrators (and only administrators) are allowed to access Atrust Client Setup by default. If you don't enable user authentication for administrators and don't set a password here, the system administrator privileges are sufficient to access Atrust Client Setup. If authentication is enabled and the password is set, administrators will need that password to enter Atrust Client Setup.

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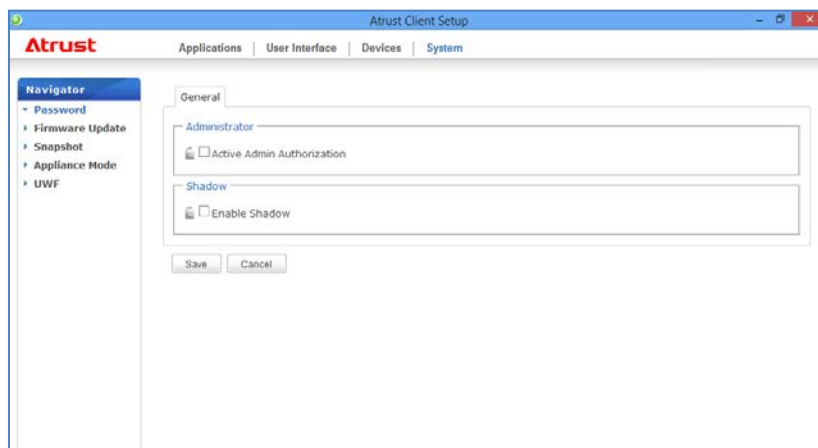
2. Under the Administrator section, click to check **Active Admin Authorization**.

3. The access privileges for administrators are granted and a window appears for you to set the password.
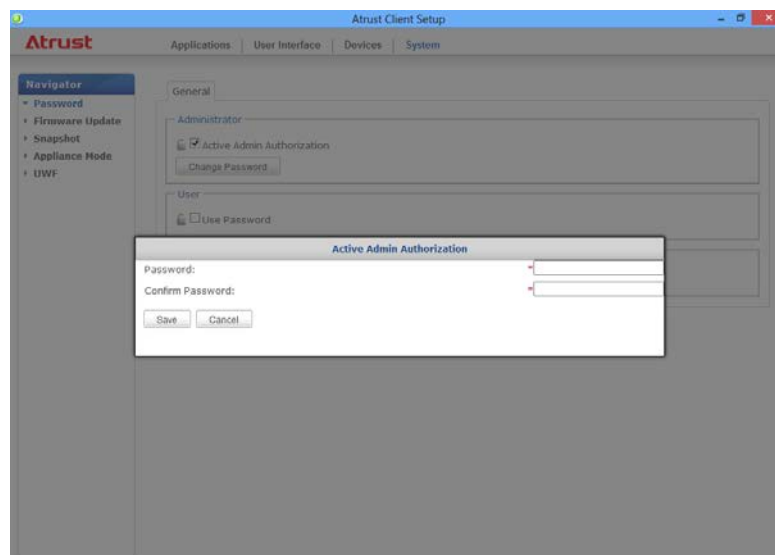
4. Type in the desired password, and then click **Save** to apply.

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

2.3.2   Setting Access Privileges and Password Also for Standard Users

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

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

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

2. Under the User section, click to check **Use Password**.
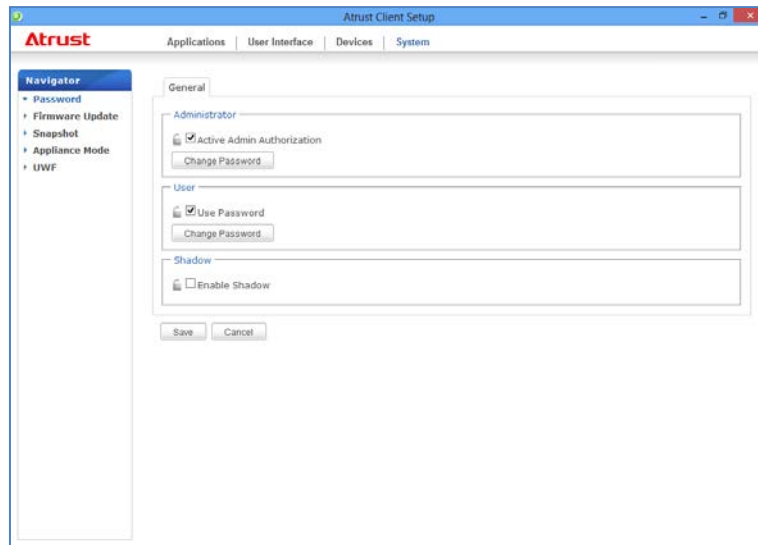
3. The access privileges for standard users are granted and a window appears for you to set the password.
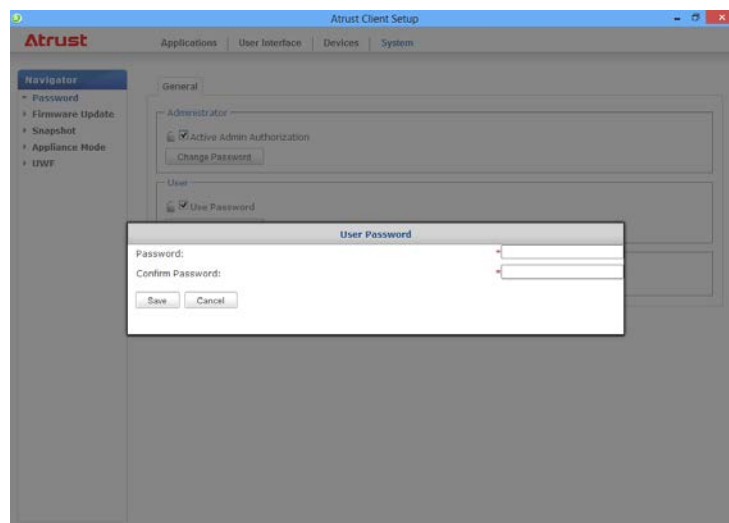
4. Type in the desired password, and then click **Save** to apply.

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

Note	For standard users of your US310e, two set of credentials are required to access Atrust Client Setup: one set of credentials is administrator credentials for Windows Embedded 8 Standard; the other is standard user credentials for Atrust Client Setup.

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	VNC (remote shadow) is useful, but has known security vulnerabilities. If the remote shadow feature is enabled on US310e, anyone who knows the password can connect to US310e from other VNC client software as well as from Atrust Device Manager.
	It is therefore important to implement security measures (such as using VNC only within the firewall or disabling VNC when it is not being used) when using this feature.

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 the password for remote assistance, do the following:

1. On Atrust Client Setup, click **System** > **Password**.
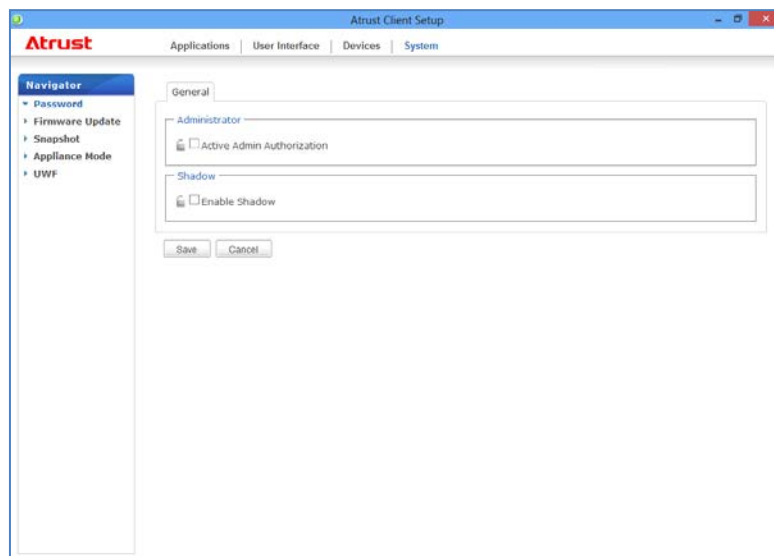
2. Under the Shadow section, click **Enable Shadow**.

3. The Shadow feature is enabled and a window appears for you to set the password for remote assistance.
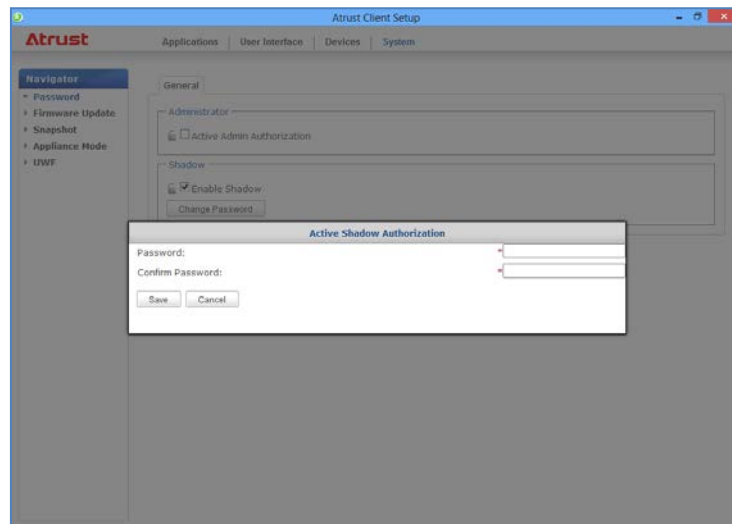
Note	When the Shadow feature is enabled, on US310e, the icon will appear in the Notification area of the Task bar. If this feature is currently being performed from a remote computer, the icon will change its color to yellow .

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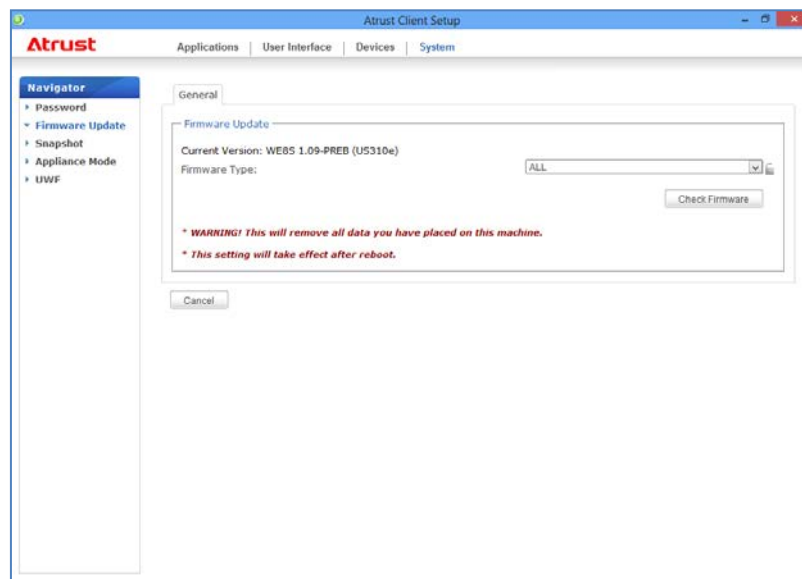
2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Firmware**. The system will then automatically download the Firmware list from the remote computer.

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.
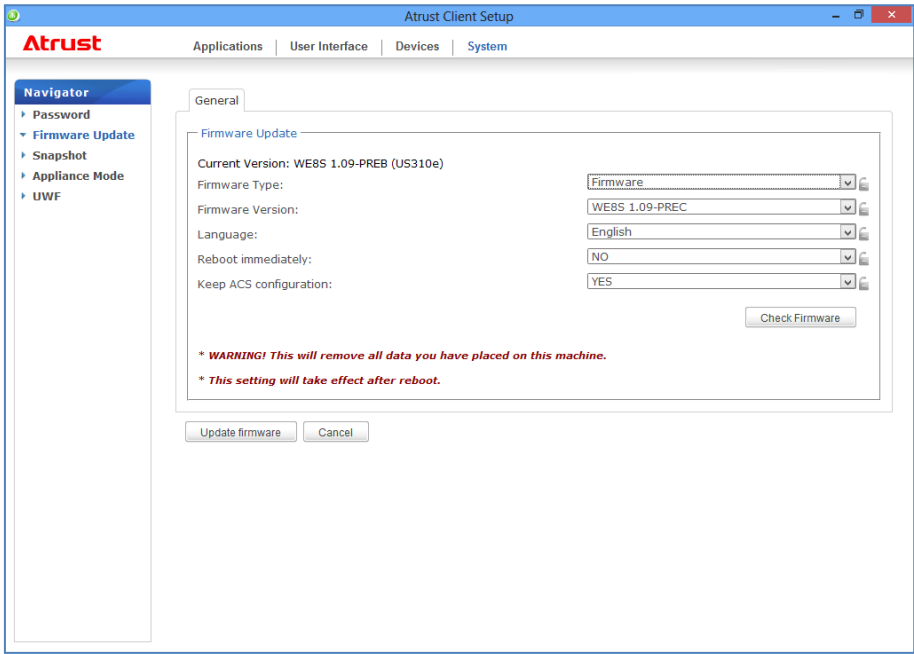
Firmware Update Options	
Item	**Description**
Firmware Type	Click to select the desired firmware type. | Type	Description | |---|---| | **ALL** | All firmware types, **Firmware** and **Snapshot**. | | **Firmware** | The system image of a client. | | **Snapshot** | The system image of a client coming from another client of the same model. |
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. About the Behavior of System Startup".

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

1. On Atrust Client Setup, click **System** > **Snapshot**.
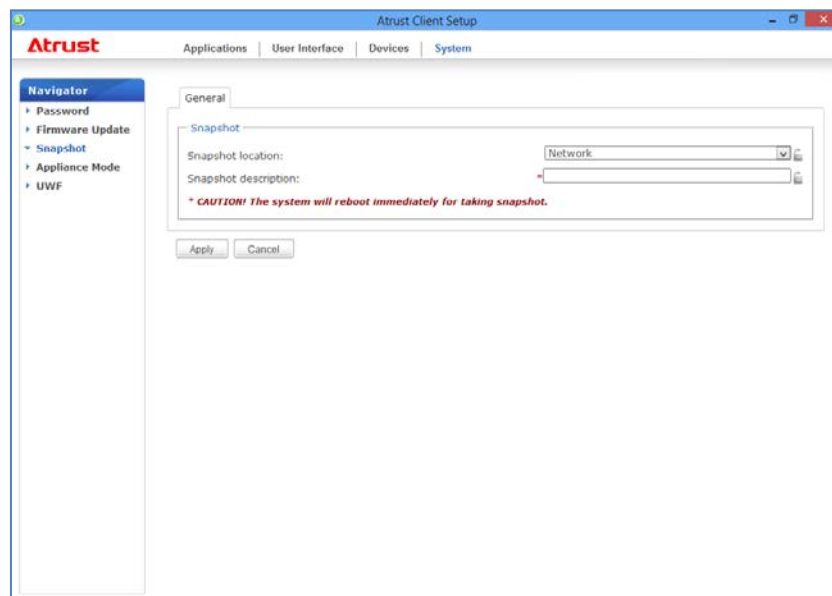
2. Under the Snapshot section, click the drop-down menu to select where to store the snapshot. Two options are available: **Network** and **USB**.

   – To store the snapshot file set on the remote computer, select **Network**.

   – To store the snapshot file set on the locally attached USB flash drive, select **USB**.

3. Type in the desired description for the snapshot, and then click **Apply**.

4. A message appears prompting for confirmation. Click **OK** to confirm.

5. The system will restart to complete the process *automatically*.

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

2.7   Deploying a System Image with a Created Snapshot

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

1. On Atrust Client Setup, click **System** > **Firmware Update**.
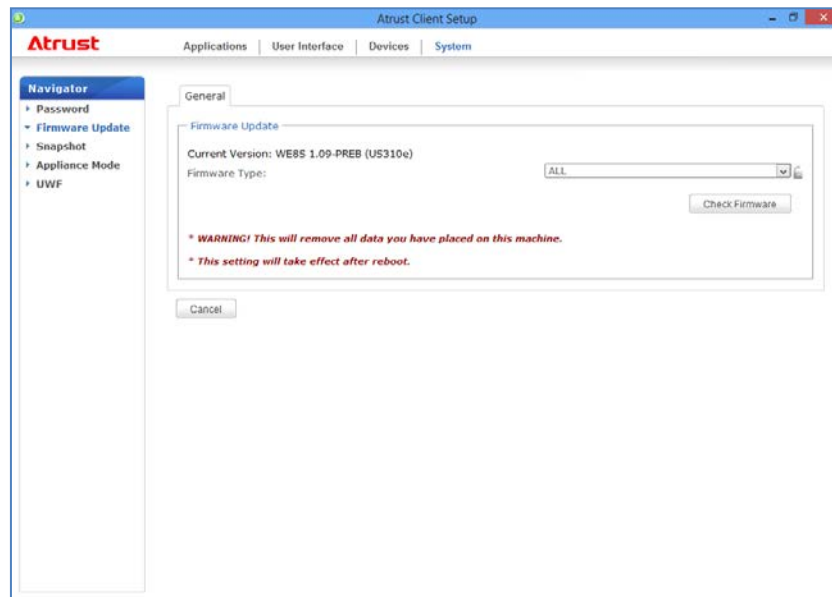
2. Under the Firmware Update section, click the Firmware Type drop-down menu to select **Snapshot**. The system will automatically download the Snapshot list from the remote computer.

3. Upon completion, a message appears notifying you that the Snapshot list has been loaded.

Note	Client snapshots stored on the remote computer are managed by Atrust Device Manager. For more information on how to manage client snapshots with Atrust Device Manager, refer to the User's Guide of Atrust Device Manager.

4. Click **OK** to continue.

5. Click drop-down menus to select the desired snapshot and other options.
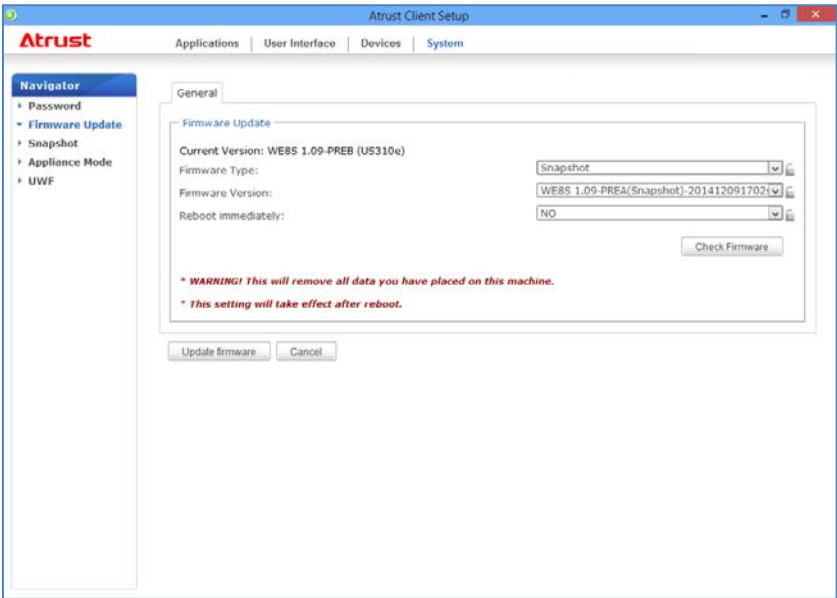
Options for Deploying a Snapshot	
Item	Description
Firmware Version	Click to select the desired snapshot from the Snapshot list.
Reboot immediately	Click to choose whether to restart the system immediately for firmware update or manually restart the system later.

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

With a Snapshot on a USB Flash Drive

To deploy a system image on your US310e with a snapshot on a USB flash drive, do the following:

(1) Plug the USB flash drive into a free USB port of the client.

(2) Start up or restart the client.

(3) During the period of POST (Power-On Self-Test), press **F7** to enter the Boot Device menu.

(4) Select to boot from the attached USB flash drive.

(5) Select **USB**, and then click **Next** to continue.
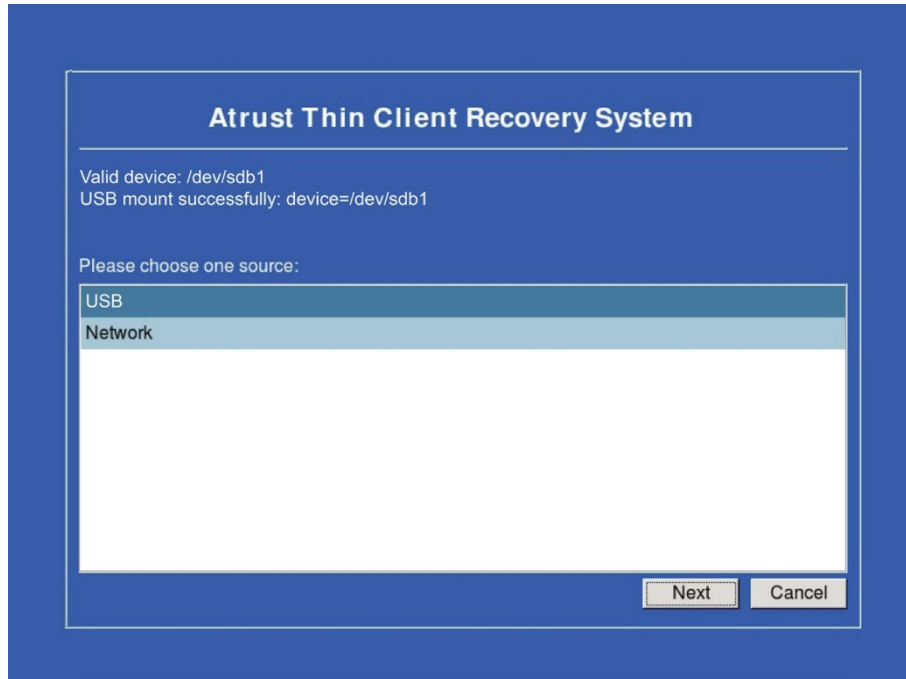
7. The recovery system starts deploying the snapshot to the client.

8. After completion, click **Finish** to restart the client.

2.8   Enabling or Disabling the Appliance Mode

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

Note

There are two modes for your thin client:

No.	Mode	Description
1	Appliance	The client will start up directly with the desired RDP / ICA / View session and turn off after exiting the session.
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 View session under **Applications** tab. You need to specify which service type and connection settings entry will be used under the Appliance mode. For detailed instructions, 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 View Connection Settings"

1. On Atrust Client Setup, click **System** > **Appliance Mode**.
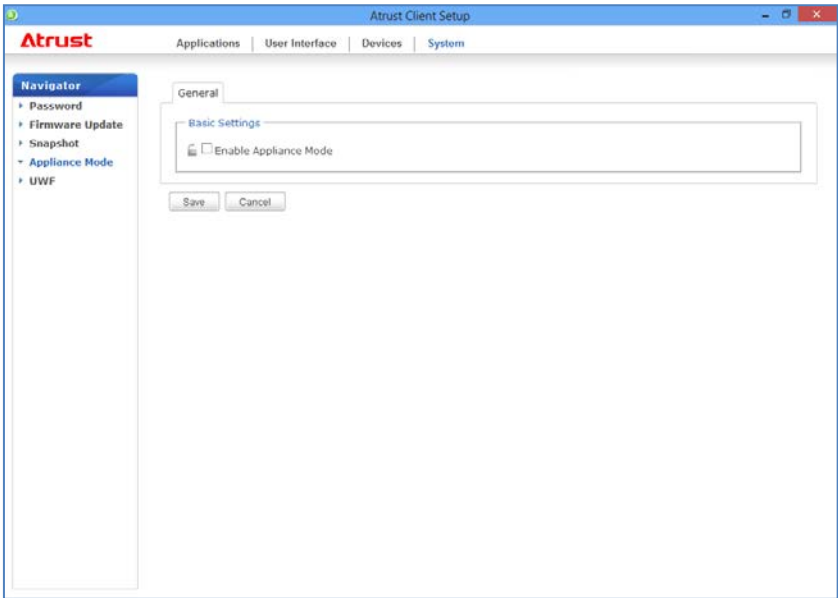
2. Click to check **Enable Appliance Mode**.

3. Other settings of the Appliance mode appear.
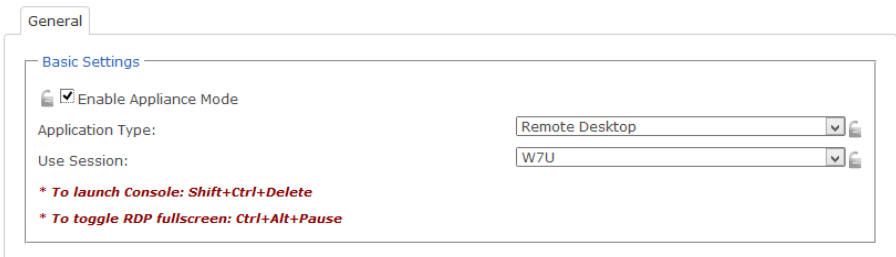
4. Click drop-down menus to select the application (or service) type: **Citrix ICA**, **Remote Desktop**, or **VMware View**, and the specific service available in that type.
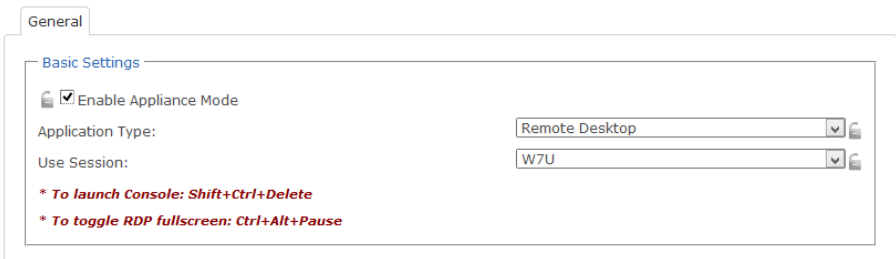
5. Click **Save** to confirm your selections.

6. The system will enter the Appliance mode after restart.

| **Note** | To disable the Appliance mode or to access Atrust Client Setup under the Appliance mode, 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. Under the Appliance mode, exit the Full Screen mode of the RDP / ICA session, or release the keyboard and mouse from the View session (virtual desktop):

    – To exit the Full Screen mode of the RDP session, press **Ctrl + Alt + Pause**.

    – To exit the Full Screen mode of the ICA session, use the XenDesktop toolbar at the top (You may not in the Full Screen mode).

    – To release the keyboard and mouse from the View session (virtual desktop), press **Ctrl + Alt**.

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

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

Note	You cannot access the Taskbar of the client operating system under the Appliance mode.

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

4. Click to uncheck **Enable Appliance Mode**, and then click **Save** to apply the change.

5. Return to the current RDP / ICA / View session:

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

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

6. Log off from the current RDP / ICA / View session.

7. The client will shut down. Restart your client manually.

2.9   Configuring UWF (Unified Write Filter)

Your US310e 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 feature is enabled by factory default. *Except for changes to ACS settings*, all the changes made in a session will not be kept after the system restart. Ensure that you choose the desired settings here before making any changes to the system.
	•	An icon in the Notification area of the Taskbar will indicate the current UWF state of your system. For details, see the description at the end of 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.
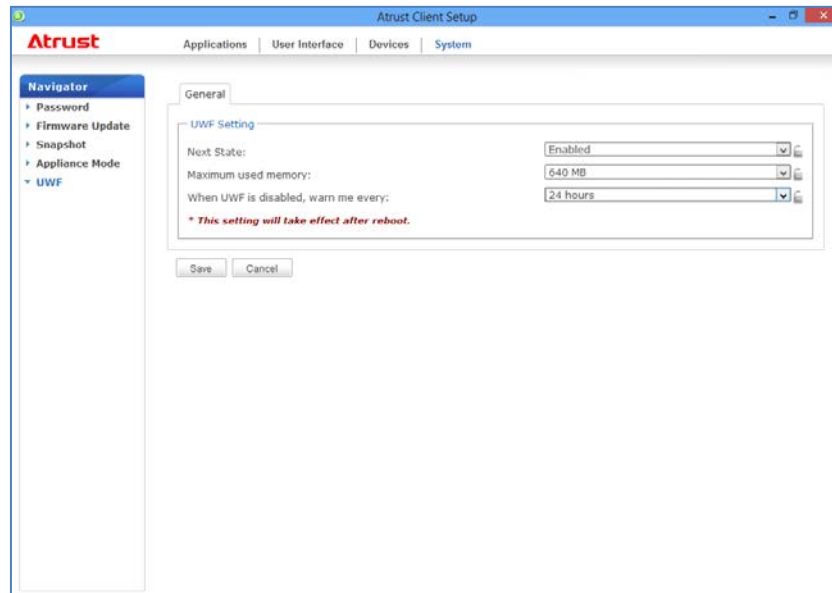
3. Click to select other options if needed.

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.

Tip	You can change the maximum memory size used *only when UWF is disabled*. Disable UWF first, and then change the memory size used. A restart is required when you switch the UWF state.
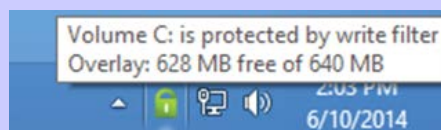
4. Click **Save** to confirm your selections.

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 US310e 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 US310e. Instead, you can use storage space on remote or virtual desktops, removable storage devices, or networks.

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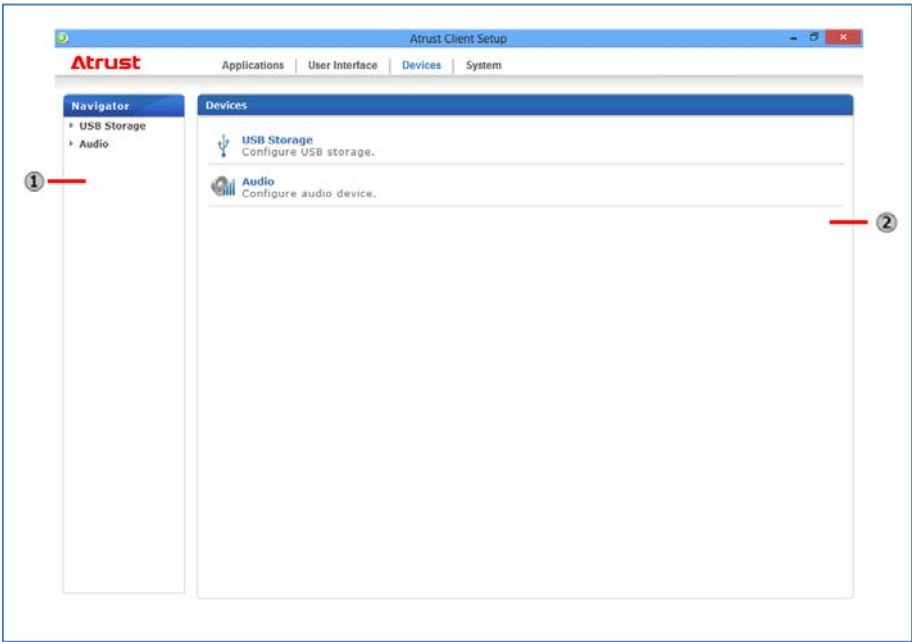
	Interface Elements	
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item on the **Devices** tab.
2	Configuration area	Configures setting values when a setting item is selected.

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**.

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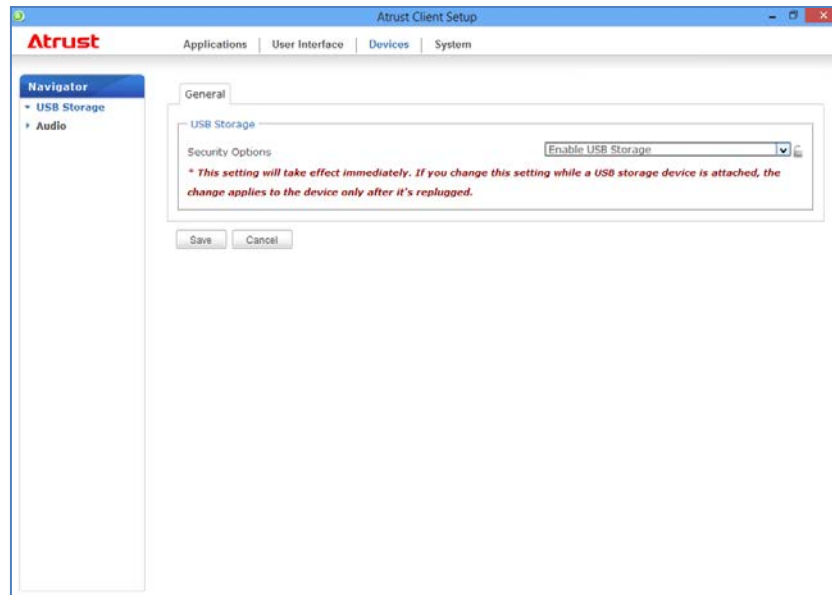
2. Click the drop-down menu to select the desired setting. Three options are available: **Enable USB Storage**, **Read-Only Access**, and **Disable USB Storage**.

Note	When **Enable USB Storage** is selected, settings of RDP / ICA connection entries under **Applications** tab may affect if you can use *mapped* USB storage devices in remote / virtual desktop sessions. For details, see sections: • Chapter 4, "5.5 Configuring Advanced RDP Connection Settings" • Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"
Important	**When Disable USB Storage is selected, Citrix ICA and VMware View / Horizon View sessions may still allow users to use locally attached USB storage devices through redirection. To really prevent the use of USB storage devices in virtual desktop sessions, some configurations in Citrix and VMware service delivery environments are required.**

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

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**.
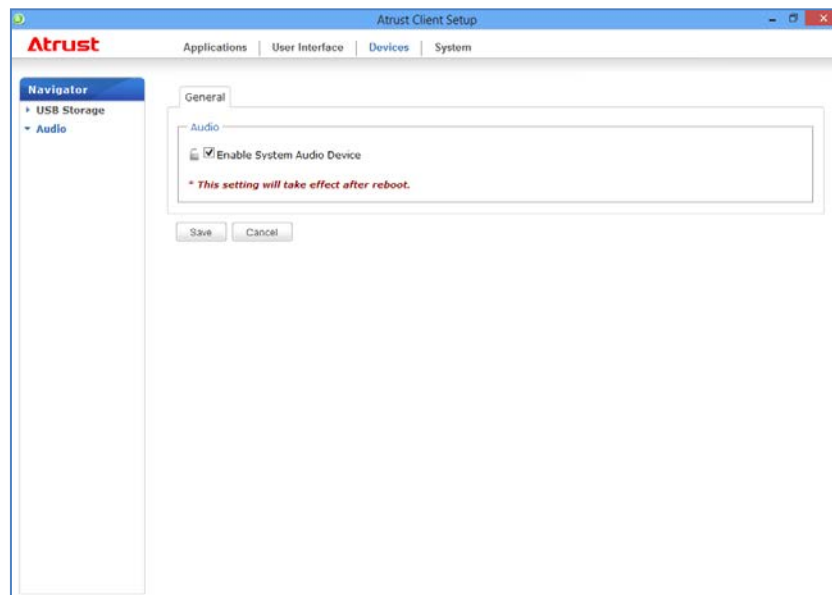
2. Click to check/uncheck **Enable System Audio Device**.

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.

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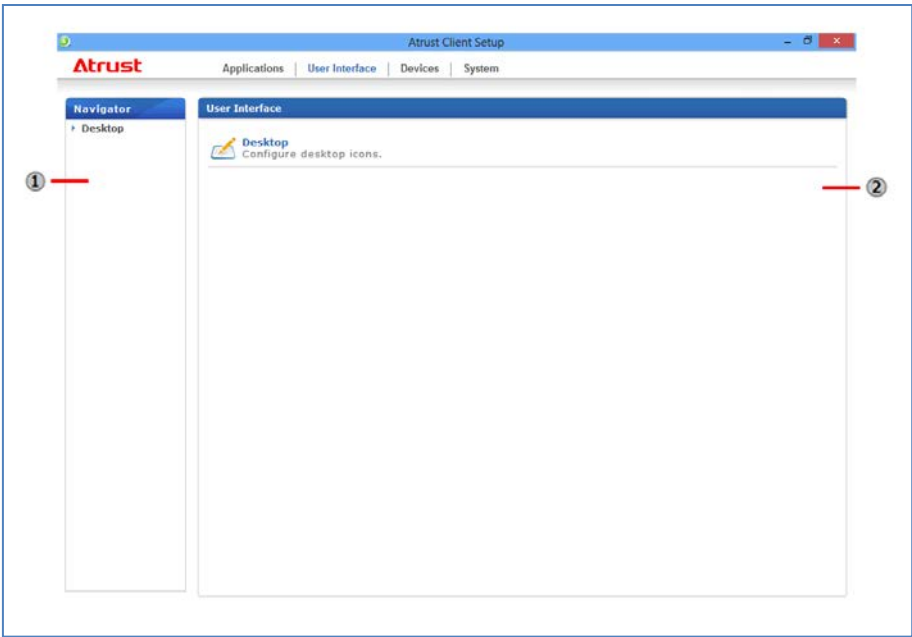
Interface Elements		
No.	**Name**	**Description**
1	Navigation area	Click to select a setting item under **User Interface** tab.
2	Configuration area	Configures setting values when a setting item is selected.

4.2 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

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

Remote Desktop Connection   Citrix Receiver   VMware Horizon View Client

Tip	You can use these standard desktop shortcuts to quickly access services. For detailed instructions, 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**.
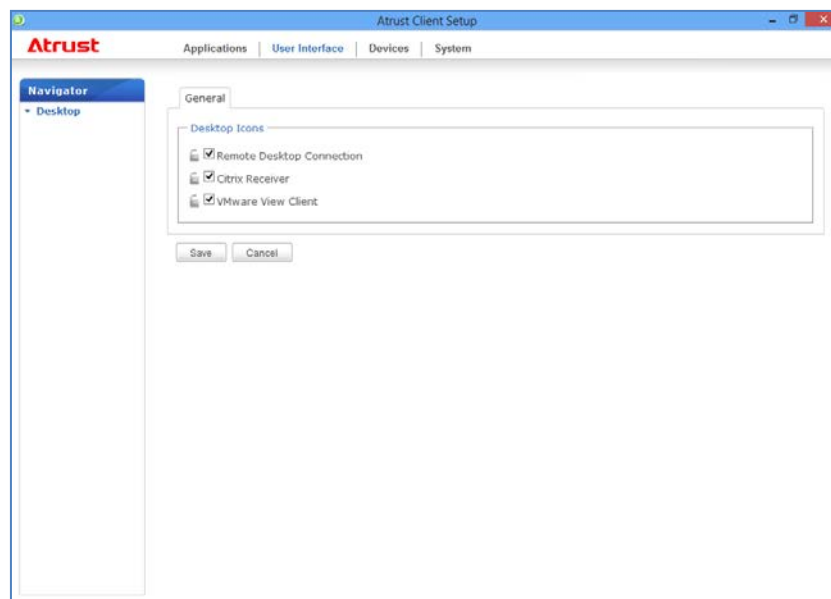
2. Click to check/uncheck **Remote Desktop Connection**, **Citrix Receiver**, or **VMware View Client**.

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.

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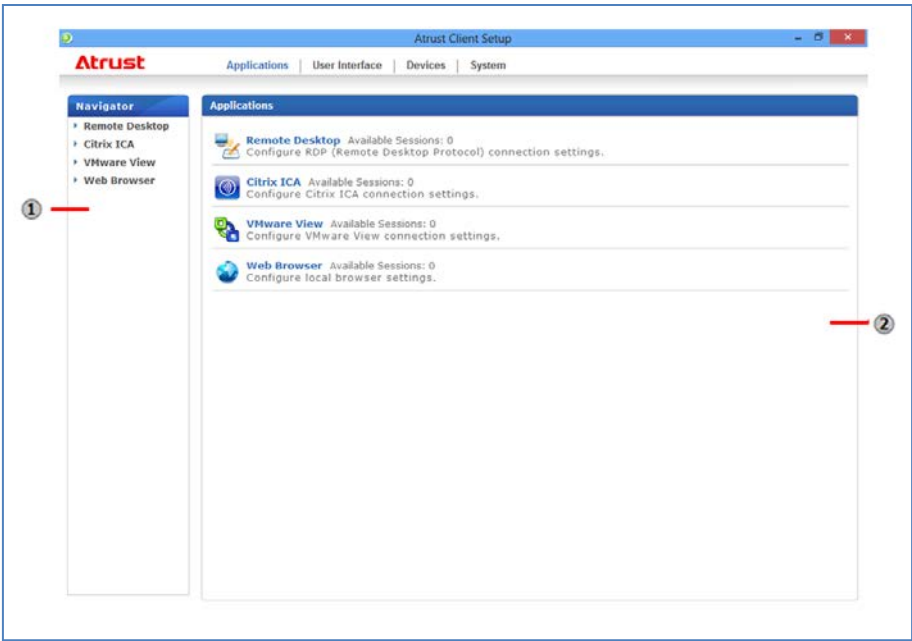
No.	Name	Description
1	Navigation area	Click to select a setting item under **Applications** tab or to select a setting entry under a selected setting item.
2	Configuration area	Configures setting values when a setting item or entry is selected.

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 View Connection Settings" • Chapter 4, "5.10 Accessing VMware View or Horizon View 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.
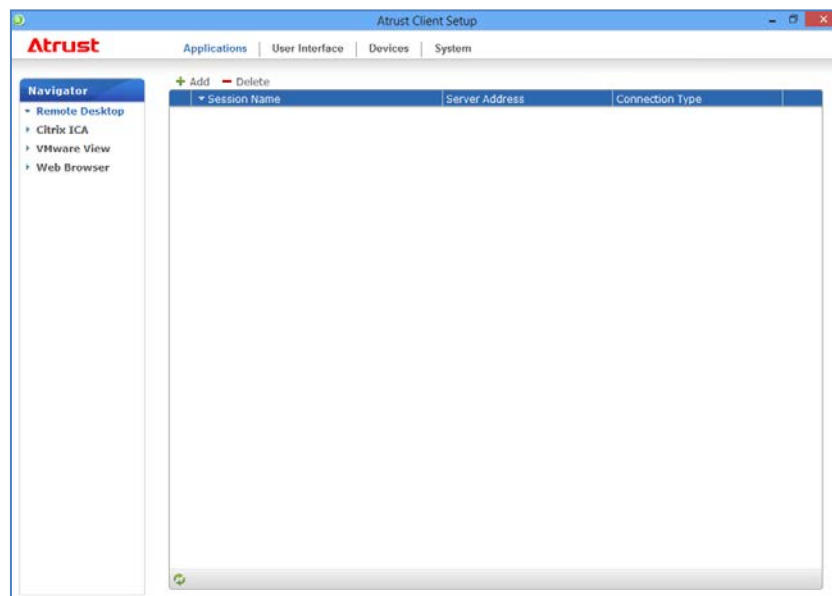
4. On **General** sub-tab, type in the session name and the server/virtual machine address under the **Server Settings** section.
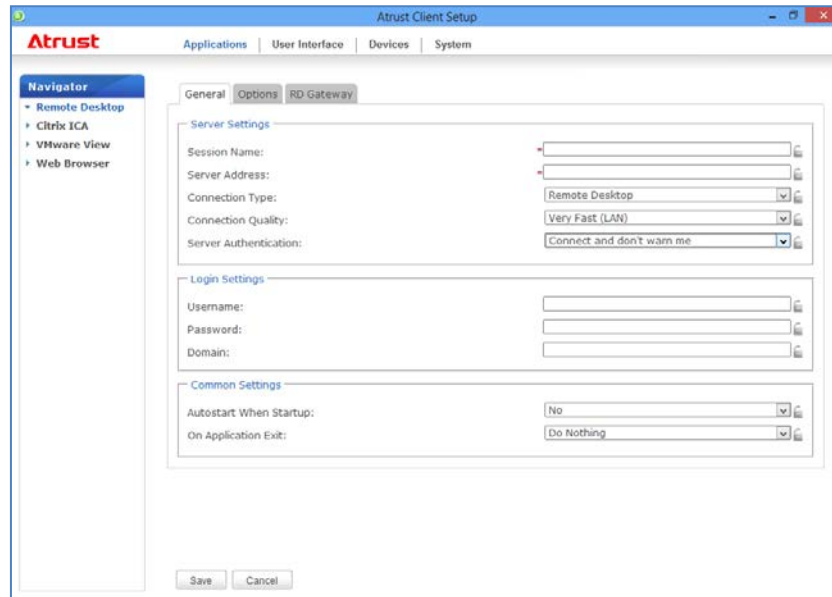
Note	• The red asterisks indicate the required fields.
	• The remote computer can be a physical server or a virtual machine. Visit Microsoft's websites at www.microsoft.com or support.microsoft.com for more information.

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 US310e supports only RD Web Access based on Windows Server 2012 R2; Windows Server 2008 R2 based is not supported.

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

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

Note	If you 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**.
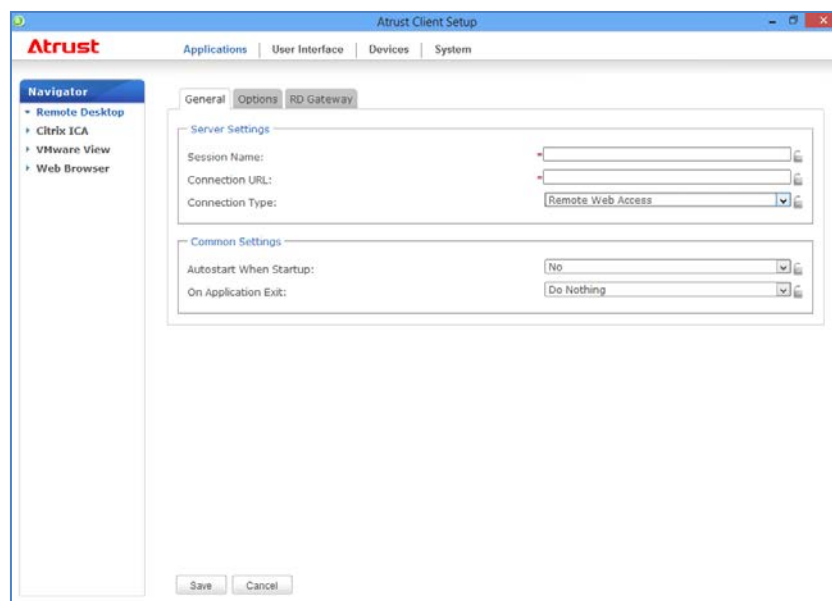
5. Type in the session name and connection URL through which Web-based remote applications/desktops is accessible.

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 US310e supports only RD Web Access based on Windows Server 2012 R2; Windows Server 2008 R2 based is not supported.

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

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

Note	If you 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.

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".

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

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 2012
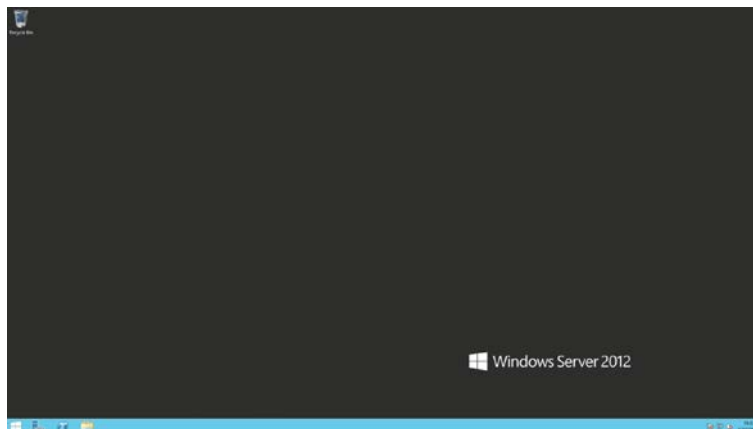
Example: Windows 8 Enterprise
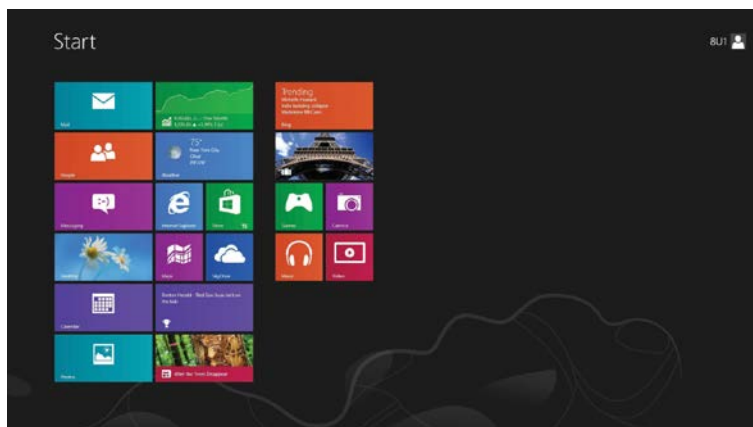
5.4.2 **Connection Type: Remote Web Access**

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.
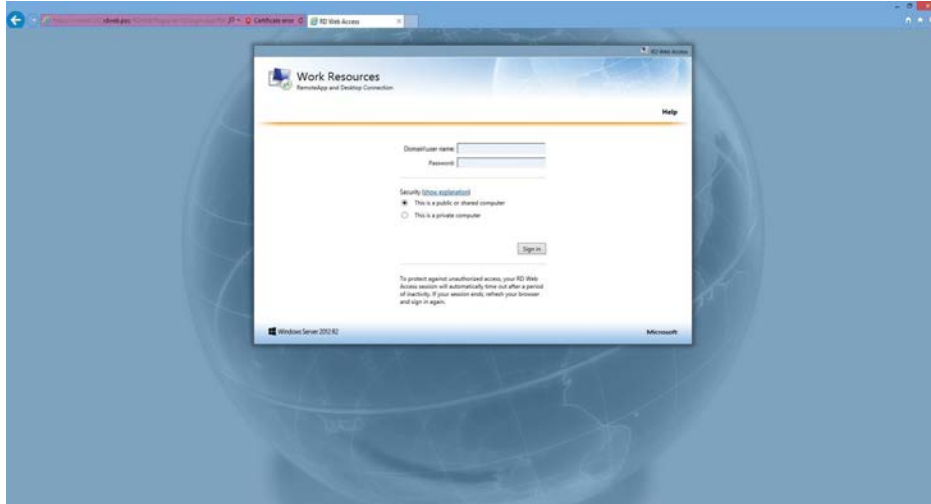
Note	• A warning message about security might appear. Consult your system administrator for details and ensure the connection is secure *first*. To bypass this message, click **Continue to this website**.
	• Click to select **Allow** to enable ActiveX Control when a popup message appears at the bottom 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**.
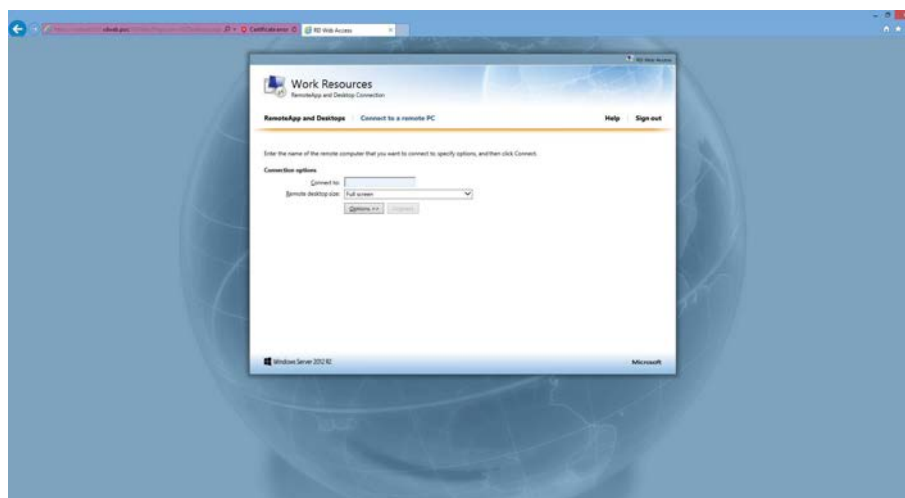
5.4.3   **Connection Type: Web Feed**

To access remote applications, do the following:

1. On Start screen, click the application tile to launch an application.
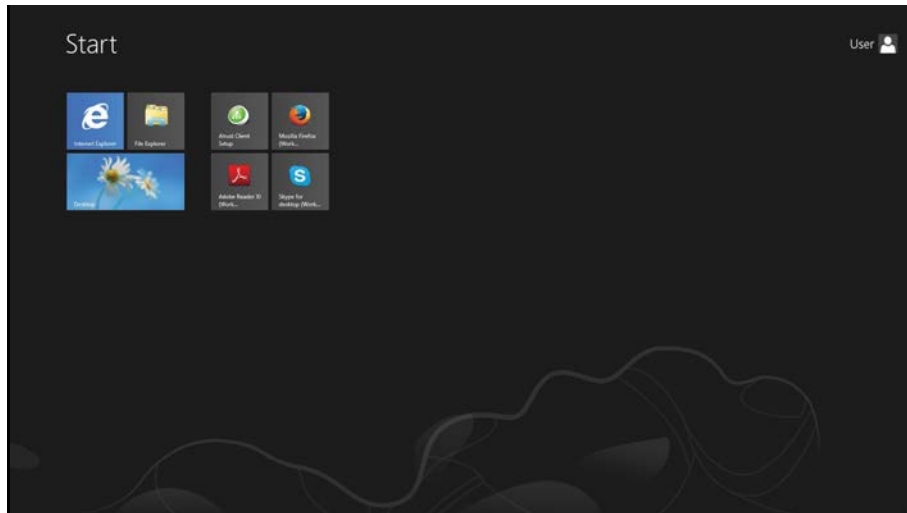
2. The applications are opened on the desktop.
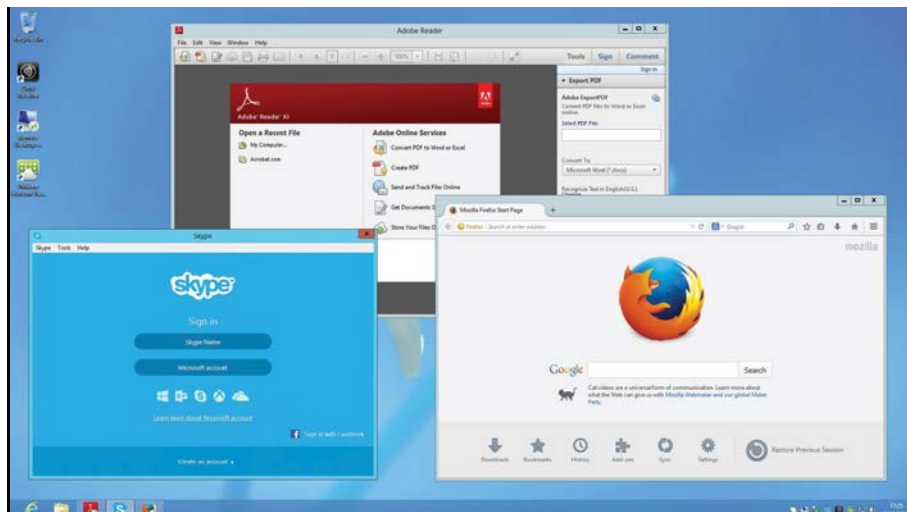
5.5 Configuring Advanced RDP Connection Settings

The table below provides a description of each setting item for RDP connections. See this table to configure advanced settings and customize your US310e 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

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

Common Settings	
Item	Description
Autostart When Startup	Select whether to open a Remote Desktop session automatically or not when Windows Embedded starts. If **Yes** is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.
On Application Exit	Select what to do when a Remote Desktop session is ended. Four options are available: **Do Nothing**, **Restart Application**, **Reboot**, and **Shutdown**. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Do Nothing**</td><td>Returns to the Windows Embedded desktop.</td></tr><tr><td>**Restart Application**</td><td>Opens a Remote Desktop session again.</td></tr><tr><td>**Reboot**</td><td>Restarts your thin client.</td></tr><tr><td>**Shutdown**</td><td>Turns off your thin client.</td></tr></table>

Options Sub-tab

Programs	
Item	Description
Start the following program on connection	Click the drop-down menu to enable/disable the Application mode. You can use this option to select the session type. Two remote session types are available: • Remote Desktop (when the Application mode is disabled) • Remote Application (when the Application mode is enabled) **NOTE:** Remote Application sessions are Remote sessions used to access only specific applications rather than full desktops. **NOTE:** Before you can open a Remote Application session, you need to add the desired application to the RemoteApp Programs list with RemoteApp Manager on the application hosted server. For detailed instructions on how to add a desired application to the RemoteApp Programs list on the server, visit Microsoft Support website at support.microsoft.com.
Start in the following folder	Type in the location of the desired application (on the host server) if **Start the following program on connection** is enabled. **NOTE:** You can type in the location/path of the desired application in this field, and specify only the name of the application in **Program path and file name** (the next field). Or, you can type in the full path and name of the application in **Program path and file name**, and leave this field empty.
Program path and file name	Type in the path and name of the desired application if **Start the following program on connection** is enabled. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Windows Media Player**</td><td>C:\Programs Files (x86)\Windows Media Player\wmplayer.exe</td></tr><tr><td>**Adobe Reader X**</td><td>C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32</td></tr></table> **NOTE:** The file extension can be omitted.

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 Embedded 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.

Local Resources Settings	
Item	**Description**
Remote Audio Playback	Click the drop-down menu to configure the computer sounds and audio playback setting in a Remote Desktop session. Three options are available: **Bring to this computer**, **Do not play**, and **Leave at remote computer**.

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

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

Option	Description
Recording from this computer	Allows audio recording in a Remote Desktop session using locally attached audio devices.
Do not record	Disables audio recording in a Remote Desktop session using locally attached audio devices.

	NOTE: When **Leave at remote computer** is selected on the drop-down menu of **Remote Audio Playback**, this setting item will be grayed out.
Apply Windows key combinations	Click the drop-down menu to select where to apply Windows key combinations. Three options are available: **On this computer**, **On the remote computer**, **Only when using the full screen**.
Drives	Click the drop-down menu to enable/disable locally attached drives in a Remote Desktop session.
Supported plug and play devices	Click the drop-down menu to enable/disable the supported plug and play devices in a Remote Desktop session.
RemoteFX USB redirection	Click to enable/disable locally attached RemoteFX USB devices. **NOTE:** To use RemoteFX USB devices in remote desktops, you need to configure the policy setting about device redirection to allow RemoteFX USB Device Redirection as well. To do so, follow the steps below: 1. Sign in to your US310e with an administrative account. 2. Disable UWF (Unified Write Filter) through Atrust Client Setup (See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)"). 3. On the *desktop* or *Start screen*, move your mouse to the bottom-right corner. The charms appear. 4. Click **Search** to select the Search charm. 5. Type **group policy** in the Search charm, and then click **Settings**. **Edit group policy** appears on the left. 6. Click to select **Edit group policy**. 7. 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**. 8. Select **Enabled** and to which users this setting applies: **Administrators Only** or **Administrators and Users**, and then click **OK**. 9. Enable UWF through Atrust Client Setup.

RD Gateway Sub-tab

Connection Settings	
Item	Description
RD Gateway Server Settings	Click the drop-down menu to choose if a RD Gateway server is used, automatically detected, or manually configured. Three options are available: **Automatically detect RD Gateway server settings**, **Use these RD Gateway server settings**, and **Do not use an RD Gateway server**.
Server Name	Type the IP address / URL / FQDN of the RD Gateway server. **NOTE:** Consult your network administrator for details.
Logon method	Click the drop-down menu to select the logon method. Three options are available: **Allow me to select later**, **Ask for password (NTLM)**, and **Smart card**. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Allow me to select later**</td><td>Users can select a logon method while connecting to the server.</td></tr><tr><td>**Ask for password (NTLM)**</td><td>Users will be prompted for a password while connecting to the server.</td></tr><tr><td>**Smart card**</td><td>Users will be prompted for a smart card while connecting to the server.</td></tr></table>
Bypass RD Gateway server for local addresses	Check to prevent traffic to and from local network addresses from being routed through the RD Gateway server and make a connection faster.
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

Server Settings	
Item	**Description**
Session Name	Type in the name for Remote Web Access sessions.
Connection URL	Type in the connection URL through which RD Web Access is available.
Connection Type	This table only provides descriptions for available settings when **Remote Web Access** is selected. Three connection types are available:

Option	Description
Remote Desktop	Provides access to remote desktops/applications.
Remote Web Access	Provides access to remote desktops/applications through a Web browser (Internet Explorer).
Web Feed	Provides access to remote applications through published Start screen tiles.

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

Option	Description
Do Nothing	Returns to the Windows Embedded desktop.
Restart Application	Opens a Remote Desktop session again.
Reboot	Restarts your thin client.
Shutdown	Turns off your thin client.

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".

Server Settings	
Item	**Description**
Session Name	Type in the name for Web Feed sessions.
Server Address	Type in the computer name or IP address of the server/virtual machine where to deliver a Web Feed session.
Connection Type	This table only provides descriptions for available settings when **Web Feed** is selected. Three connection types are available:

Option	Description
Remote Desktop	Provides access to remote desktops/applications.
Remote Web Access	Provides access to remote desktops/applications through a Web browser (Internet Explorer).
Web Feed	Provides access to remote applications through published Start screen tiles.

Login Settings	
Item	**Description**
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server. **NOTE:** Leave this field blank if the server doesn't belong to any domain.

RemoteApp and Desktop Connection	
Item	**Description**
Update Now	Click to fetch and update the published applications list from the server.

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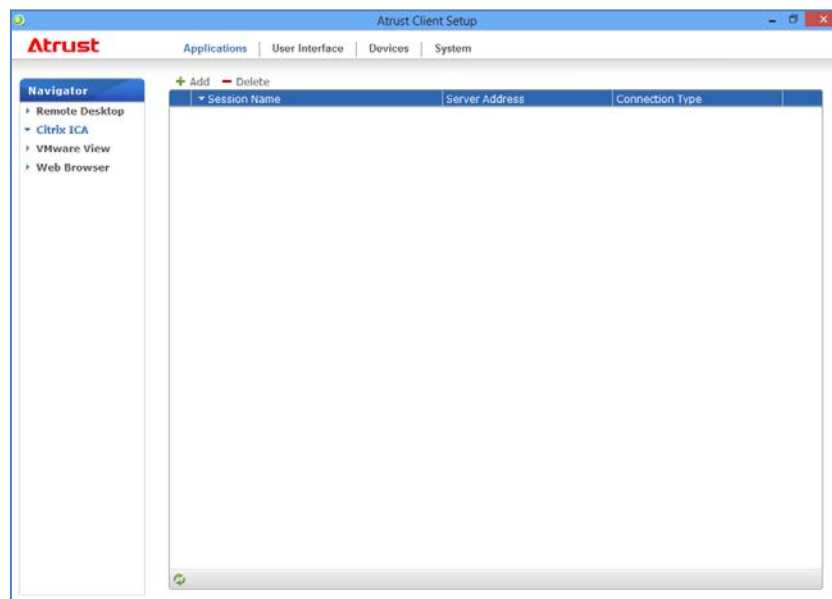
Note	If you have not created any entry, the ICA Connection list will be empty.

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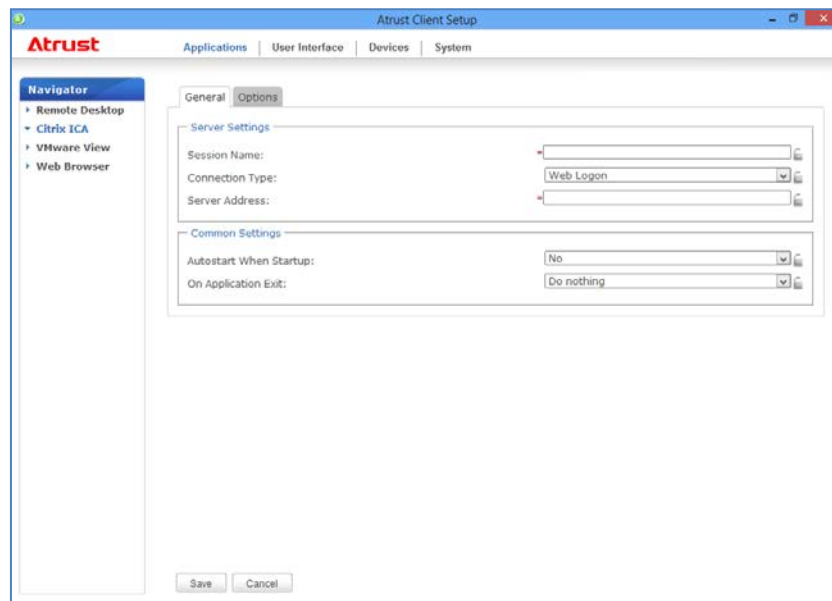
Note	The applicable or best suitable information type of the server side may vary with your Citrix environment. Consult your system administrator for more information.

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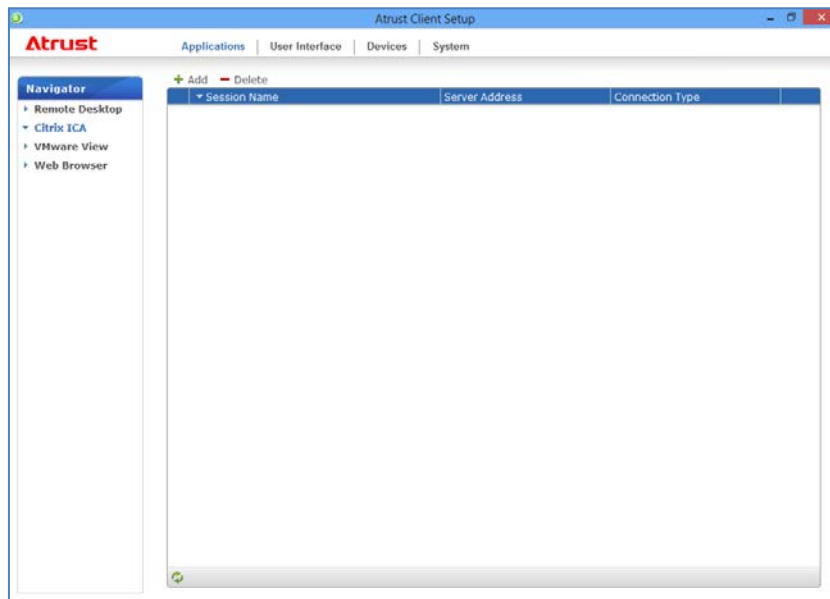
| **Note** | If you have not created any entry, the ICA Connection list will be empty. |

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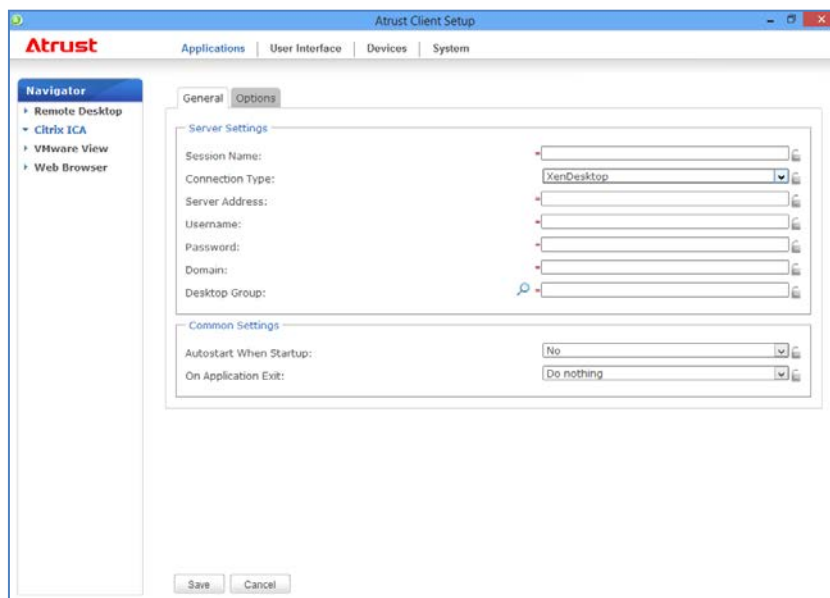
5. Type the session name, the IP address / FQDN of the server through which XenDesktop is accessible, user credentials, the domain of the server, and then click the Search icon (🔍) to discover available desktop groups.

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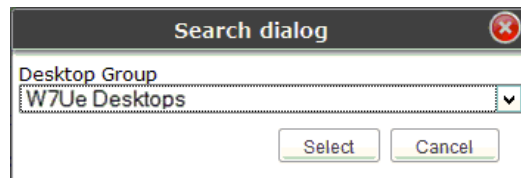
7. The selected desktop group name automatically appears in the Desktop Group field.

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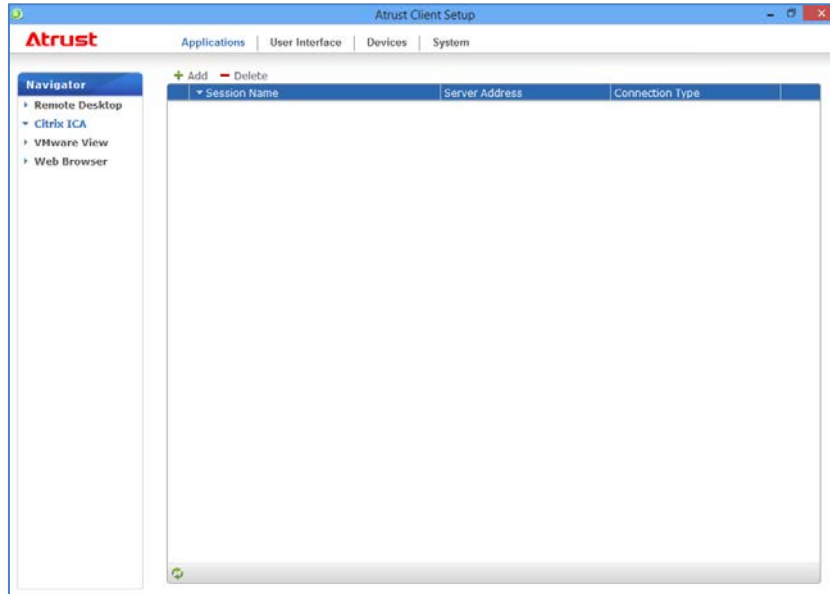
Note	If you have not created any entry, the ICA Connection list will be empty.

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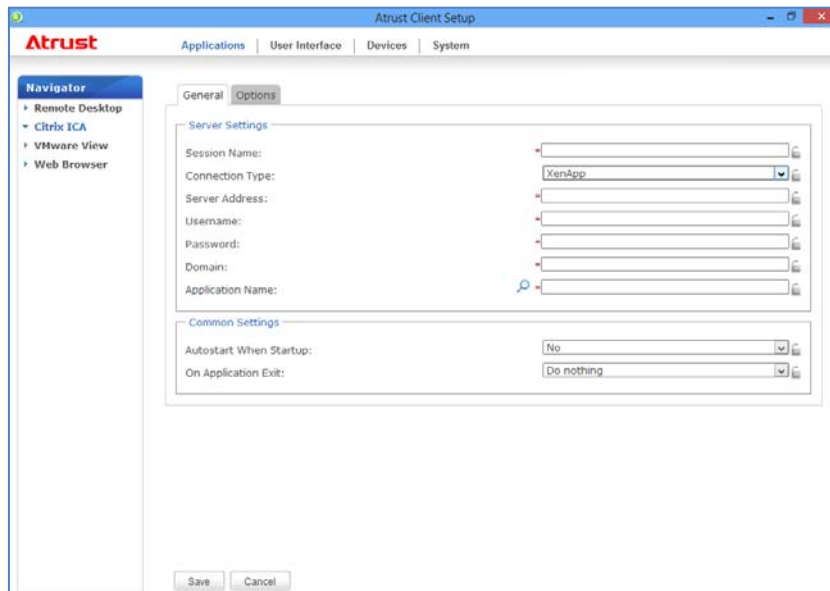
5. Type the session name, the IP address / FQDN of the server through which XenApp is accessible, user credentials, the domain of the server, and then click the Search icon (🔍) to discover available applications.

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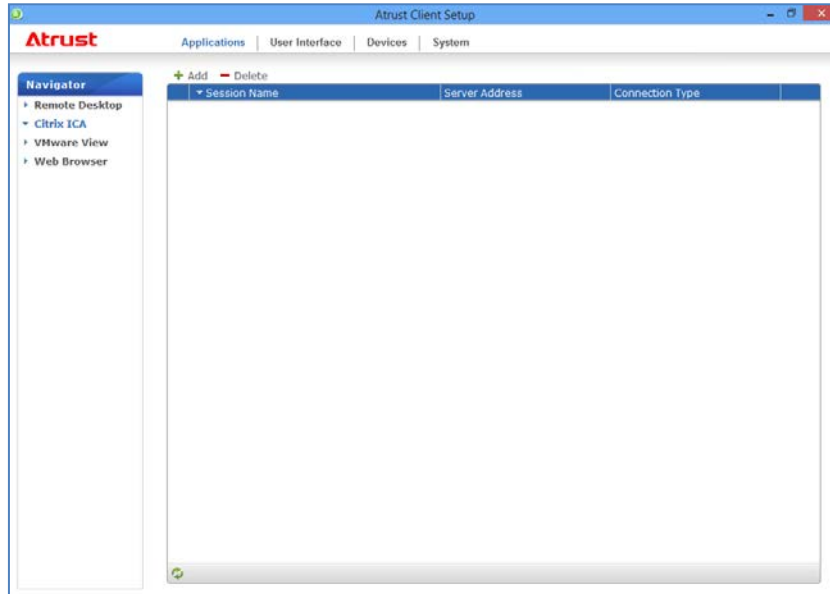
| Note | If you have not created any entry, the ICA Connection list will be empty. |

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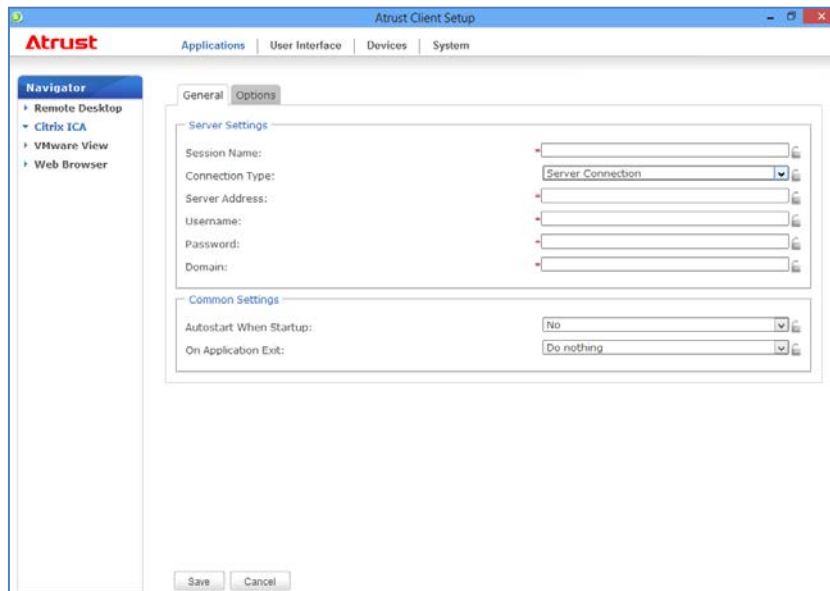
5. Type the session name, the IP address / FQDN of the server, user credentials, and the domain of the server.

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.
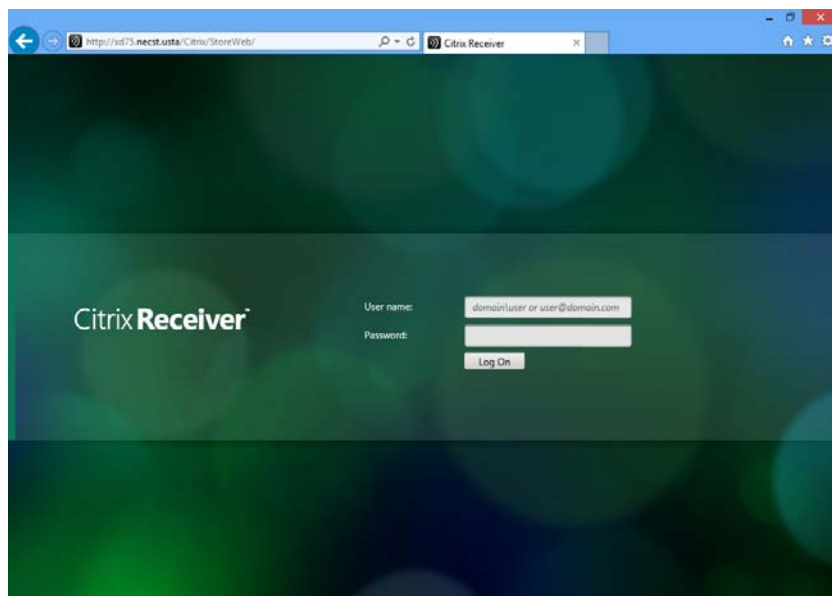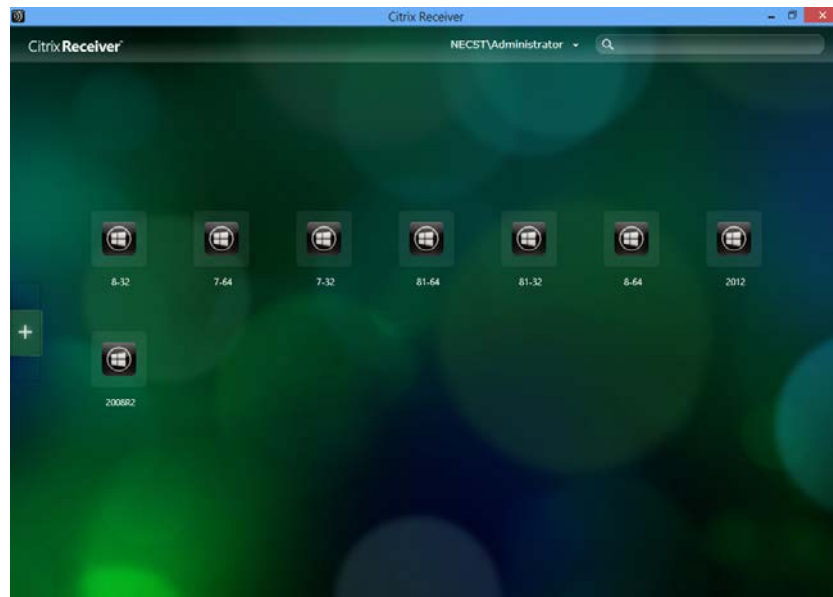

3. Type in the required credentials and domain name, and then click **Log On**.

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

Server Settings	
Item	Description
Session Name	Type in the name for Web Logon sessions.
Connection Type	This table only provides descriptions for available settings when **Web Logon** is selected. Four connection types are available: | Option	Description
Web Logon	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).
XenDesktop	Provides desktop delivery services.
XenApp	Provides application delivery services.
Server Connection	Provides full server access services for administrators (XenApp servers only). | NOTE: When **Web Logon** is selected, your US310e 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".
Server Address	Type in the computer name or IP address of the server or virtual machine to which to deliver the Web Logon session.
Common Settings	
Item	Description
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when US310e starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	Select what to do when a Citrix ICA session is ended. Four options are available: | 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

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

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

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 **XenDesktop** is selected. Four connection types are available:

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

Item	Description
Server Address	Type in the IP address / FQDN of the server through which XenDesktop is accessible.
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server.
Desktop Group	Type in the desktop group. **NOTE:** You can use the Search icon (🔍) in front of the field to discover available desktop groups. For detailed instructions, see Chapter 4, "5.6.2 Connection Type: XenDesktop".

Common Settings	
Item	Description
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when US310e starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	Select what to do when a Citrix ICA session is ended. Four options are available: **Do nothing**, **Restart Application**, **Reboot**, and **Shutdown**.

Option	Description
Do nothing	Returns to the Windows 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 US310e 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 during a low-speed connection.
Off	Disables audio playback in opened ICA sessions.

Item	Description
Encryption	Click the drop-down menu to select the desired encryption method. Five options are available: **Basic**, **RC5 128 bit (login only)**, **RC5 40 bit**, **RC5 56 bit**, **RC5 128 bit**.
Apply Windows key combinations (Ex. Alt + Tab keys)	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**.

5.8.3 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, "5.8.3 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

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 **XenApp** is selected. Four connection types are available: <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Web Logon**</td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr><tr><td>**XenDesktop**</td><td>Provides desktop delivery services.</td></tr><tr><td>**XenApp**</td><td>Provides application delivery services.</td></tr><tr><td>**Server Connection**</td><td>Provides full server access services for administrators (XenApp servers only).</td></tr></table>
Server Address	Type in the IP address and FQDN of the server through which XenApp is accessible.
Username	Type in the user/account name used for authentication.
Password	Type in the password of the user account used for authentication.
Domain	Type in the domain of the server. **NOTE:** Type in the full computer/server name if your XenApp server doesn't belong to any domain.
Application Name	Type in the application name. **NOTE:** 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".
Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a Citrix ICA session automatically or not when US310e starts. If **Yes** is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.
On Application Exit	Select what to do when a Citrix ICA session is ended. Four options are available: **Do nothing**, **Restart Application**, **Reboot**, and **Shutdown**. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Do nothing**</td><td>Returns to the Windows Embedded 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

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 through this connection.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE: Mapping Local Serial Ports** is not available because US310e 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 through this connection.

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 during a low-speed connection.
Off	Disables audio playback in opened ICA sessions.

Item	Description
Encryption	Click the drop-down menu to select the desired encryption method. Five options are available: **Basic**, **RC5 128 bit (login only)**, **RC5 40 bit**, **RC5 56 bit**, **RC5 128 bit**.
Apply Windows key combinations (Ex. Alt + Tab key)	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, "5.8.3 Settings for the Connection Type of XenApp".
	• For descriptions of settings for the connection type of XenApp, see Chapter 4, "5.8.4 Settings for the Connection Type of Server Connection".

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:

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

Item	Description
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.

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. Three options are available: **No preference**, **Better Speed (16-bit)**, and **Better Appearance (32-bit)**. { Option / Description table below }

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

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 through this connection.
Mapping Local Serial Ports	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If **Yes** is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. **NOTE: Mapping Local Serial Ports** is not available because US310e 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 through this connection.

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: { Option / Description table below }

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 during a low-speed connection.
Off	Disables audio playback in opened ICA sessions.

Item	Description
Encryption	Click the drop-down menu to select the desired encryption method. Five options are available: **Basic**, **RC5 128 bit (login only)**, **RC5 40 bit**, **RC5 56 bit**, **RC5 128 bit**.
Apply Windows key combinations (Ex. Alt + Tab keys)	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**.

5.9   Configuring Basic VMware View 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.
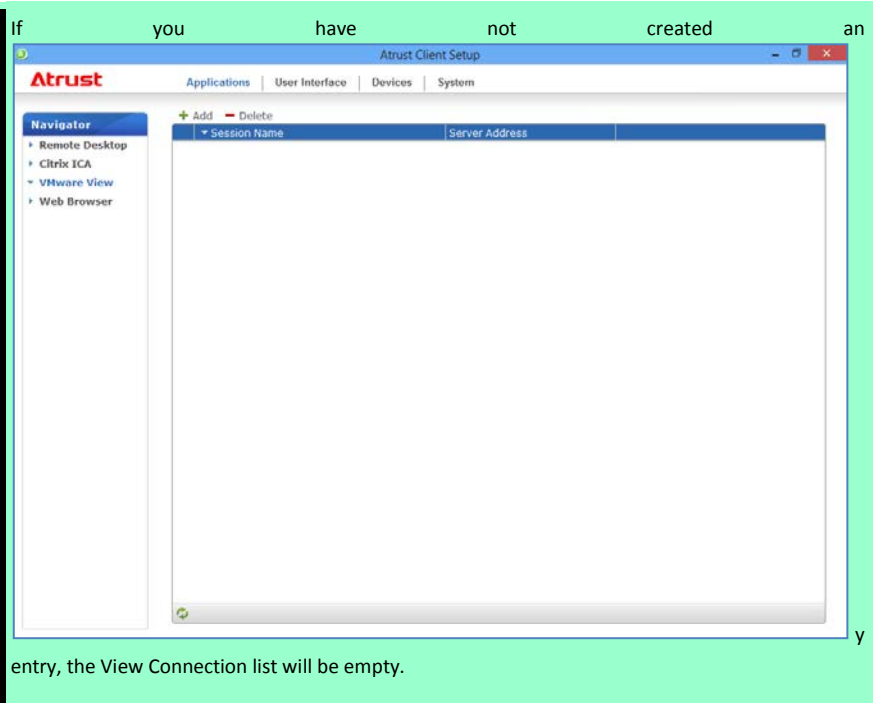
Note	• For more information on VMware desktop virtualization solutions, visit VMware website at www.vmware.com.
	• You can also access VMware View or Horizon View services through the standard desktop shortcut **VMware Horizon View Client**. For detailed instructions on how to access services via the standard desktop shortcut, see Chapter 3, "4. Accessing VMware View and Horizon View 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 an
	y
	entry, the View Connection list will be empty.

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

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

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

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

5.10   Accessing VMware View or Horizon View Services

To access VMware View or Horizon View 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 import a certificate.

> **Note**   For how to import a certificate, see Chapter 5, "16. Saving 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**.

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

Server Settings	
Item	Description
Session Name	Type in the name for VMware View or Horizon View sessions.
Connection Server	Type in the computer name or IP address of the View Connection Server. **NOTE:** For more information on View Connection Server, visit VMware website at www.vmware.com.
Port	Type in the port number used to communicate with the View Connection Server. To use the default value, simply leave it blank.
Use secure connection (SSL)	Check/Uncheck to enable/disable secure connection.
Certificate checking mode	Click to select whether to verify the identity of the remote server and whether to connect to an untrusted server. Three options are available: **Do not verify server identity certificates**, **Warn before connecting to untrusted servers**, and **Never connect to untrusted servers**. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Do not verify server identity certificates**</td><td>Do not verify the identity of the remote server and connect to it anyway.</td></tr><tr><td>**Warn before connecting to untrusted servers**</td><td>Warns and allows users to choose whether to connect or not.</td></tr><tr><td>**Never connect to untrusted servers**</td><td>Disallows untrusted connections.</td></tr></table>

Login Settings	
Item	Description
Log in as current user	Check to log in to VMware View or Horizon View services with the current user credentials. When checked, the User Name, Password, and Domain Name fields will be grayed out.
User Name	Type in the user name for authentication.
Password	Type in the password for authentication.
Domain Name	Type in the domain name of the View Connection Server.
Desktop Name	Type in the desktop name. Or, leave it blank for users to select one. **NOTE:** If **Manual** is selected for the Display Protocol field below, this field will be grayed out.
Display Protocol	Click the drop-down menu to select the display protocol. Three options are available: **Manual**, **Microsoft RDP**, and **PCoIP**. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Manual**</td><td>Manually select the desired display protocol.</td></tr><tr><td>**Microsoft RDP**</td><td>Use Microsoft RDP as the display protocol.</td></tr><tr><td>**PCoIP**</td><td>Use VMware PCoIP as the display protocol.</td></tr></table>

Common Settings	
Item	Description
Autostart When Startup	Select whether to open a VMware View or Horizon View session automatically or not when US310e starts. If **Yes** is selected, when you log in to the system, the VMware View or Horizon View session will be opened automatically.
On Application Exit	Select what to do when a VMware View or Horizon View session is ended. <table><tr><th>Option</th><th>Description</th></tr><tr><td>**Do Nothing**</td><td>Returns to the Windows Embedded desktop.</td></tr><tr><td>**Restart Application**</td><td>Opens a VMware View or Horizon View session again.</td></tr><tr><td>**Reboot**</td><td>Restarts your thin client.</td></tr><tr><td>**Shutdown**</td><td>Turns off your thin client.</td></tr></table>

Options Sub-tab

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

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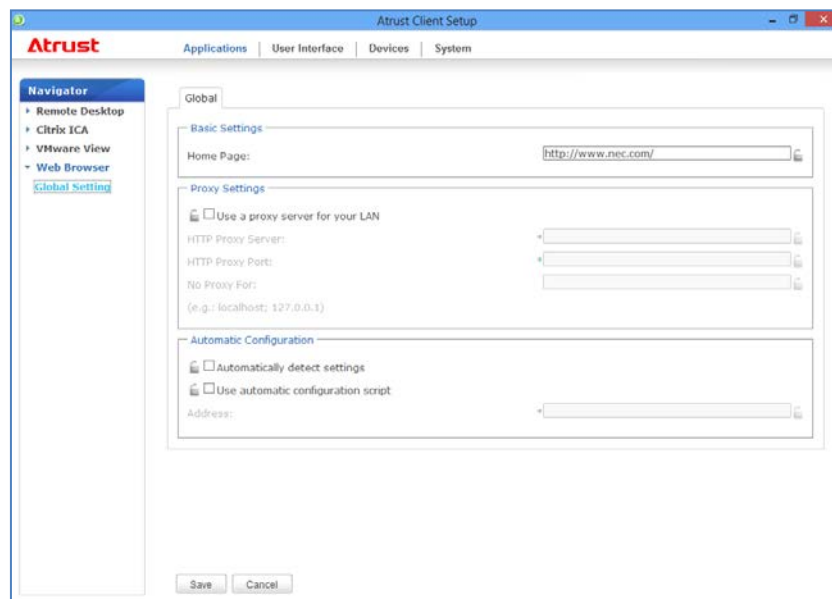
2. See the table below to set up home page, proxy, and automatic configuration settings, and then click **Save** to apply.

Basic Settings	
Item	Description
Home Page	Type in the URL of a Web page for quick access via the Home button.
Proxy Settings	
Item	Description
Use a proxy server for your LAN	Check to use a proxy server in your local area network.
HTTP Proxy Server	Type in the IP address of the proxy server.
HTTP Proxy Port	Type in the communication port of the proxy server.
No Proxy For	Type in the IP address(es) to bypass the proxy server.
Automatic Configuration	
Item	Description
Automatically detect settings	Check to automatically detect browser settings.
Use automatic configuration script	Check to allow automatic configuration and indicate the IP address where a configuration file is located.
Address	Type in the IP address when **Use automatic configuration script** is selected.

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.
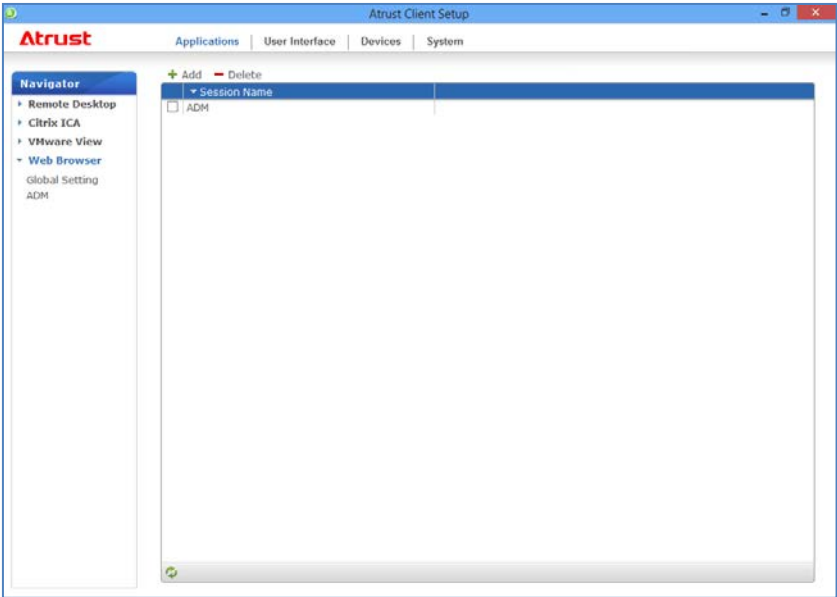
Note	If you have not created any entry, the Browser Session list will be empty.

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).

Common Settings	
Item	**Description**
Autostart When Startup	Select whether to open a browser session automatically or not when Windows Embedded starts.
On Application Exit	Select what to do when a browser session is ended. Four options are available: | Option	Description
Do Nothing	Returns to the Windows Embedded desktop.
Restart Application	Opens a Remote Desktop session again.
Reboot	Restarts your thin client.
Shutdown	Turns off your thin client.	

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

NEC Express5800 Series
US310e

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. Mapping Network Drives
Describes how to map the network drives.

7. Participating in Domains
Describes how to participate in domain.

8. Using the Net and Tracert Utilities
Describes how to use network utilities.

9. Managing Users and Groups with User Accounts
Describes how to create, modify, and configure the user account.

10. Changing the Computer Name of a Thin Client
Describes how to change computer name of US310e.

11. Setting Date and Time
Describes how to set date and time of US310e.

12. Configuring Dual Monitor Display
Describes how to configure dual monitor display, and how to use the span mode.

13. Installing CMO Terminal Agent
Describes how to install CMO Terminal Agent.

14. Configuring Wireless Local Area Network (LAN) Settings
Describes how to configure wireless LAN settings.

15. Saving Wireless Connections
Describes how to retain wireless connection under the UWF environment.

16. Saving 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 Writer 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 US310e 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 Embedded Standard 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 software, 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. *1

  *1 US310e does not support standby operations.

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	The Remote Desktop Services Client Access License (RDS CAL) is always preserved regardless of whether the Unified Writer Filter is enabled or disabled.

3.1   Changing Passwords with the Unified Writer Filter Enabled

On Microsoft Windows based computers, machine account passwords are regularly changed by using the domain controller for security purposes. The same password process is applicable for a thin client if the thin client is a member of such a domain. With the Unified Writer Filter enabled, a thin client will successfully make this password change with the domain controller. However, because the Unified Writer Filter is enabled, the new password will not be retained the next time the thin client is booted. In such cases, you can use the following options:

- Disable the machine account password change on the thin client by setting the `DisablePasswordChange` registry entry to a value of 1.

- Disable the machine account password change on the Windows based server by using the Microsoft documentation for the operating system. For example, on Windows Server 2008, set the `RefusePasswordChange` registry entry to a value of 1 on all domain controllers in the domain (instead of on all workstations). The thin clients will still attempt to change their passwords every 30 days, but the change will be rejected by the server.

3.1.1   Disabling the machine account password change on the thin client

1. To start Registry Editor, click **Start**, **Run**, type "regedit" in the **Open** box, and then click **OK**.
2. Locate and click the following registry subkey:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
3. In the right pane, right-click the `DisablePasswordChange` entry.
4. On the **Edit** menu, click **Modify**.
5. In the **Value data** text box, enter a value of 1, and then click **OK**.
6. Quit the Registry Editor.

3.1.2   Disabling the machine account password change in domain controller

1. To start Registry Editor, click **Start**, **Run**, type "regedit" in the **Open** box, and then click **OK**.
2. Locate and click the following registry subkey:

    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Enter `RefusePasswordChange` as the registry entry name, and then click **Enter**.
5. On the **Edit** menu, click **Modify**.
6. In the **Value data** text box, enter a value of 1, and then click **OK**.
7. Quit the Registry Editor.

3.2 Running Unified Writer Filter Command Line Options

US310e 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)".

Important	**Administrators should use file security to prevent unauthorized use of these commands.**

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.

Enable-HORM

Enables Hibernate Once/Resume Many (HORM) mode immediately.

Disable-HORM

Disables Hibernate Once/Resume Many (HORM) mode immediately.

Reset-Settings

Restores the original settings captured at installation.

Important	**Because US310e is an UEFI device, Hibernate Once/Resume Many (HORM) mode is unavailable. Do not use the Enable-HORM command.**

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.

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.

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.

Get-Files {<drive> | <volume>}

Displays a list of files in the volume cached by the UWF overlay. Either drive letter or the volume name can be used to specify the volume.

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	US310e does not support Windows Update in UWF Servicing Mode. Do not use UWF Servicing Mode. To upgrade the firmware of US310e, 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 US310e, 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.

Programs and Features
Power Options
Event Viewer
System
Device Manager
Disk Management
Computer Management
Command Prompt
Command Prompt (Admin)

Task Manager
Control Panel
File Explorer
Search
Run

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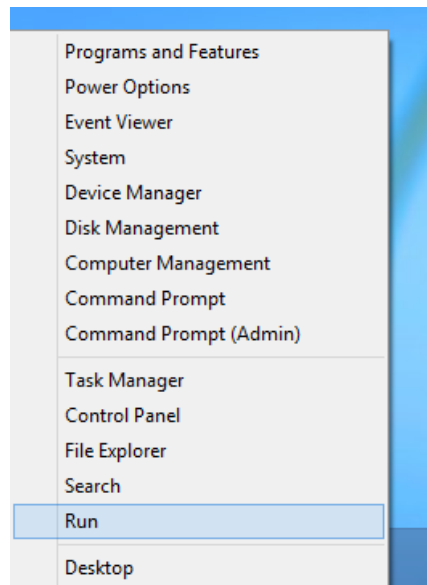
3. Type **netplwiz** in the **Open** dialog box, and then click **OK**.

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.

OK   Cancel   Browse...
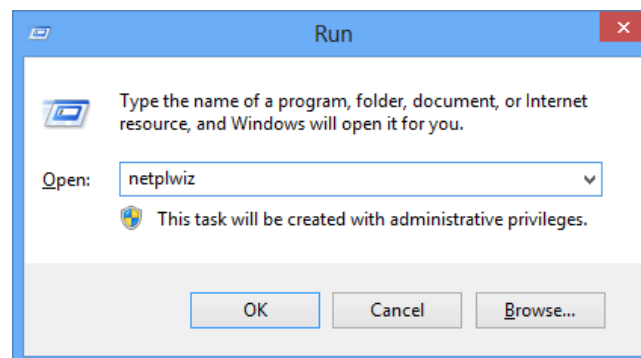
4. Click the **Users** tab in the **User Accounts** dialog box, and select the **Users must enter a user name and password to use this computer** check box.
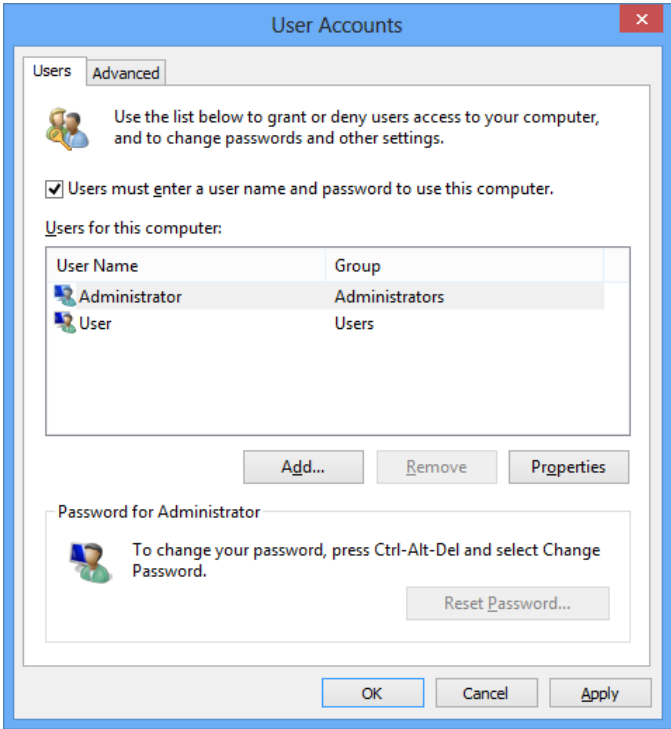
5. Select the name of the user for which you want to configure auto sign-in from the list of users.

    * As an example, select the User account.
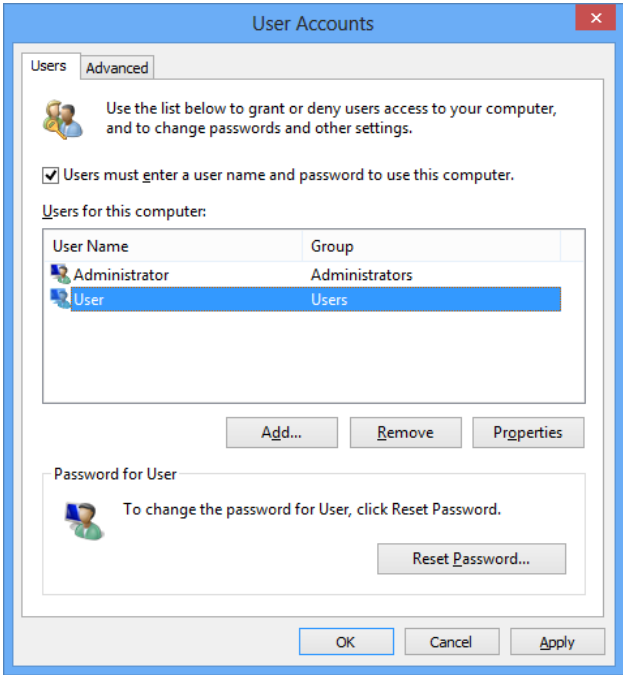
6. Clear the **Users must enter a user name and password to use this computer** checkbox, and click **OK**.
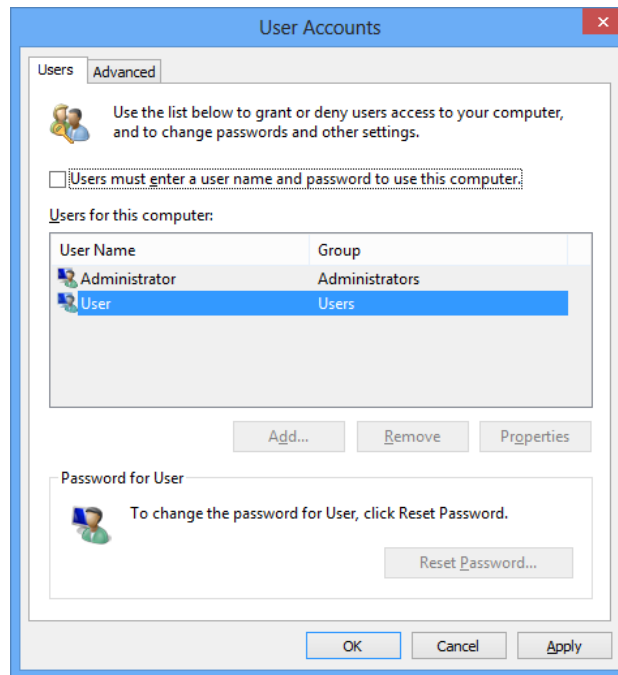
7. The **Automatically sign in** dialog appears. Type the password to be used at sign-in in the **Password** and **Confirm Password** boxes, and then click **OK**.
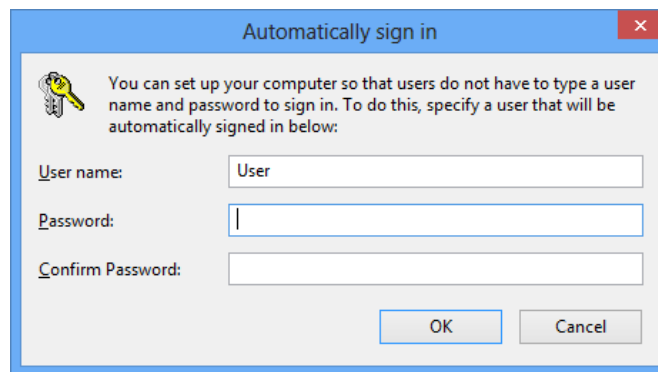
8. Restart the computer to make sure that you can sign in to the system as the configured user.

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. Mapping Network Drives

Administrators can map network drives. However, to retain the mappings after the thin client is restarted, you must complete the following:

- Select the **Reconnect at logon** check box.

- To retain the setting changes after US310e is restarted, you need to disable the Unified Writer Filter. For details, see *Chapter 4,* "2.9 Configuring UWF (Unified Write Filter)".

Tip	A remote home directory can also be assigned by using a user manager utility or by other means known to an administrator.

7. Participating in Domains

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

Participating in Domains
As an administrator, you can use the **Computer Name** tab on the **System Properties** dialog box (**Start** > **Control Panel** > **System** > **Change Settings**) to join a thin client to a domain.

Important	**Exercise caution when joining the thin client to a domain as the profile downloaded at log-on could overflow the UWF overlay or flash memory.**

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.

To make the domain changes permanent, complete the following:

1. Disable the Unified Writer Filter.

2. Join the domain.

3. Reboot the thin client.

4. Sing in with the domain account.

5. Enable the Unified Writer Filter.

6. Reboot the thin client.

8. 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.

9. Managing Users and Groups with User Accounts

Use the **User Accounts** window (**Start** > **Control Panel** > **User 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

Tip	For detailed information about using the **User Accounts** window, click the help icon and examples links provided throughout the wizards. For example, you can use the Windows **Help and Support** window (click the help icon in the **User Accounts** window) to search for items such as user profiles and user groups and obtain links to detailed steps on creating and managing these items.

9.1   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 US310e 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 **User Accounts** window (**Start** > **Control Panel** > **User Accounts**).

2. Click the **Manage Another Account** link to open the **Manage Accounts** window.

3. Click the **Create a New Account** link to open and use the wizard.

4. After creating the Standard Users and Administrators you want, the users will appear in the **Manage Accounts** window (**Start** > **Control Panel** > **User Accounts** > **Manage Another Account**).

9.2   Editing User Accounts

To edit the default settings of a Standard User or Administrator account, click on the account you want to modify in the **Manage Accounts** window (**Start** > **Control Panel** > **User Accounts** > **Manage Another Account**), and then make your changes.

9.3   Configuring User Profiles

To configure the Default, Administrator, and User profiles stored on the thin client, open the **User Profiles** window (**Start** > **Control Panel** > **User Accounts** > **Configure Advanced User Profile Properties**) and use the command buttons (**Change Type**, **Delete**, **Copy to**) according to Microsoft documentation provided throughout the wizards.

10. 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.

The Remote Desktop Service Client Access License (RDSCAL) is preserved regardless of the UWF status (enabled or disabled). This maintains the license information used to identify the computer and facilitates image management on the thin client.

11. 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. Use the **Date and Time** dialog box (**Start** > **Control Panel** > **Date and Time** or by clicking the time area on the taskbar and then clicking the **Change date and time settings** link) to edit the time and date as needed.

12. Configuring Dual Monitor Display

Use the **Screen Resolution** window (**Control Panel** > **Display** icon > **Change Display Settings** link) to configure the dual monitor settings as described in the Microsoft documentation 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.

12.1   Creating a Remote Desktop Connection Shortcut for Span Mode

To allow a standard user to connect to a remote desktop in span mode (mstsc.exe /span), a shortcut for connecting to span mode must be created on the desktop of the standard user. Follow the steps below to create the shortcut.

Important	To maintain the Remote Desktop Connection shortcut for span mode, disable the UWF (Unified Writer Filter) before creating the shortcut. Enable the UWF once the shortcut has been created.

1. Sign in to US310e as an Administrator.

2. Right-click the **Remote Desktop Connection** shortcut on the desktop, and select **Copy**.
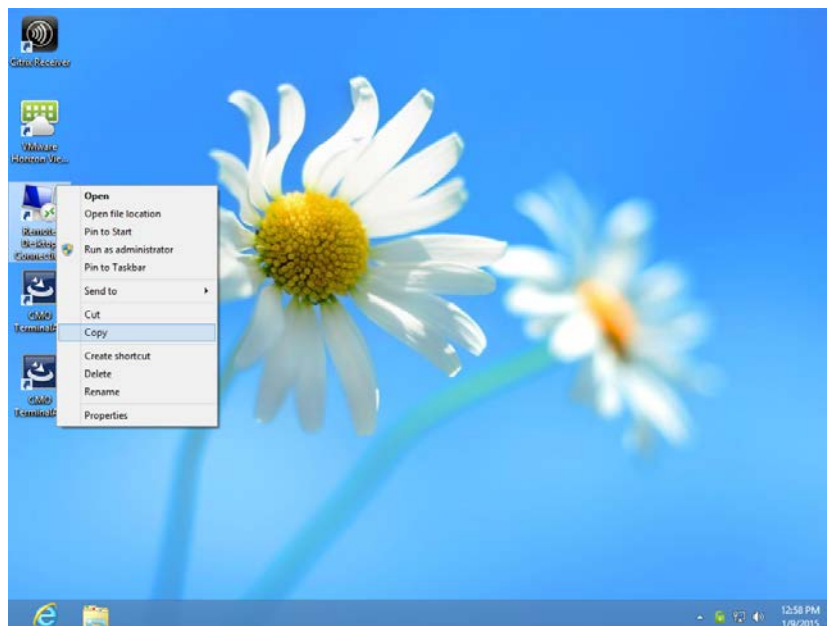
3. Use Explorer to access the following folder, and select **Paste shortcut** on right-click menu.

C:\Users\User\Desktop
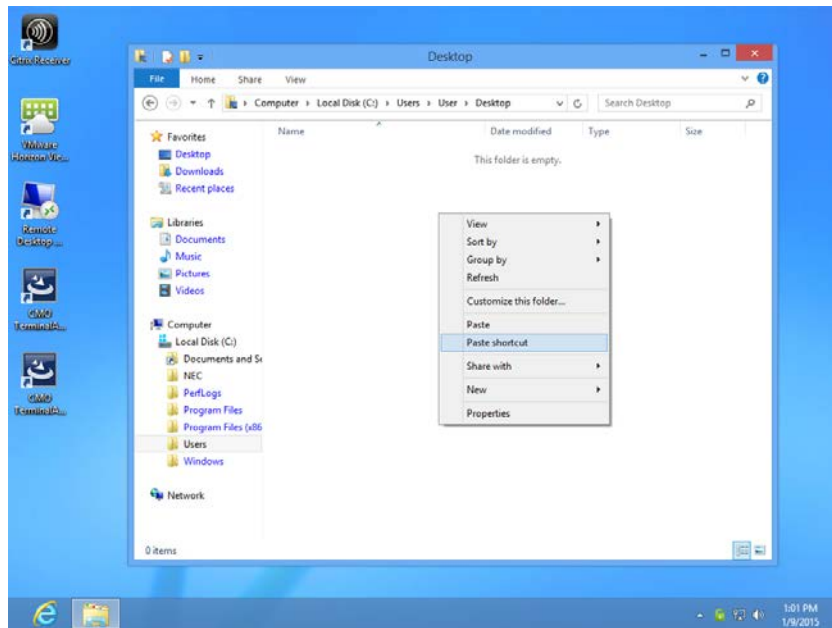
4. Open the **Properties** dialog box for the shortcut you pasted in step 3.
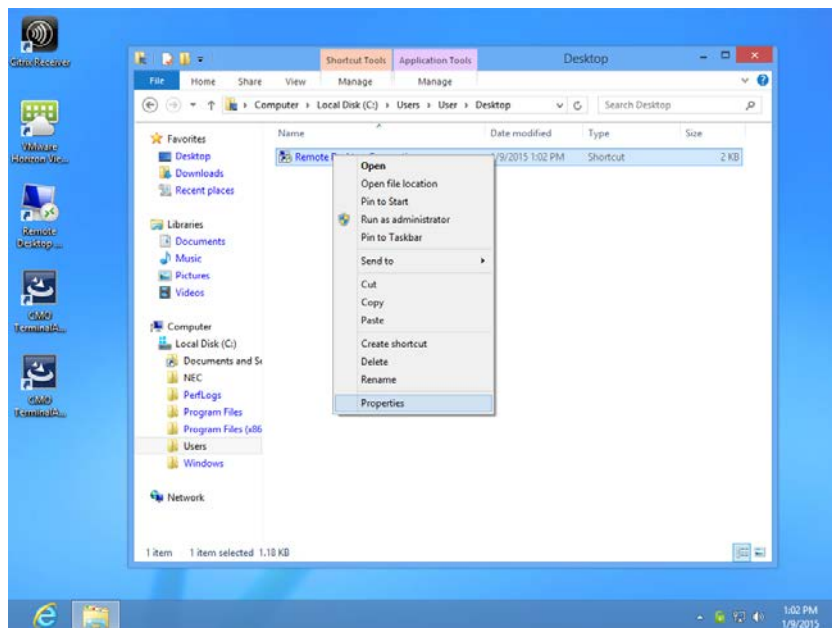
5. On the **Shortcut** tab, add "/span" to the end of the character string in the **Target** box.

   Before: %windir% \System32\mstsc.exe

   After: %windir% \System32\mstsc.exe /span
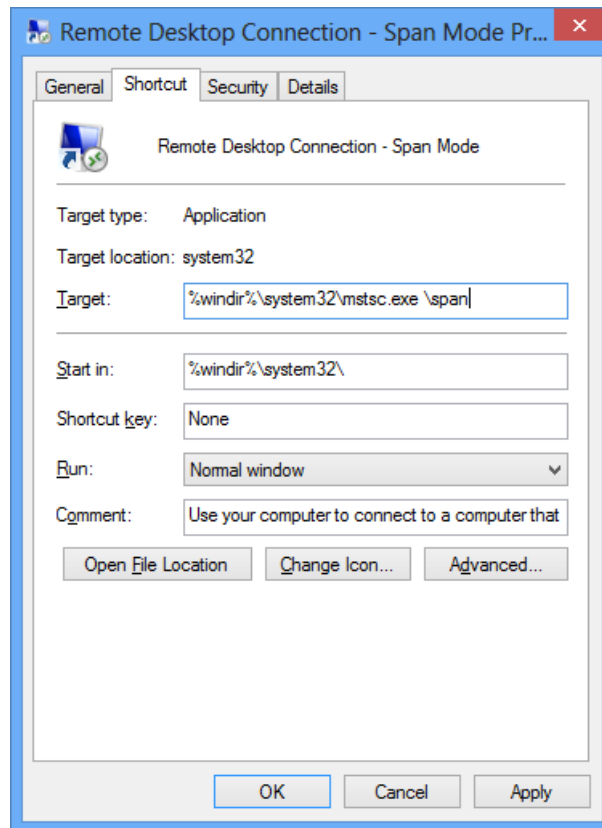
6. On the **General** tab, change the name of the shortcut, and click **OK**.

   The shortcut name "Remote Desktop Connection – Span Mode" is used as an example below.
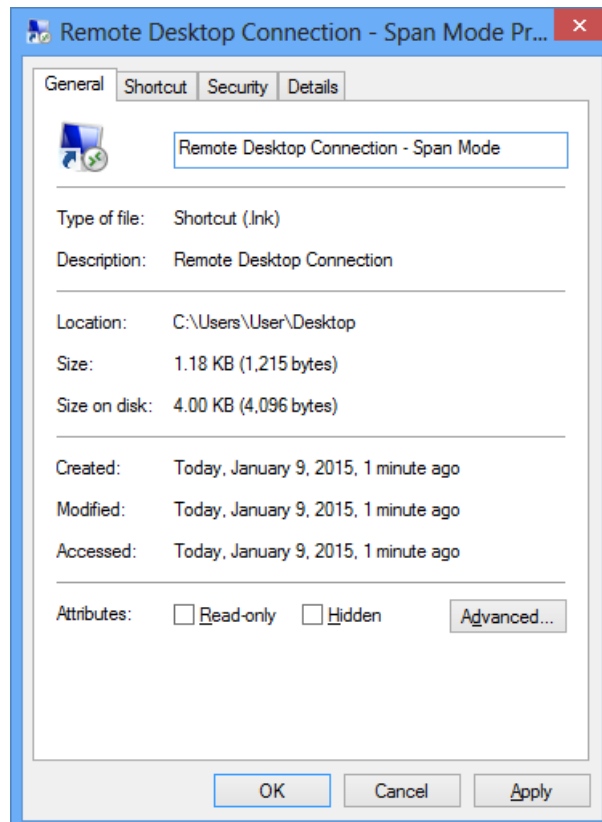
7. Sign in to US310e as a standard user, and launch the Remote Desktop Connection - Span Mode shortcut created on the desktop.
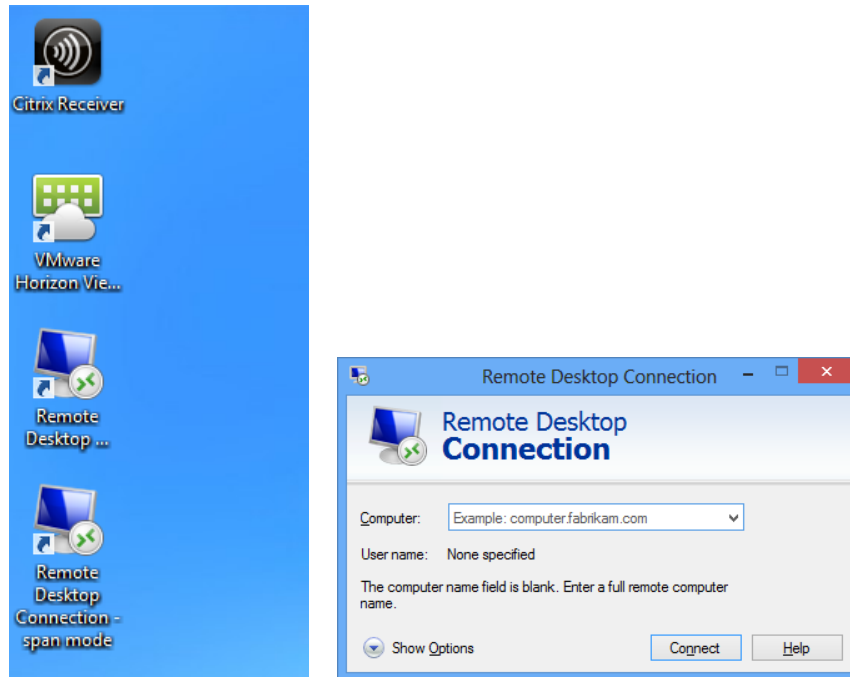
Note	If you select **RDP Options** -> **Display** tab -> **Display configuration** and select the **Use All My Monitors for the Remote Session** check box, you will be connected to the virtual PC in multiple monitors mode (that is, the primary and secondary monitors will be connected to the virtual PC independently).

8. Log on to the virtual PC and check that US310e is connected to the virtual PC in span mode.

   If you maximize the window for applications such as Notepad in Remote Desktop Connection - Span Mode, it will be displayed across multiple monitors.

13. Installing CMO Terminal Agent

To access NEC Client Management Option (CMO) services from US310e, use CMO Terminal Agent. CMO Terminal Agent is not installed on US310e by default; however, US310e includes the following installers:

- CMO Terminal Agent Version 4.3

- CMO Terminal Agent Version 5.0

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 5.0 to Version 4.3, first uninstall Version 5.0, and then install Version 4.3.**

The table below shows the compatibility between the CMO Terminal Agent and server component versions (CMO Configuration Console, CMO Manager, CMO Manager Extension Pack, CMO Connector, and CMO Command).

Server component version	CMO Terminal Agent version			
	4.1	4.2	4.3	5.0
4.1	○	×	×	×
4.2	○	○	×	×
4.3	○	○	○	×
5.0	○	○	○	○

Install CMO Terminal Agent as follows:

1. Sign in to US310e 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**.
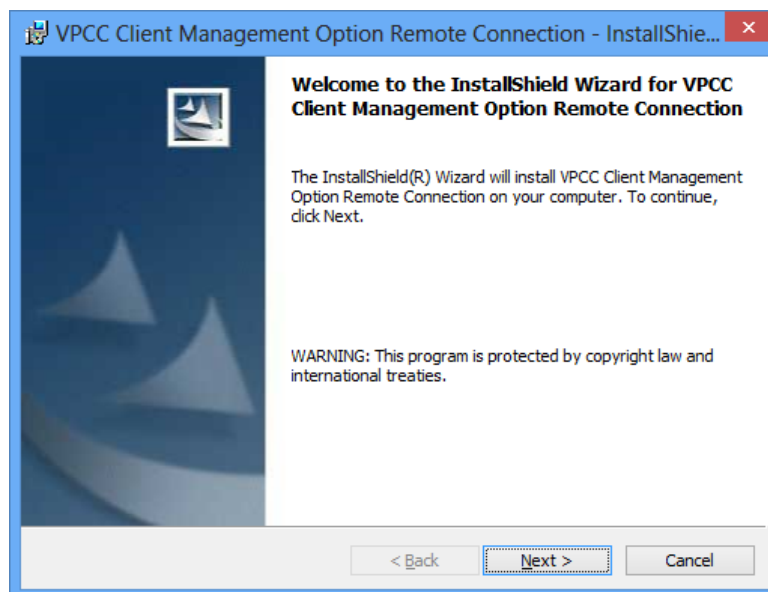
4. Select the method for obtaining Client Management Option Manager that is appropriate for your environment, and then click **Next**.
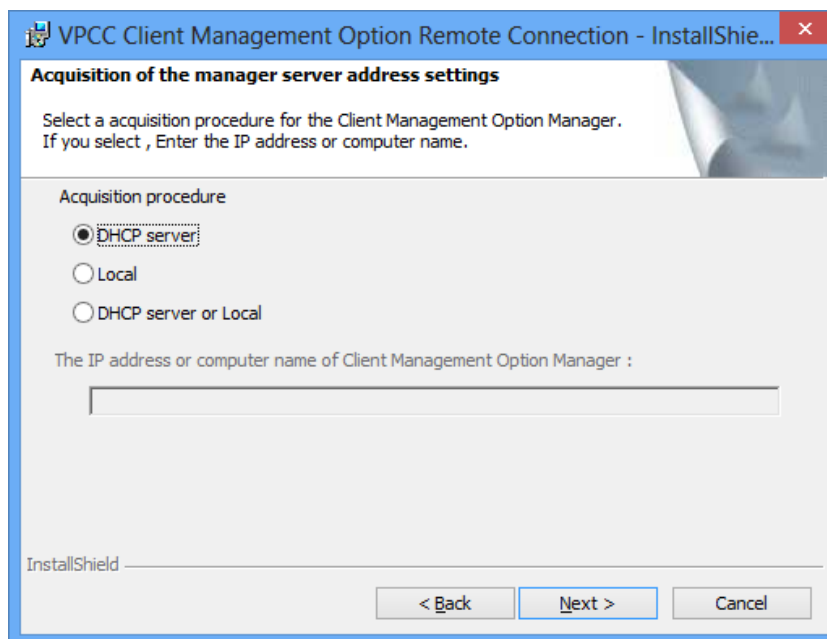
5. Type in the domain information, and then click **Next**.

   * If you selected **DHCP Server** in step 4, this step is skipped.
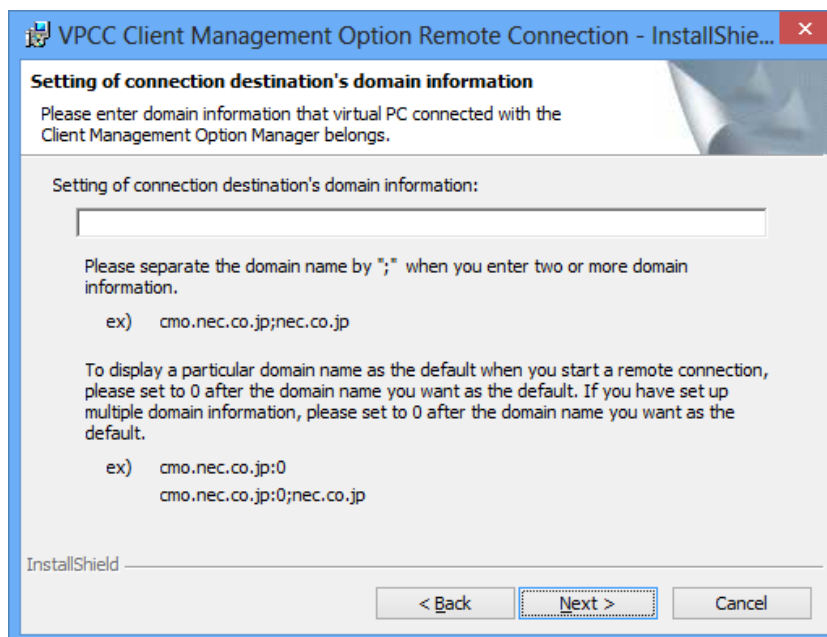
6. Specify the installation folder, and then click **Next**.
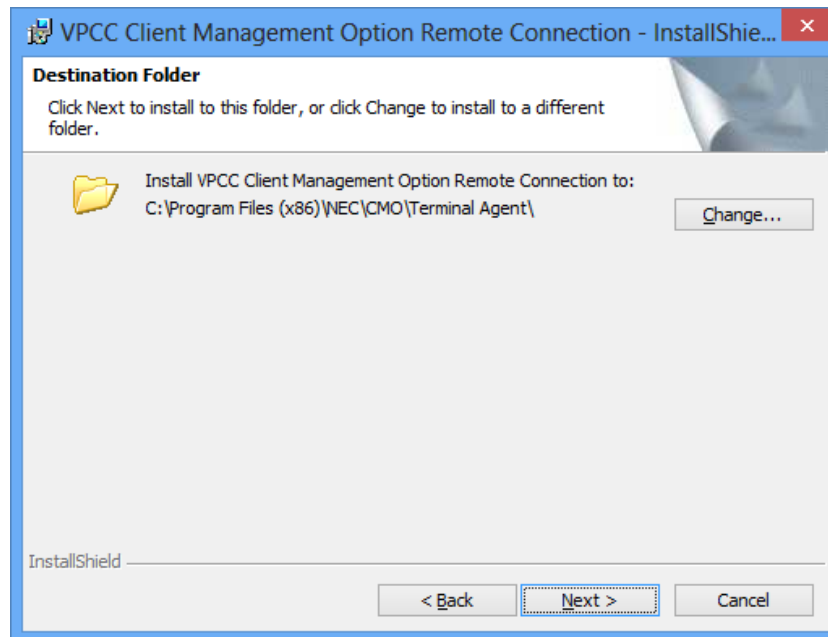
7. Click **Install**.
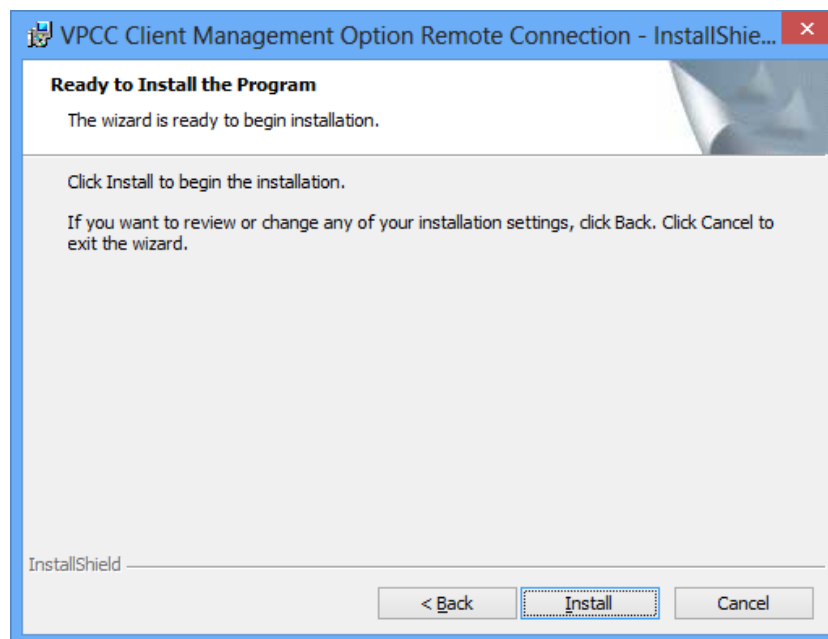
8. Click **Finish**.
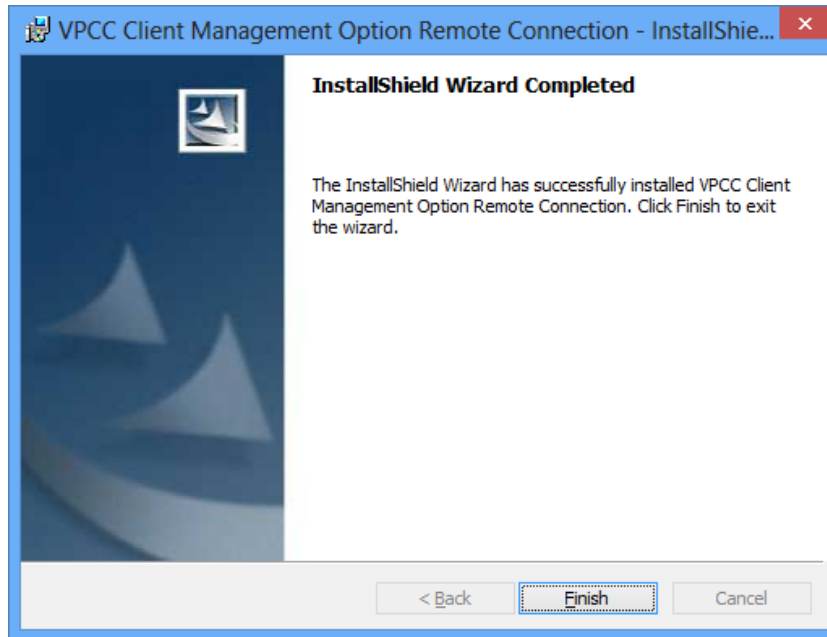
9. On the desktop, move the mouse pointer to the bottom-left corner, and then right-click **Start** to open the popup menu.

10. Click **Add or Remove Programs**.

11. 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.
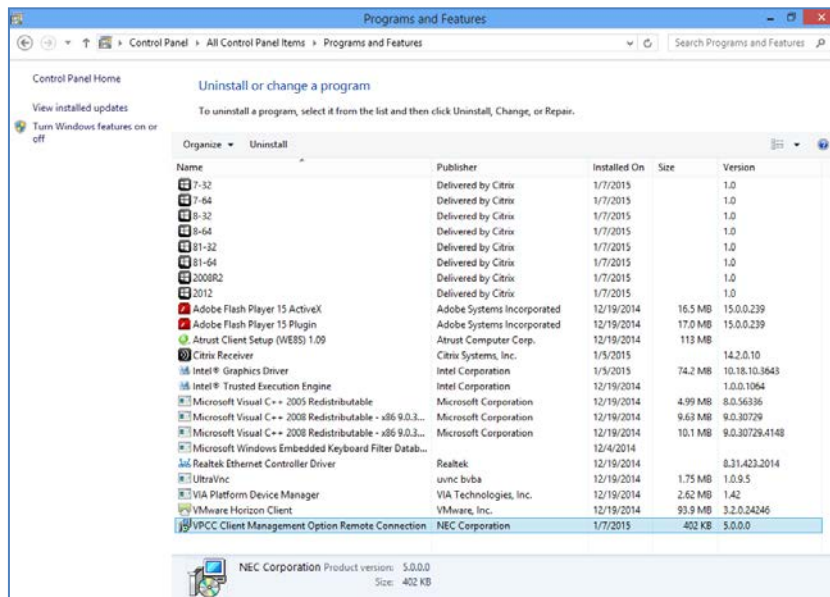
12. Sign out from the Administrator account.

13. Sign in as a User.

14. Wait until the CMO Terminal Agent shortcut appears on the **Start** screen.
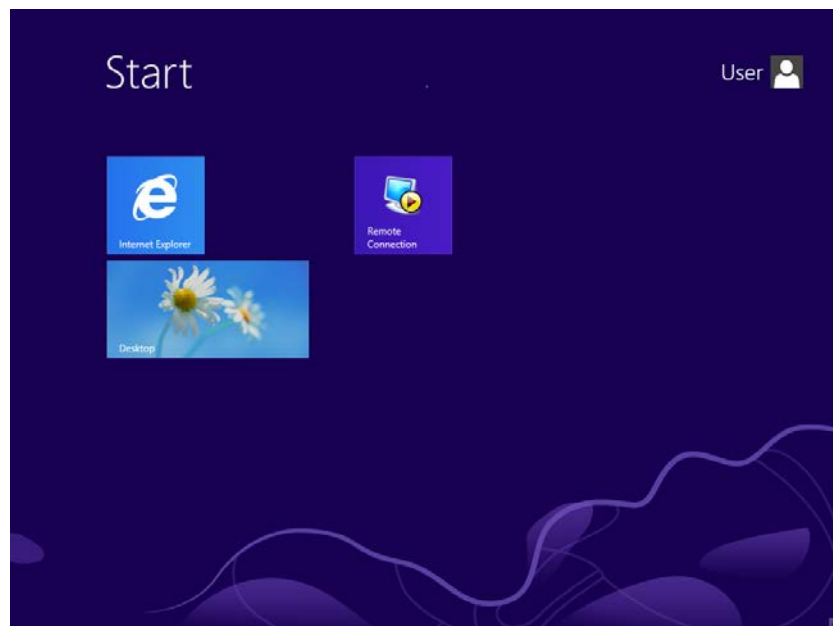
Note	CMO Terminal Agent is registered in the Startup menu when it is installed, and is automatically launched when you sign in to US310e.

14. Configuring Wireless Local Area Network (LAN) Settings

In US310e wireless LAN model, clicking the **Network and Sharing Center** icon in the Control Panel allows you to:

Manage wireless networks (click the Manage Wireless Networks link):

- **Add**

  Click **Add** to open and use the wizard to add a wireless network. To edit an existing wireless network, right-click it, and then select **Properties** to open the **Network Properties** dialog box.

- **Adapter Properties**

  Click **Adapter Properties** to open and use the properties dialog box for the wireless adapter.

- **Profile Types**

  Click **Profile Types** to open and use a dialog box to enable or disable the ability to create Per User Profiles.

- **Network and Sharing Center**

  Click **Network Sharing and Center** to return to the **Network and Sharing Center** dialog box that provides network settings and gives access to network settings.

Change Adapter Settings (click the Change Adapter Settings link):

- Click **Organize** to open the list of options you can use to organize your network connections.

- Select a connection to display the list of command buttons you can use to view the status, connect to, enable, disable, diagnose, rename, and change the settings of the connection.

Change Advanced Sharing Settings (click the Change Advanced Sharing Settings link):

Select the network profile settings you want for each of your networks.
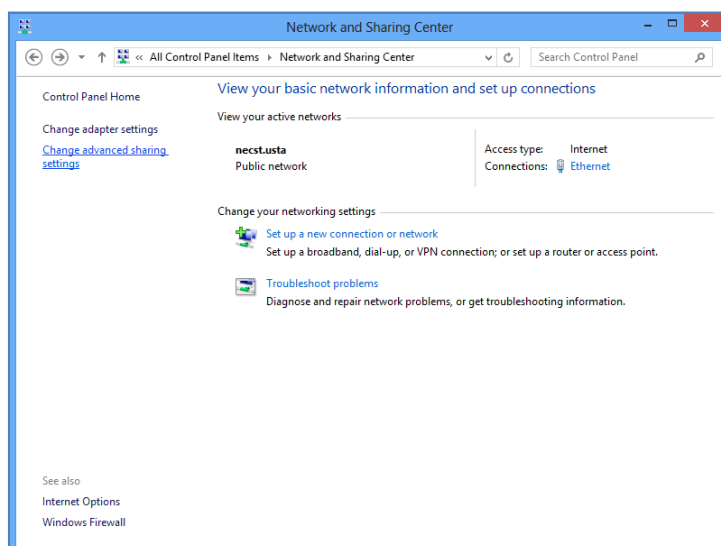
For information about preserving your wireless connections so that they persist across restarts, see Chapter 5, "15. Saving Wireless Connections".

15. Saving Wireless Connections

When using Windows Embedded 8 Standard (WE8S), UWF (Unified Write Filter) must be disabled to retain the wireless access configuration in UWF Enable mode. (See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".)

When you configure wireless access after the UWF is disabled, the authentication credentials are retained even after a reboot, eliminating the need to re-authenticate each time the client systems are restarted. The utility saves the service set identifier (SSID) for wireless connections across workgroup modes and domains. When thin clients restart, they are automatically connected to the desired wireless access point.

Windows Embedded Standard clients can connect to wireless networks by using the following network authentication modes:

- Open mode that uses WEP

- Shared mode that uses WEP

- WPA Personal (WPA-PSK) authentication that uses AES and TKIP

- WPA2 Personal (WPA2-PSK) authentication that uses AES and TKIP

- WPA Enterprise (WPA-Enterprise) authentication that uses AES and TKIP

- WPA2 Enterprise (WPA2-Enterprise) authentication that uses AES and TKIP

- IEEE802.1X Encryption WEP

You can use PEAP with any of the authentication methods below for wireless authentication.

- EAP-PEAP (EAP-MS-CHAP v2, TLS)

- EAP-TLS

- EAP-TTLS

- Non-Microsoft EAP authentication methods

Note	PEAP is not supported for use with EAP-MD5.

15.1   Using PEAP Fast Reconnect

When clients connect to an 802.11 wireless network, the authenticated session has an expiration interval configured by the network administrator to limit the duration of authenticated sessions. To avoid the requirement for authenticated clients to periodically re-authenticate and resume a session, you can enable the fast reconnect option.

PEAP supports fast reconnect, as long as each wireless access point is configured as a client of the same IAS (RADIUS) server. Fast reconnect must be enabled on both the wireless client and the RADIUS server.

When PEAP fast reconnect is enabled, after the initial PEAP authentication succeeds, the client and the server cache TLS session keys. When users associate with a new wireless access point, the client and the server use the cached keys to re-authenticate each other until the cache has expired. Because the keys are cached, the RADIUS server can quickly determine that the client connection is a reconnect. This reduces the delay in time between an authentication request by a client and the response by the RADIUS server. It also reduces resource requirements for the client and the server.

If the RADIUS server that cached the session keys is not used, full authentication is required, and the user is again prompted for credentials or a PIN. This can occur in the following situations:

- The user associates with a new wireless access point that is configured as a client of a different RADIUS server.

- The user associates with the same wireless access point, but the wireless access point forwards the authentication request to a different RADIUS server.

In both situations, after the initial authentication with the new RADIUS server succeeds, the client caches the new TLS session keys. Clients can cache TLS session keys for multiple RADIUS servers.

16. Saving the Certificate

In Windows Embedded Standard 8 (WE8S), the Unified Writer Filter (UWF) protects the clients from undesired flash memory writes. The protected and cached flash memory contents are retained while the thin client is active, but they are lost when the thin client is restarted or shut down. In the same manner, certificates installed while UWF is enabled are lost when the thin client is restarted or shut down.

If you want to use the certificates even after the thin client is restarted or shutdown, disable UWF, and do the following:

1. Log on to US310e as an administrator.

2. On the desktop, move the mouse pointer to the bottom-left corner, and then right-click on the appeared **Start** to open the popup menu.

3. Click to select **Run** on that popup menu.

4. Click **Run**, type "mmc" in the **Open** box, and then click **OK**.
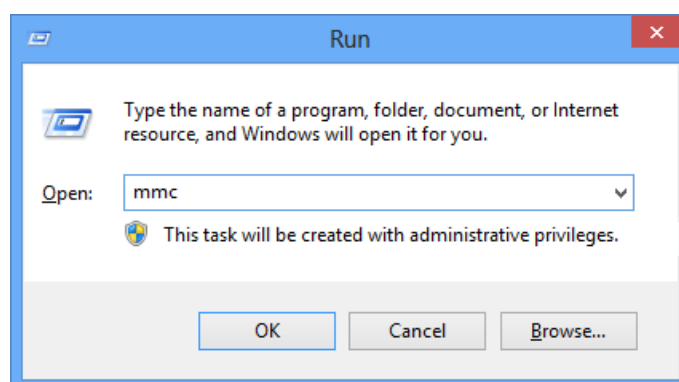
5. On the Console window, click the **File** menu to select **Add/Remove Snap-in**.
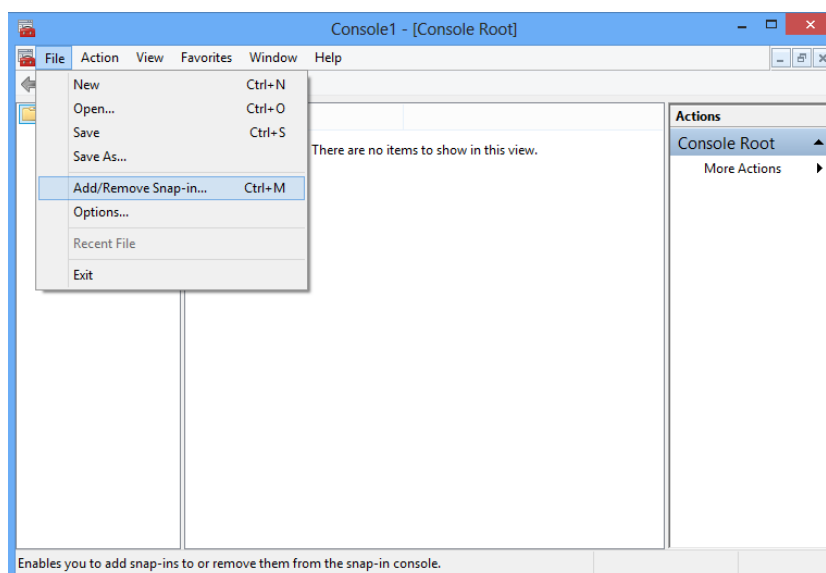
6. On the **Add or Remove Snap-ins** window, click **Certificates** > **Add** > **Computer account** > **Local computer** > **Finish** > **OK** to add the Certificates snap-in.
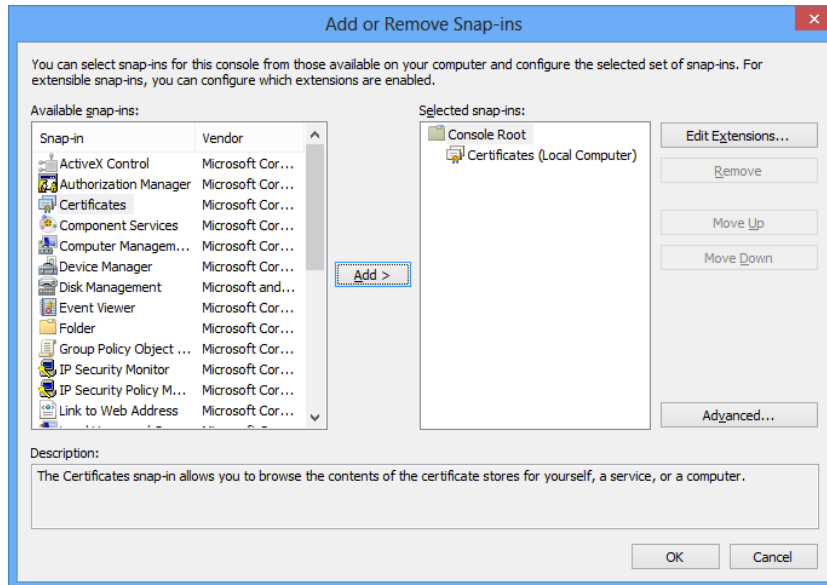
7. On the Console window, click to expand the group tree of Certificates, right-click on **Trusted Root Certification Authorities**, and then select **All Tasks** > **Import** on the popup menu.
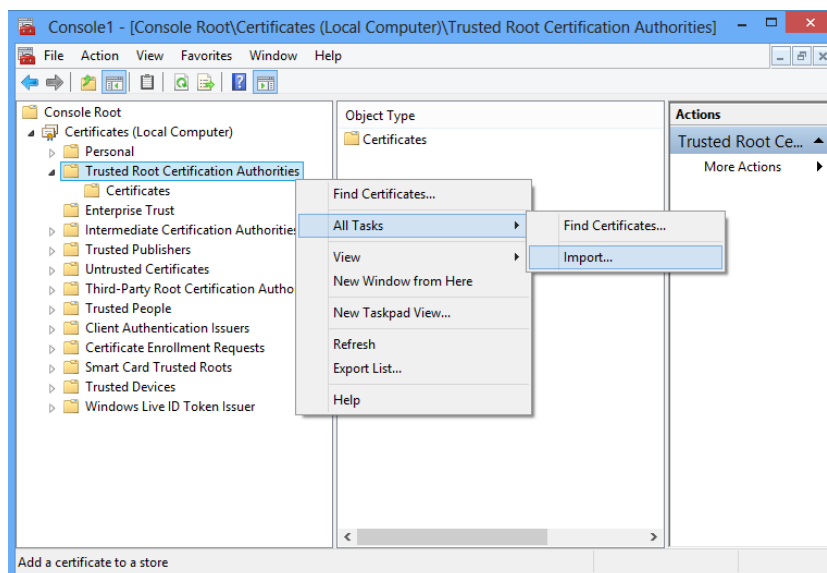
8. Follow the **Certificate Import Wizard** to import your certificate, and then close the Console window when this is complete.
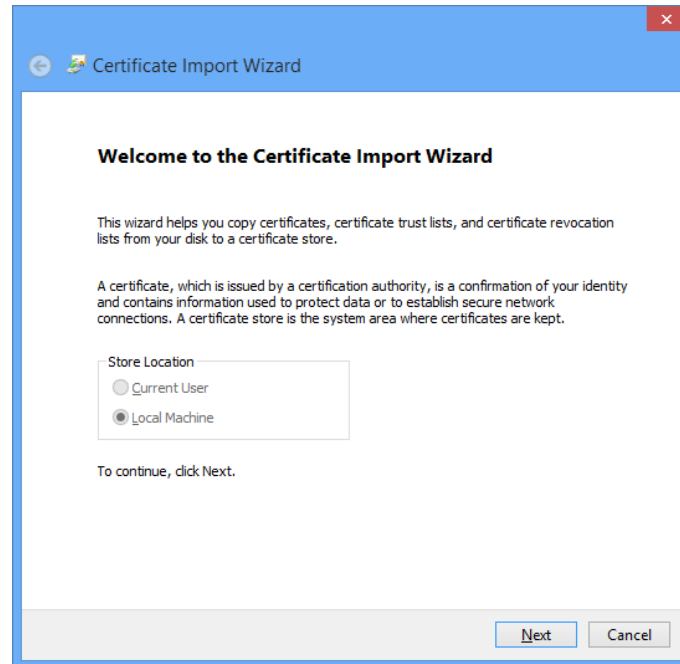
To use the certificates you installed, such as the user certificate used to authenticate a wireless LAN connection, even after the terminal is restarted, configure the thin client so that the certificates are reserved while UWF is enabled.

Important	**The user cannot customize root certificates to be retained after restart. To enable retention, the root certificates must be installed by the administrator while UWF is disabled. For details, see Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".**

Add user certificates to the UWF exclusion list so that they are not discarded after the terminal is restarted.

1. Log on to US310e as an administrator.

2. Click **Start**, **Run**, type "cmd" in the **Open** box, and then click **OK**.

3. Add the following user-specific folders to the Unified Writer Filter Exclusion List:

    (1) uwfmgr file add-exclusion c: \Users\<*username*>\AppData\Roaming\Microsoft\Crypto

    (2) uwfmgr file add-exclusion c: \Users\<*username*>\AppData\Roaming\Microsoft\Protect

    (3) uwfmgr file add-exclusion c: \Users\<*username*>\AppData\Roaming\Microsoft\SystemCertificates

4. Restart US310e to apply the addition to the exclusion list.

NEC Express5800 Series
US310e

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**

   Describes remote administration of US310e using Atrust Device Manager.

2. **Restoring Default Settings**

   Describes how to restore the default settings of US310e.

3. **Configuring and Using Peripherals**

   Describes how to configure and use peripherals.

4. **US310e Activation**

   Describes activation of US310e.

1. Using Atrust Device Manager (ADM) Software for Remote Administration

Atrust Device Manager^{TM} (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/

Important	**US310e is designed based on the premise that Atrust Device Manager is used for remote administration. Be sure to install Atrust Device Manager in the environment in which you are using US310e.**

When ACS is registered in an ADM Server, the managed status is enabled, and other ADM Servers become unable to detect the ACS. This specification is intended to prevent access from the malicious servers. If thin client isn't registered as a management target of the ADM server, it is detected by a malice server, and settings may be changed. Therefore, please be sure to make the thin client running in the production environment to the state registered as a management target of the ADM server.

Important	**If thin client that ACS configuration is set in kitting environment is migrated from kitting environment to production environment, it is necessary to be careful. In this case, you need to remove this thin client information from the kitting environment ADM server. If this operation is not performed, production environment ADM server cannot register this thin client.** **Reset Mode remove ACS configuration not only ACS managed status. Please be careful.** **The production environment ADM server executes "Pull Settings" after detecting thin client. As a result, the thin client ACS settings are synchronized to the ADM server. Thin client ACS settings are overwritten on the settings of the ADM server side when you execute the "Pull Settings". Please be careful.** **For how to use Reset Mode, see Chapter 6, "2.2 Restoring Settings by Using Atrust Client Setup"**

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 Default 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 Settings by Using Atrust Client Setup".)

- 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 Embedded 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

    US310e provides two imaging software products to re-image your thin client that runs Windows Embedded Standard:

    – Atrust Recovery USB Disk Creator^{TM}

    Recommended for smaller environments. (See Chapter 6, "2.3 Imaging Devices with Atrust Recovery USB Disk Creator".)

    – Atrust Device Manager^{TM}

    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 Device 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 US310e" 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 US310e.

2. Press the **Delete** key on the keyboard while the NEC logo is displayed on the screen.

3. Move to the **Save & Exit** menu of BIOS Setup.
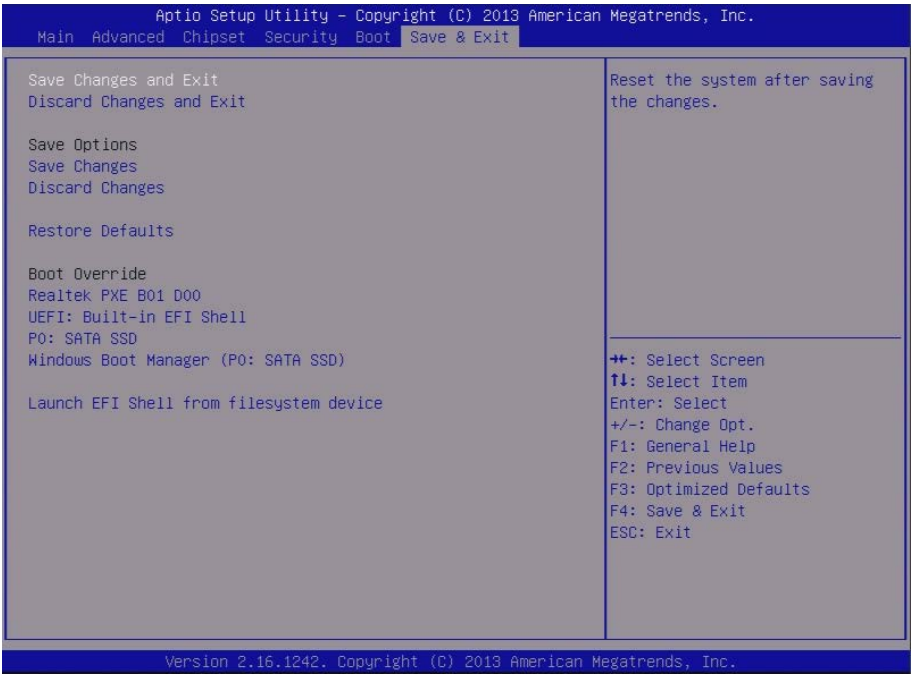
4. Select **Restore Defaults**, and press **Enter**.

5. A confirmation message "Load Optimized Defaults?" appears. Select **Yes**, and then press **Enter**.
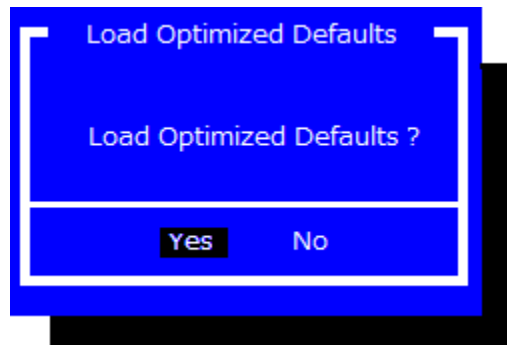
6. Select **Save Changes and Exit**, and then press **Enter**.

7. A confirmation message "Save configuration and reset?" appears. Select **Yes**, and then press **Enter**.
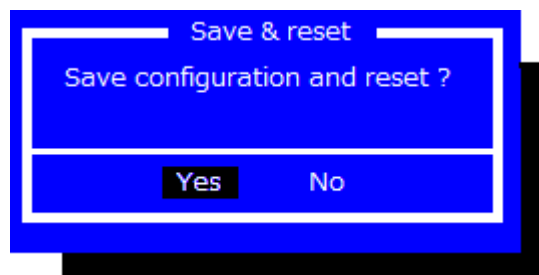
8. US310e restarts with the restored BIOS settings.

2.2   Restoring Settings by Using Atrust Client Setup

Reset Mode enables you to restore settings under Atrust Client Setup to the factory defaults. Additionally, it also releases a managed US310e 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 US310e 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 US310e 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 your US310e, do the following:

1. Restart your US310e.

2. During the POST (Power-On Self-Test) period, press **Esc** on the keyboard to enter NEC Thin Client Menu.
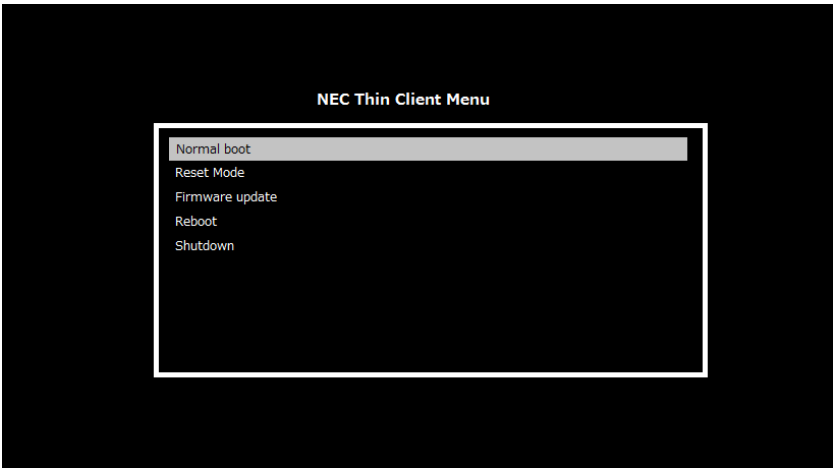
Note	Five options are available on NEC Thin Client Menu: **Normal boot**, **Reset Mode**, **Firmware Update**, **Reboot**, and **Shutdown**. See the table below for the description of each option:

Menu option	Description
Normal boot	Powers up your US310e as the normal startup procedure.
Reset Mode	Resets Atrust Client Setup settings and remote management status for your US310e.
Firmware Update	Updates firmware for your US310e through the network.
Reboot	Restarts your US310e.
Shutdown	Powers off your US310e.

Note	To perform **Firmware Update**, an Atrust Device Manager (ADM) server is required. Connect US310e 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** to continue.
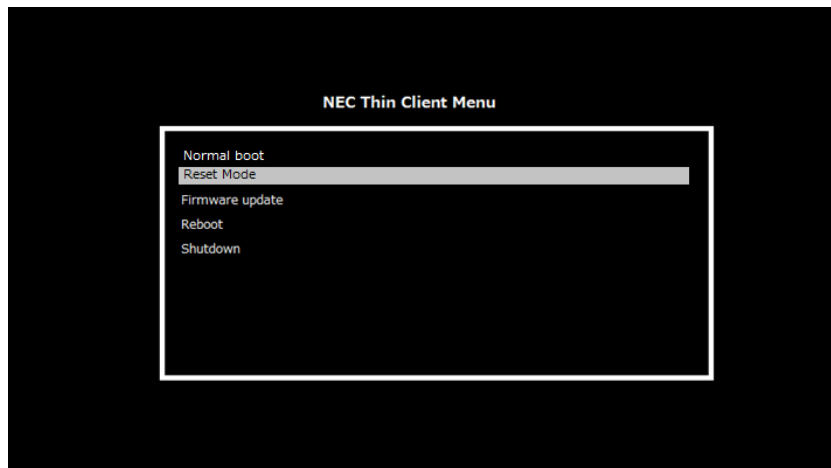
4. A message appears prompting you for confirmation. Type **y** to confirm, then press **Enter** to continue.
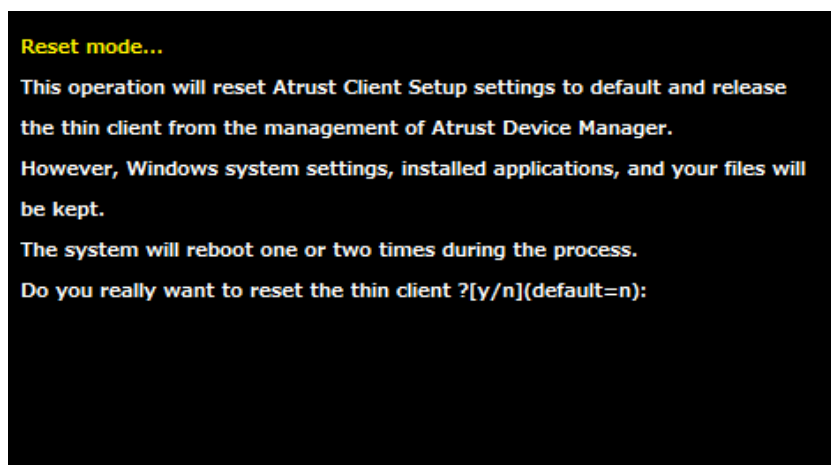
5. US310e will restart automatically.

6. After the auto sign-in, the following message will appear. Wait for a while, or click **Restart Now**.
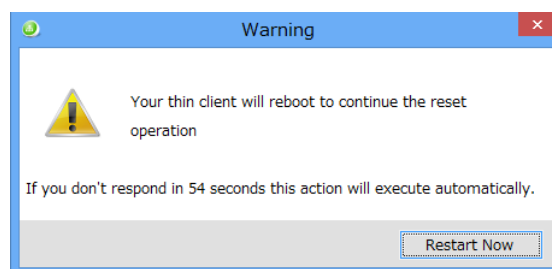
7. US310e will restart.

8. After the auto sign-in, the following message will appear. Wait for a while.
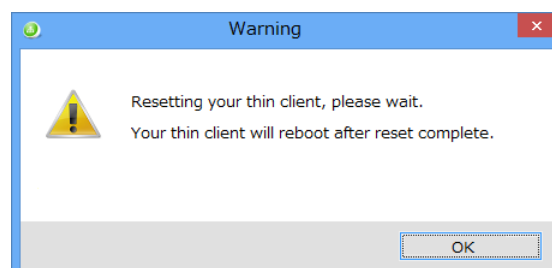
9. When US310e is restarted automatically, the restoration is completed.

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	Because the disk size of US310e is 8 GB or more, a USB flash drive of 16 GB or more is required to obtain the firmware image by using the Atrust Recovery USB Disk Creator.

3. Configuring and Using Peripherals

US310e can be connected to peripheral devices.

NEC only supports the peripheral devices that are connected by using accessories that come with US310e 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 US310e

This section describes how to activate (authenticate) US310e (Windows Embedded 8 Standard). You need to activate US310e to use all the features of Windows Embedded 8.

US310e is activated when shipped from the factory. However, if the firmware image of US310e is upgraded or recovered using ADM (Atrust Device Manger) or Atrust Device USB Disk Creator, US310e must be activated again.

Important	Disable the UWF (Unified Writer Filter) before starting activation. Upon completion of activation, enable the UWF. See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)" for how to configure UWF.

You can activate US310e via the Internet or by phone.

- Via the Internet

  Connect your US310e to the Internet, power it on, sign in with an Administrator account, and then perform the following steps:

  1. Restart your US310e.

  2. Select **Start → Apps → Control Panel → All Control Panel Items**.

  3. Select **System** on **All Control Panel Items**.
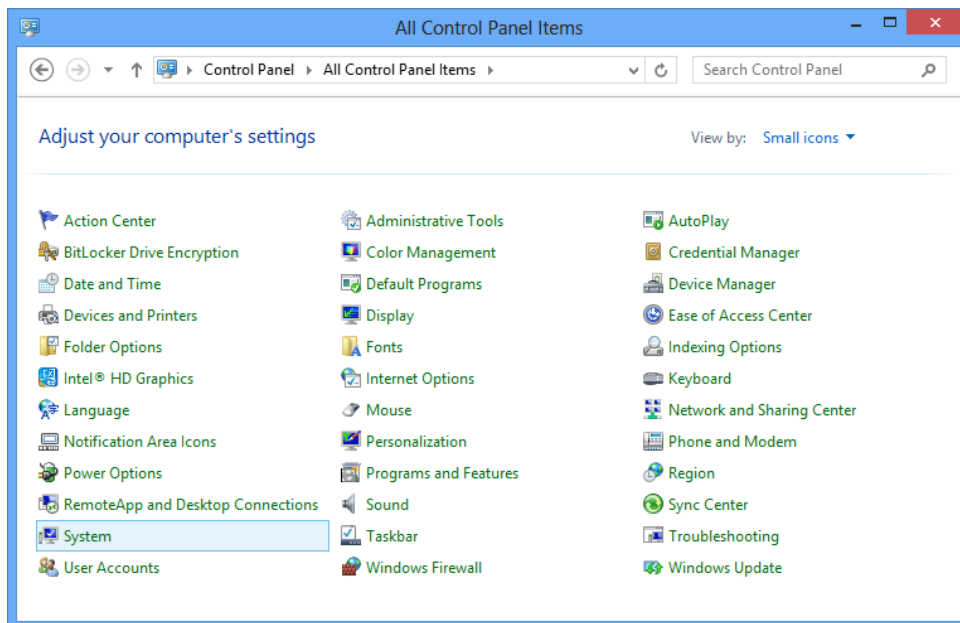
4. Click **Windows activation** in **View basic information about your computer**.
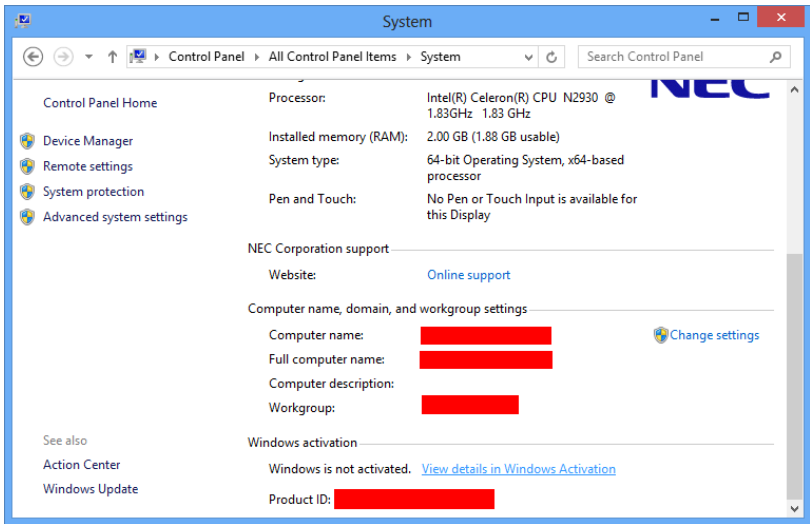
5. Click **Activate.**
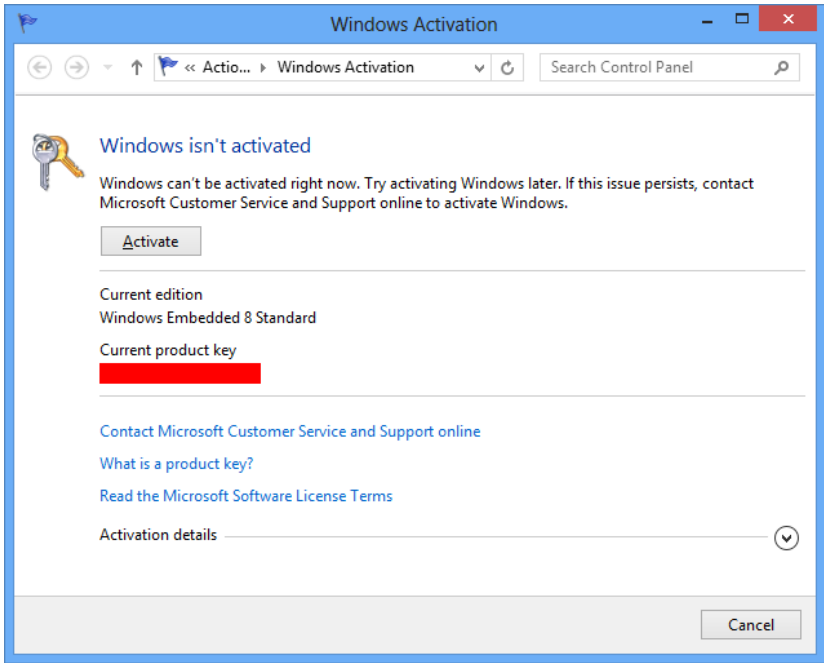
6. Windows activation dialog starts. Wait for the process to complete.
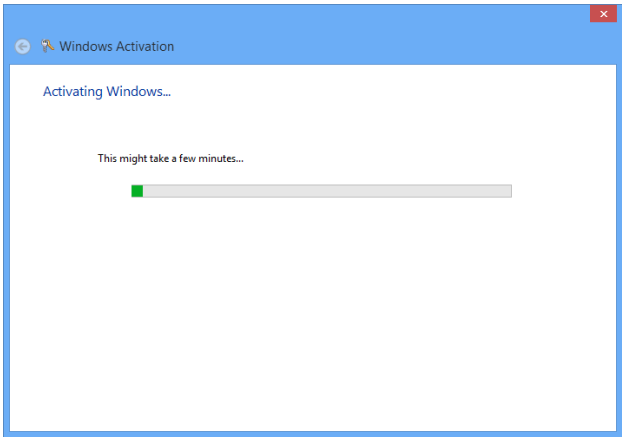
7. Upon completion of Windows activation, click **Close**.
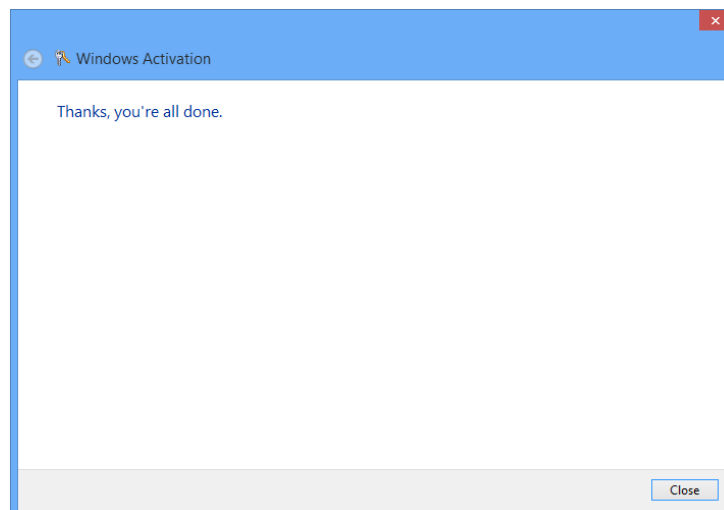
8. Confirm that **Windows is activated** is shown, and click **OK**.
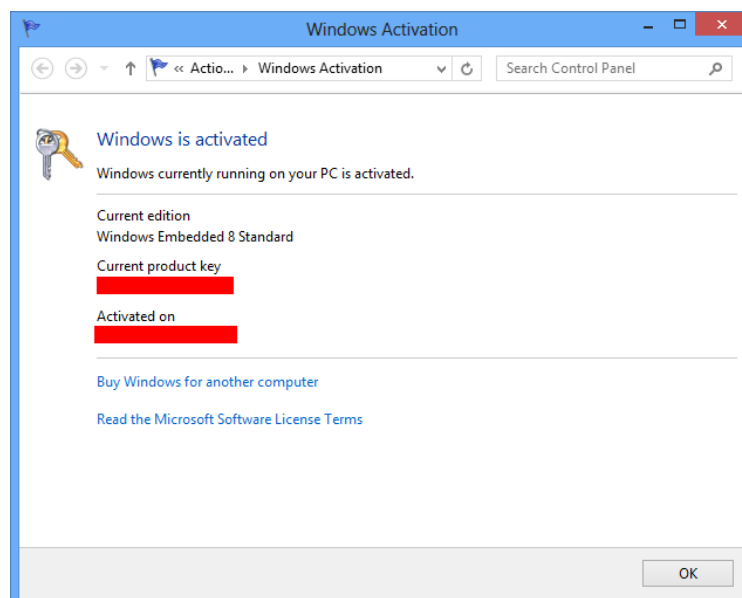
- By phone

    If the Internet is unavailable, you can activate your license by calling Microsoft.

    1. Restart your US310e.

    2. On the **Start** screen, open the **Search** charm. Type in **slui 4**, and select "slui 4" in the search results.
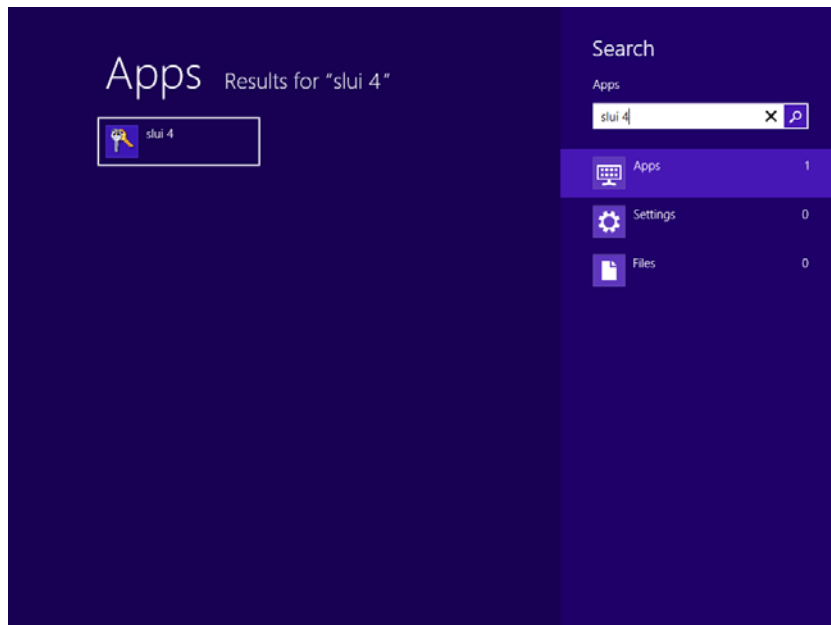
    3. Click the down arrow under **Click the nearest location** to select your region, and then click **Next**.
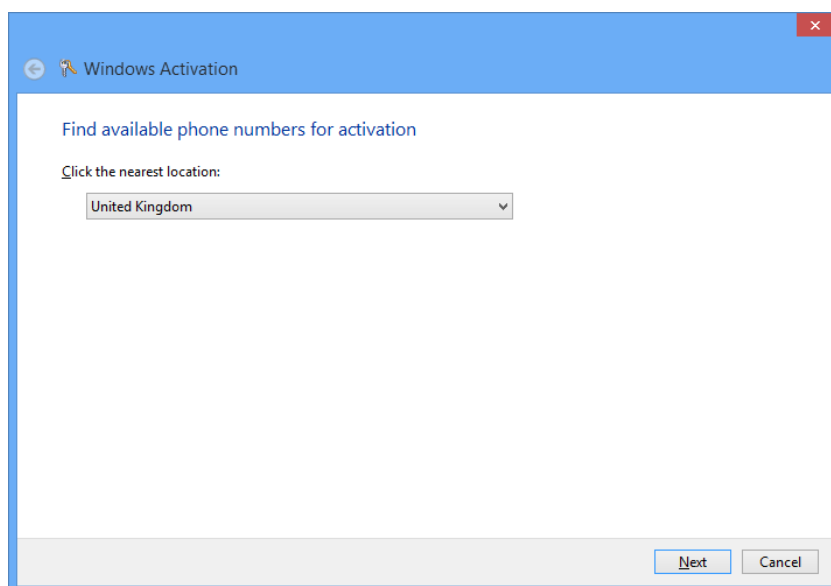
4. Call the phone number displayed on the screen. Prepare to type in the number shown under **Install ID**.

5. Follow the instructions given by the telephone system. Note down the confirmation ID number if specified.

6. Type in the confirmation ID.

7. Click the **Activate** button.

8. A message window indicating successful completion appears.

NEC Express5800 Series
US310e

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 US310e.

2. **Understanding Session Services**

   Describes the server environment of the session services available for your US310e.

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 View, 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 View, 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 View guidelines

  VMware Horizon View 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 View, see Chapter 7, "2.3 Configuring VMware Horizon View 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 or 2012 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 Server 2008 (R2)

- Windows Server 2012 (R2)

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.

US310e 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 View Session Services**

VMware Horizon View 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 View can be found on the VMware website at http://www.vmware.com.

VMware Horizon View 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 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 Manager

  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 Manager. 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 Manager, CMO Manager 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 US310e 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 US310e by default. Use the installer bundled with US310e to install it separately. For how to install CMO Terminal Agent, see Chapter 5, "13. 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 Manager.

8

Software Information, Notes, and Restrictions

This chapter describes US310e software information, and notes and restrictions on using US310e.

1. Software Information

Describes software incorporated in and used with US310e.

2. Notes and restrictions

Describes notes and restrictions on using US310e.

1. Software Information

This section describes software incorporated in and used with US310e.

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	US310e
Build version of English OS	WE8S 1.10-INTL
Build version of Japanese OS	WE8S 1.10-INTL

1.3   BIOS

Item	Description
Platform	US310e
BIOS version	US310e v1.49

1.4   Applications

Application	Version
Adobe Flash Player ActiveX	15.0.0.239
Adobe Flash Player Plugin	15.0.0.239
Atrust Client Setup (WE8S)	1.09
Citrix Receiver (Standard)	4.2.0.10(14.2.0.10)
Intel® Graphics Driver	10.18.10.3643
Intel® Trusted Execution Engine	1.0.0.1064
Internet Explorer	10.0.9200.16384
Microsoft .NET Framework 4.5	4.5.50709
Microsoft Visual C++ 2005 Redistributable	8.0.56336
Microsoft Visual C++ 2008 Redistributable (x86)	9.0.30729.17
Microsoft Visual C++ 2008 Redistributable (x86)	9.0.30729.4148
Realtek Ethernet Controller Driver	8.31.423.2014
Remote Desktop Client (RDP8.0)	6.2.9200
UltraVNC	1.0.9.5
VIA Platform Device Manager	1.42
VMware Horizon View Client	3.2.0.24246
Windows Media Player	12.0.9200.16578

1.5   Media Codecs

Your US310e contains the following codecs:

Audio

- WMA

- Dolby Digital (AC-3)

- Dolby Digital Plus (E-AC-3)

- AAC

- MP3

Video

- WMV

- MPEG-4 Visual (MPEG-4 Part 2)

- AVC.H.264 (MPEG-4 Part 10)

- VC-1

2. Notes and Restrictions

This section describes notes and restrictions on using US310e.

2.1 Features and Software Not Supported

NEC does not provide support for the features below.

- US310e(Windows Embedded 8 Standard) does not support the following enterprise features.
    - DirectAccess
    - BranCache
    - AppLocker
    - Enterprise Sideloading
- US310e (Windows Embedded 8 Standard) does not support Windows Store applications.
- 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).
- Windows Defender cannot be used.
- The UWF HORM (Hibernate Once/Resume Many) mode cannot be used.
- The Disk Cleanup utility cannot be used.
- The *Turn Windows features on or off* feature 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.
- Windows System Assessment Tool cannot be used.
- A Microsoft account cannot be used.
- The USB 3.0 host controller specification cannot be used. The BIOS USB mode is set to EHCI (USB 2.0) by default. Do not change the BIOS setting to XHCI (USB 3.0) mode. Use the default EHCI mode as is.

2.2   **Notes and Restrictions**

- 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.

- The mp4 files may be pixelated when played back on RDP, Citrix, or VMware.

- Noise will be generated on a sound when playing back HTML5 files on YouTube while connected to Remote Desktop Session Host (2012 R2).

- Recording cannot be performed in an RDP connection with VMware Horizon View version 5.3 virtual machine running Windows 8.1, but PCoIP can be used.

- If you copy a file whose size exceeds the pre-set maximum memory size (640 MB by default) of UWF to C drive of US310e while the UWF is enabled, US310e becomes extremely unstable.

- Depending on Flash contents for playback, videos may not be displayed by Internet Explorer on a local computer.

- If you install Delivery Controller and StoreFront of Citrix on another server, you will fail to acquire the XenDesktop/XenApp desktop group when configuring the ICA settings of ACS (Atrust Client Setup).

- If US310e is powered on with a Gemalto .NET smart card inserted into the smart card reader (Prox-DU, GemPC USB-SW, or SCR3310), the system will halt with a B4 BIOS POST code.

- If you a connect Microsoft 400/600 wired keyboard to a USB port and press Delete to launch the BIOS Setup utility, there is an approximate 1/50 probability that the keyboard will be disabled.

- If you connect US310e to a VMware Horizon 6.0 virtual machine running Windows 8.1 (x64) and play back a file on YouTube, the performance of the remote session is degraded. (Files can be played back smoothly on Windows 7.)

- If you connect US310e to a VMware Horizon 6.0 virtual machine running Windows 8.1 (x64) and play back an MP4 file using Microsoft Media Player, the performance of the remote session is degraded at a resolution of 1920 x 1080. (MP4 files can be played back smoothly on Windows 7.)

- If you connect US310e to a VMware Horizon 6.0 virtual machine running Windows 8.1 (x64) and play back a WMV file using Microsoft Media Player, the performance of the remote session is degraded at a resolution of 1920 x 1080. (WMV files can be played back smoothly on Windows 7.)

- 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 US310e 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 US310e 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.

- If **Lock the taskbar** is selected (checked) in the taskbar properties and if you select **Toolbar** > **Desktop** from the right-click menu of the taskbar, the Toolbar icon will be displayed incorrectly.

- If you select to check **Combine when taskbar is full** in **Taskbar Properties**, the taskbar icon will be displayed incorrectly.

- On US310e where Windows has been activated (license authenticated), a watermark (OS name and Build Number Information) may be displayed on lower right corner of the desktop of standard user account. However, you can ignore this watermark since US310e has already been activated. The watermark will disappear when any window opens on desktop.

- Help is unavailable for the standard user account. If you select Help (i.e., to click **Help** on Remote Desktop Connection), a message indicating that no Help file is installed is displayed.

- If you connect the attached USB wireless adapter, the adapter name will be shown as **Wi-Fi2**, however, this does not affect the system operation.

- When connecting to VMware Horizon View environment through Web browser, the clipboard between VMware Horizon View and local terminal is disabled.

- If you signed in with the standard user account and click Browse (i.e., select **Control Panel** > **Mouse** > **Pointer** tab > **Browse**), a message indicating that the process is canceled due to restriction of this computer is displayed. However, clicking **OK** will open the Browse window.

- With the standard user account, you cannot select a theme in **Windows Standard Themes**. You can select a theme from **High-Contrast Themes**.

- Even if **Return to Logon Screen at Resume** is enabled in screensaver setting, the screen before the screensaver works is displayed instead of Windows Sign-on screen.

- When the USB devices are connected to US310e, some devices start autoplay. To suppress the autoplay feature for all of the accounts including Administrator account, disable the UWF first, set the group policy according to the steps described below, and then enable the UWF.

    (1)   Sign in US310e with an Administrator account.

    (2)   Click **Run** from the Start menu.

    (3)   Enter **gpedit.msc**, and click **OK**.

    (4)   Select **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Autoplay Policies**.

    (5)   Double-click **Turn Off AutoPlay**, select **Enable** in the dialog box opened, select **All Drives** as an option, and then click **OK**.

    (6)   Double-click **Prevent AutoPlay From Remembering User Choice**, select **Enable** in the dialog box opened, and then click **OK**.

    (7)   Double-click **Enable or Disable AutoPlay for Non-volume Devices**, select **Enable** in the dialog box opened, and then click **OK**.

    (8)   Double-click **Default Behavior for AutoRun**, select **Enabled** in the dialog box opened, select **Do not execute any autorun commands** as an option, and then click **OK**.

    (9)   Click **Run** from the Start menu.

    (10) Enter **gpupdate /force**, and click **OK**.

- If you select a theme from High-Contrast Theme with the standard user account, the window color will be changed. When you sign-in again, the window color will return to its original color.

- Input method cannot be added to Japanese, Chinese and Korean languages.

- The **Change how your mouse works** and **Change how your keyboard works** available in **Control Panel** > **Ease of Access Center** do not work properly. Do not use the **Change how your mouse works** or **Change how your keyboard works**.

- In US310e local environment, the shortcut keys combined with Windows logo key are disabled.

- In ICA session created by Atrust Client Setup, the session window will be minimized when **Left Alt** + **Left Shift** + **NumLock** keys are pressed to change mouse key feature.

- If you create a remote desktop by specifying "Web Feed" for connection type on Add / Edit Remote Desktop in Atrust Client Setup, the change made in Options tab of the remote desktop will not be applied to the new remote desktop connection.

- If "Manual" is specified and saved on Add / Edit VMware View session of Atrust Client Setup with the setting for Desktop Name remained, the desktop specified here is launched when connecting to VMware View session. In this case, select "Microsoft RDP" or "PCoIP" for connection method to remove the desktop name, and then change connection method to "Manual".

- If "SSL/TSL+HTTPS serverlocation" is specified as network protocol when specifying an option for Add / Edit Citrix ICA Session in Atrust Client Setup, an error will occur when connecting to Citrix ICA session. Do not specify "SSL/TSL+HTTPS serverlocation" for network protocol.

- In Citrix ICA session connected with XenDesktop 7 or later, "RC5 128 bit (login only)", "RC5 40 bit", and "RC5 56 bit" keys cannot be used for encryption due to specification of XenDesktop. In Atrust Client Setup, "RC5 128 bit (login only)", "RC5 40 bit", "RC5 56 bit", and "RC5 128 bit" keys can be used for encryption by specifying an option on Add / Edit Citrix ICA Session. However, if you use XenDesktop 7 or later and use encrypted connection, use only "RC5 128 bit" key. Do not use "RC5 128 bit (login only)", "RC5 40 bit", or "RC5 56 bit" key.

- In the password setting for remote shadows in Atrust Client Setup, specify less than eight characters although more than eight characters can be entered. If more than eight characters are entered, only the first eight characters are set as a password. In addition, when setting a password while the remote shadow is enabled, only the first eight characters are used for authentication although more than eight characters can be entered in the text box.

- If you need to upgrade the Adobe Flash Player ActiveX and the Adobe Flash Player Plugin, use the Archived Flash Player versions. Download the modules of desired version from the Archived Flash Player versions site, and expand it on US310e with administrative user. Install "flashplyerxx_xxx_xxx_winax.exe" and "flashplayerxx_xxx_xxx_win.exe" from the unzipped folder. For the file "flashplyerxx_xxx_xxx_winax.exe", first right-click the file and select **Properties** from the menu, select **Compatibility** tab, **Compatibility**, and select the **Run this program in Compatibility** checkbox. Select **Windows 7** from the drop-down list, and click **OK** to close the dialog. Then, launch the installer and install the modules according to the wizard.

- The Flash Player Settings Manager that allows you to configure the Flash Player is not installed. To install the Flash Player Settings Manager, first uninstall the Adobe Flash Player ActiveX and the Adobe Flash Player Plugin, then install the Adobe Flash Player according to upgrade procedure described above.

- 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 View 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.

- Even if the default home page of Internet Explorer is changed in Internet Explorer>Internet options > General>Home page, the setting is overwritten by Atrust Client Setup after sign out or shutdown. To change default home page of Internet Explorer, the setting must be configured in Atrust Client Setup> Application>Web Browser->Global Setting>Basic Settings>Home page.

NEC Express5800 Series
US310e

9

Operation and Maintenance

This chapter describes troubleshooting and how to maintain US310e to keep it running smoothly.

1. Cleaning of US310e

Describes how to clean US310e 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 US310e.

4. User Support

Describes user support related to US310e.

1. Cleaning

Clean US310e on a regular basis to keep it in good shape.

WARNING
⚠️⚠️🚫 **Observe the following instructions to use US310e safely. Failure to follow these instructions may result in loss of life or serious personal injury.** • **Do not disassemble, repair, or alter US310e.**

1.1　Cleaning of US310e

Wipe off dirt on the surface of US310e with a soft cloth. If dirt is hard to remove, US310e 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 US310e.** • **Do not allow US310e, plugs, cables, rear connectors or the surrounding area to become wet.**

1. Confirm that the power of US310e is off.

2. Pull out the power cord of US310e 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 US310e 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 US310e with a dry cloth.

2. Troubleshooting

Any of the problems listed in this section might be resolved by updating the US310e firmware. For how to update the firmware, see Chapter 6, "2. Restoring Default 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 US310e, RDP connection to the virtual PC might fail. Set the correct date and time. The date and time are not set immediately after US310e 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 US310e

[?] **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 US310e is malfunctioning, depending on the conditions under which it is being used.
Wait for a while, and if the problem is not resolved, restart US310e.
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 system will not enter standby mode:**

→ US310e does not support standby operations.
If US310e starts operating strangely after attempting to enter standby mode, restart it.

[?] **The screen will not display the maximum resolution:**

→ Check that the DVI-VGA adapter that you are using is the one supplied with US310e.
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 US310e, contact your service representative.

WARNING

Observe the following instructions to use US310e 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 US310e.**
- **Do not remove the lithium battery.**
- **Do not handle US310e with the power cord of US310e connected to a power source.**

CAUTION

Observe the following instructions to use US310e safely. Failure to follow these instructions may cause a fire, personal injury, or property damage.

- **Do not drop US310e.**

Important
- **When carrying out major work such as changing the floor layout, contact your sales or service representative.**
- **To enable US310e and built-in devices to operate properly following relocation or storage, it is recommended to keep US310e in a place where standard room temperature can be maintained.**
- **Observe the storage conditions (temperature: –10°C to 55°C, humidity: 20% to 80% and no condensation) when storing US310e.**

1. Turn off US310e. (The Power status LED goes off.)

2. Pull out the power cord connected to US310e from the inlet.

3. Remove all cables connected to US310e.

4. Pack US310e securely so as to avoid damage, shock and vibration.

Important   **Before operating US310e 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 US310e 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.

10

Appendix

**NEC Express5800 Series
US310e**

Appendix A   Specifications

Provides specifications of US310e.

Appendix A   Specifications

Item	Specification
Processor	Intel® Celeron® N2930 1.83 GHz Quad-core processor
Memory	16GB flash memory / 2GB 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) External wireless LAN option: 802.11 a/b/g/n/ac (2.4GHz, 5GHz supported) (N8120-118) Supports WPA Personal, WPA2 Personal, WPA Enterprise, WPA2 Enterprise, and WPA Enterprise Authentication
Display	Single: Max. 1920x1200@32 bpp Dual: Max. 1920x1080@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, monitor ×1, and wireless LAN adapter (N8120-118) ×1): Approx. 12.2 watts
Temperature range	Operating: 10°C to 35°C (50°F to 95°F), when mounted vertically 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, EN 60950, CSA60950 FCC Class B, CE, VCCI WEEE, RoHS compliant

US310e
User's Guide

Second edition, May 2015

NEC Corporation
7-1 Shiba 5-Chome, Minato-Ku
Tokyo 108-8001, Japan