

Express5800 Series

---

## **US310e User's Guide**



### **FW WE8S 1.30-INTL**


- Chapter 1 About US310e**
- Chapter 2 Before Getting Started**
- Chapter 3 Using US310e**
- Chapter 4 Configuring Client Settings with Atrust Client Setup**
- Chapter 5 Administrative Utilities and Settings**
- Chapter 6 System Administration**
- Chapter 7 Establishing a Server Environment**
- Chapter 8 Software Information, Notes, and Restrictions**
- Chapter 9 Operation and Maintenance**
- Chapter 10 Appendix**

---


# 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.
---	-----------------	---

---

	User's Guide	
	Precautions for Use	<i>Be sure to read this section before using this device.</i> 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

<b>Documents for US310e .....</b>	<b>2</b>
<b>Contents .....</b>	<b>3</b>
<b>Notations Used in This Document .....</b>	<b>8</b>
Notations used in the text .....	8
Abbreviations of Operation Systems .....	9
<b>Trademarks.....</b>	<b>10</b>
<b>Warnings and Additions to This Document .....</b>	<b>11</b>
To find the necessary information .....	11
<b>Confirmation of Accessories .....</b>	<b>12</b>
<b>Transfer to Third Parties .....</b>	<b>12</b>
<b>Disposal.....</b>	<b>12</b>
<b>Shipping .....</b>	<b>12</b>
<b>License, Rights, and Regulatory Compliance .....</b>	<b>13</b>
Rights 13	
Restricted Rights Legend.....	13
Regulatory Compliance for Thin Clients .....	13
AC Adapter .....	13
FCC Statement.....	13
Industry Canada Class B Emission Compliance Statement/ Avis de conformité à la réglementation d'Industrie Canada .....	13
WEEE Directive.....	14
Vietnam RoHS information relevant for Vietnam market .....	14
Turkish RoHS information relevant for Turkish market .....	14
台灣電池規制 (廢棄物清理法) .....	14
限用物質含有情況標示聲明書 (Declaration of the Presence Condition of the Restricted Substances Marking) .....	14
<b>Precautions for Use (Be Sure to Read) .....</b>	<b>15</b>
Safety Precautions .....	15
Symbols Used in This document and on Warning Labels .....	16
Safety notes.....	17
General 17	
Power supply and power cord .....	18
Installation, relocation, storage, and connection .....	19
Battery unit.....	20
During Operation .....	20
Wireless features (when using N8120-118 (option)).....	21
Cleaning and working with internal devices .....	21
For Proper Operation .....	22
<b>Chapter 1 About US310e .....</b>	<b>24</b>
<b>1. Introduction.....</b>	<b>25</b>
<b>2. Names and Functions of Components .....</b>	<b>26</b>
<b>2.1 Front View .....</b>	<b>26</b>
<b>2.2 Rear View.....</b>	<b>27</b>
2.2.1 DVI-I port .....	28
2.2.2 DVI-D port.....	28
2.2.3 USB 2.0 port.....	28

2.2.4 USB 3.0 port.....	28
2.2.5 LAN connector .....	28
2.2.6 Power connector.....	28
<b>2.3 Top View .....</b>	<b>29</b>
<b>3. Installation and Connection .....</b>	<b>30</b>
<b>3.1 Installation .....</b>	<b>30</b>
3.1.1 Placing on a desk .....	30
3.1.2 Mounting on the back of a monitor.....	31
<b>3.2 Connection .....</b>	<b>35</b>
<b>4. Setting up the System BIOS .....</b>	<b>37</b>
<b>4.1 Overview.....</b>	<b>37</b>
<b>4.2 Starting SETUP .....</b>	<b>37</b>
<b>4.3 Keys and Screens .....</b>	<b>38</b>
<b>4.4 Parameters.....</b>	<b>39</b>
4.4.1 Main.....	39
4.4.2 Advanced menu .....	40
4.4.3 Chipset menu.....	41
4.4.4 Intel IGD Configuration .....	42
4.4.5 South Bridge .....	43
4.4.6 Security menu.....	44
4.4.7 Boot .....	45
4.4.8 Save & Exit .....	46
<b>Chapter 2 Before Getting Started .....</b>	<b>47</b>
<b>1. UWF (Unified Write Filter) .....</b>	<b>48</b>
<b>2. Default User Accounts .....</b>	<b>49</b>
<b>3. the Behavior of System Startup .....</b>	<b>51</b>
<b>3.1 Switching the Sign-In User .....</b>	<b>51</b>
<b>4. Standard / Customized Desktop Shortcuts .....</b>	<b>53</b>
<b>5. Connecting to a Printer .....</b>	<b>54</b>
<b>6. Connecting to a Monitor .....</b>	<b>55</b>
<b>6.1 Supported Monitor Configurations.....</b>	<b>55</b>
<b>Chapter 3 Using US310e .....</b>	<b>56</b>
<b>1. Standard Shortcuts .....</b>	<b>57</b>
<b>2. Accessing Citrix Services .....</b>	<b>58</b>
<b>2.1 Accessing Citrix Service with Internet Explorer .....</b>	<b>58</b>
<b>2.2 Accessing Citrix Service through the Citrix Receiver Shortcut .....</b>	<b>60</b>
<b>3. Accessing Microsoft Remote Desktop Services .....</b>	<b>62</b>
<b>3.1 Accessing Microsoft Remote Desktop Services by Using Remote Desktop Connection .....</b>	<b>62</b>
<b>3.2 Accessing Microsoft Remote Desktop Services by Using Remote Desktop Connection (Span Mode) .....</b>	<b>64</b>
<b>3.3 Accessing Remote Desktop Services by Using RemoteApp and Desktop Connection .....</b>	<b>66</b>
<b>3.4 Accessing Remote Desktop Services by Using Internet Explorer .....</b>	<b>69</b>
<b>4. Accessing VMware View and Horizon View Services .....</b>	<b>70</b>
<b>4.1 Accessing VMware View and Horizon View Services by Using VMware Horizon View Client .....</b>	<b>70</b>
<b>4.2 Accessing VMware View and Horizon View Services by Using Internet Explorer .....</b>	<b>72</b>
<b>5. Accessing NEC Client Management Option (CMO) Services .....</b>	<b>73</b>
<b>5.1 Accessing NEC Client Management Option (CMO) Services by Using CMO Terminal Agent .....</b>	<b>73</b>
<b>6. Browsing the Internet by Using Internet Explorer.....</b>	<b>75</b>

<b>Chapter 4</b>	<b>Configuring Client Settings with Atrust Client Setup</b>	<b>76</b>
<b>1.</b>	<b>Atrust Client Setup (ACS)</b>	<b>77</b>
1.1	Interface Overview	77
1.2	Client Settings	78
<b>2.</b>	<b>Configuring System Settings</b>	<b>79</b>
2.1	System Tab Overview	79
2.2	Available Settings	80
2.3	Setting a Password to Access Atrust Client Setup	81
2.4	Configuring Shadow Settings for Remote Assistance	83
2.5	Updating Firmware from the Management Computer	85
2.6	Taking Snapshots for Mass Deployment	87
2.7	Deploying a System Image Using a Taken Snapshot	89
2.7.1	Deploying a Snapshot System Image via Network	89
2.7.2	Deploying a Snapshot System Image from a USB Flash Memory	91
2.7.3	About snapshot diversion restriction by change of parts	92
2.8	Enabling or Disabling the Appliance Mode	94
2.8.1	Enabling the Appliance Mode	94
2.8.2	Disabling the Appliance Mode	97
2.9	Configuring UWF (Unified Write Filter)	99
<b>3.</b>	<b>Configuring External Device Settings</b>	<b>101</b>
3.1	Devices Tab Overview	101
3.2	Available Settings	101
3.3	Configuring Settings for USB Storage Devices	102
3.4	Disabling or Enabling Attached Audio Devices	103
<b>4.</b>	<b>Configuring User Interface Settings</b>	<b>104</b>
4.1	User Interface Tab Overview	104
4.2	Available Settings	104
4.3	Configuring the Display of Standard Desktop Shortcuts for Quick Access	105
<b>5.</b>	<b>Configuring Service Access Settings</b>	<b>106</b>
5.1	Applications Tab Overview	106
5.2	Available Settings	107
5.3	Configuring Basic RDP Connection Settings	108
5.3.1	Connection Type: Remote Desktop	108
5.3.2	Connection Type: Remote Web Access	110
5.3.3	Connection Type: Web Feed	111
5.4	Accessing Remote Desktop Services	113
5.4.1	Connection Type: Remote Desktop	113
5.4.2	Connection Type: Remote Web Access	114
5.4.3	Connection Type: Web Feed	116
5.5	Configuring Advanced RDP Connection Settings	117
5.5.1	Settings for the Connection Type of Remote Desktop	117
5.5.2	Settings for the Connection Type of Remote Web Access	122
5.5.3	Settings for the Connection Type of Web Feed	123
5.6	Configuring Basic ICA Connection Settings	124
5.6.1	Connection Type: Web Logon	124
5.6.2	Connection Type: XenDesktop	126
5.6.3	Connection Type: XenApp	128
5.6.4	Connection Type: Server Connection	130
5.7	Accessing Citrix Services	132
5.7.1	For Connection Types of XenDesktop, XenApp, and Server Connection	132
5.7.2	For Connection Types of Web Logon	132
5.8	Configuring Advanced ICA Connection Settings	134
5.8.1	Settings for the Connection Type of Web Logon	134
5.8.2	Settings for the Connection Type of XenDesktop	136
5.8.3	Settings for the Connection Type of XenApp	138
5.8.4	Settings for the Connection Type of Server Connection	140
5.9	Configuring Basic VMware View Connection Settings	142
5.10	Accessing VMware View or Horizon View Services	144
5.11	Configuring Advanced View Connection Settings	146

<b>5.12</b> Configuring Web Browser Settings.....	148
5.12.1 Configuring General Browser Session Settings .....	148
5.12.2 Configuring Specific Browser Session Settings .....	149
<b>Chapter 5 Administrative Utilities and Settings .....</b>	<b>151</b>
<b>1. Launching UWF Automatically .....</b>	<b>152</b>
<b>2. Utilities Affected by Shutdown and Restart.....</b>	<b>153</b>
<b>3. Using the Unified Write Filter (UWF).....</b>	<b>154</b>
<b>3.1</b> Changing Passwords with the Unified Writer Filter Enabled .....	155
3.1.1 Disabling the machine account password change on the thin client .....	155
3.1.2 Disabling the machine account password change in domain controller.....	155
<b>3.2</b> Running Unified Writer Filter Command Line Options .....	156
<b>4. Automatic Sign-In .....</b>	<b>159</b>
<b>5. Saving Files and Using Local Drives .....</b>	<b>162</b>
<b>6. Mapping Network Drives .....</b>	<b>163</b>
<b>7. Participating in Domains .....</b>	<b>164</b>
<b>8. Using the Net and Tracert Utilities .....</b>	<b>165</b>
<b>9. Managing Users and Groups with User Accounts .....</b>	<b>166</b>
<b>9.1</b> Creating User Accounts.....	166
<b>9.2</b> Editing User Accounts .....	166
<b>9.3</b> Configuring User Profiles .....	166
<b>10. Changing the Computer Name of a Thin Client .....</b>	<b>167</b>
<b>11. Setting Date and Time .....</b>	<b>168</b>
<b>12. Configuring Dual Monitor Display.....</b>	<b>169</b>
<b>13. Installing CMO Terminal Agent .....</b>	<b>170</b>
<b>14. Setting up a Wireless Local Area Network (LAN).....</b>	<b>175</b>
<b>14.1</b> Selecting a Network (SSID) for Connection .....	175
<b>14.2</b> Manually Creating a Network Profile for Connection .....	180
<b>14.3</b> Managing a Network Profile .....	185
14.3.1 Checking a Network Profile (SSID) .....	185
14.3.2 Deleting a Network Profile (SSID) .....	189
14.3.3 Managing a Network Profile (SSID) from the Command Prompt.....	191
<b>15. Saving Wireless Connections .....</b>	<b>192</b>
<b>15.1</b> Using PEAP Fast Reconnect .....	193
<b>16. Saving the Certificate .....</b>	<b>194</b>
<b>Chapter 6 System Administration .....</b>	<b>197</b>
<b>1. Using Atrust Device Manager (ADM) Software for Remote Administration .....</b>	<b>198</b>
<b>2. Restoring Default Settings.....</b>	<b>199</b>
<b>2.1</b> Restoring BIOS Settings.....	200
<b>2.2</b> Restoring Settings by Using Atrust Client Setup.....	202
<b>2.3</b> Imaging Devices with Atrust Recovery USB Disk Creator .....	204
<b>3. Configuring and Using Peripherals .....</b>	<b>205</b>

<b>4. Activating US310e</b> .....	<b>206</b>
<b>4.1</b> Via the Internet.....	207
<b>4.2</b> By phone.....	210
<b>4.3</b> Activating US310e via the Volume Activation Management Tool (VAMT).....	212
<b>Chapter 7 Establishing a Server Environment</b> .....	<b>213</b>
<b>1. Understanding How to Configure Your Network Services</b> .....	<b>214</b>
<b>1.1</b> Using Dynamic Host Configuration Protocol (DHCP).....	214
<b>1.2</b> Using Domain Name System (DNS).....	214
<b>2. Understanding Session Services</b> .....	<b>215</b>
<b>2.1</b> Configuring Citrix ICA Session Services.....	216
<b>2.2</b> Configuring Microsoft RDP Session Services.....	216
<b>2.3</b> Configuring VMware Horizon View Session Services.....	217
<b>2.4</b> Configuring NEC Client Management Option (CMO) Services.....	218
<b>Chapter 8 Software Information, Notes, and Restrictions</b> .....	<b>219</b>
<b>1. Software Information</b> .....	<b>220</b>
<b>1.1</b> Disk Configuration.....	220
<b>1.2</b> OS Build.....	220
<b>1.3</b> BIOS.....	222
<b>1.4</b> Applications.....	223
<b>1.5</b> Media Codecs.....	224
<b>2. Notes and Restrictions</b> .....	<b>225</b>
<b>2.1</b> Features and Software Not Supported.....	225
<b>2.2</b> Notes and Restrictions.....	226
<b>Chapter 9 Operation and Maintenance</b> .....	<b>232</b>
<b>1. Cleaning</b> .....	<b>233</b>
<b>1.1</b> Cleaning of US310e.....	233
<b>2. Troubleshooting</b> .....	<b>234</b>
<b>2.1</b> Problems When Connecting to Virtual PCs.....	234
<b>2.2</b> Other Problems with Using US310e.....	234
<b>3. Relocation and Storage</b> .....	<b>235</b>
<b>4. User Support</b> .....	<b>236</b>
<b>4.1</b> Before Requesting Repairs.....	236
<b>4.2</b> When Requesting Repairs.....	236
<b>4.3</b> About Repair Parts.....	236
<b>Chapter 10 Appendix</b> .....	<b>237</b>
<b>Appendix A Specifications</b> .....	<b>238</b>

---

## 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.

<b>Important</b>	Indicates critical items that must be observed when handling US310e or its software. If the procedures described are not followed, <i>hardware failure, data loss, and other serious malfunctions might occur.</i>
<b>Note</b>	Indicates items that must be confirmed when handling US310e or its software.
<b>Tip</b>	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 10	Windows 10 Enterprise 64-bit (x64) Edition
	Windows 10 Enterprise 32-bit (x86) Edition
Windows 8.1	Windows 8.1 Enterprise 64-bit (x64) Edition
	Windows 8.1 Enterprise 32-bit (x86) Edition
Windows 8	Windows 8 Enterprise 64-bit (x64) Edition
	Windows 8 Enterprise 32-bit (x86) Edition
Windows 7	Windows 7 Enterprise 64-bit (x64) Edition
	Windows 7 Enterprise 32-bit (x86) Edition
Windows 2012	Windows Server 2012 R2 Datacenter Edition
	Windows Server 2012 R2 Standard Edition
	Windows Server 2012 Datacenter Edition
	Windows Server 2012 Standard Edition
Windows 2008	Windows Server 2008 R2 Standard Edition
	Windows Server 2008 R2 Enterprise Edition
	Windows Server 2008 32-bit Standard Edition
	Windows Server 2008 32-bit Enterprise Edition
	Windows Server 2008 64-bit Standard Edition
	Windows Server 2008 64-bit Enterprise Edition

---

## Trademarks

---

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.58support.nec.co.jp/global/download/>

---

## To find the necessary information

---

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

---

## Confirmation of Accessories

---

Refer to the attached startup guide to confirm the accessories in the 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.

## 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"

## Turkish RoHS information relevant for Turkish market

EEE Yönetmeliğine Uygundur

## 台灣電池規制 (廢棄物清理法)



廢電池請回收

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

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

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



## Precautions for Use (Be Sure to Read)

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

### Safety Precautions

Follow the instructions in this document for the safe use of 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:



Indicates there is a risk of death or serious personal injury.

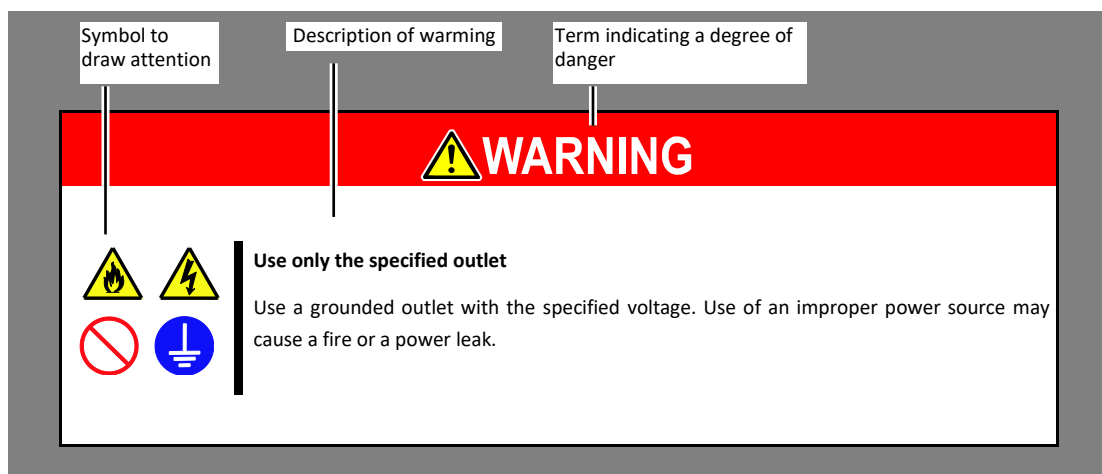


Indicates there is a risk of burns, other personal injury, or property damage

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









## 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

 <b>WARNING</b>	
	<p><b>Do not use US310e for services which may directly affect human lives and for which critically high reliability is required.</b></p> <p>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.</p>
 	<p><b>Do not use US310e if any smoke, odor, or noise is present.</b></p> <p>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.</p>
 	<p><b>Do not insert wires or metal objects.</b></p> <p>Do not insert wires or metal objects into ventilation holes or USB connectors. Doing so may cause an electric shock.</p>

 <b>CAUTION</b>	
   	<p><b>Keep water or foreign matter away from US310e.</b></p> <p>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 enters 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.</p>

## 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))

 <b>CAUTION</b>	
	<p><b>Keep US310e at least 30 cm away from an internal artificial cardiac pacemaker.</b></p> <p>Use US310e at least 30 cm away from an internal artificial cardiac pacemaker. Internal artificial cardiac pacemakers may be affected by radio waves.</p>
	<p><b>Turn off the power or wireless communication features of US310e in places where use of US310e is prohibited.</b></p> <p>Turn off the power or wireless communication features of US310e in places where use of US310e is prohibited (such as medical treatment facilities).</p> <p>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.</p>
	<p><b>Turn off the wireless communication features of US310e if US310e cause radio interference.</b></p> <p>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.</p>

## Cleaning and working with internal devices

 <b>CAUTION</b>	
  	<p><b>Do not disassemble, repair, or alter US310e.</b></p> <p>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.</p>
  	<p><b>Disconnect the power plug before opening US310e.</b></p> <p>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.</p> <p>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.</p>

---

## 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:  $-10^{\circ}\text{C}$  to  $55^{\circ}\text{C}$  ( $14^{\circ}\text{F}$  to  $131^{\circ}\text{F}$ ), 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.

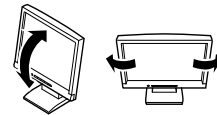
You have "good working posture" as described above when no part of your body is under excess strain, in other words when your muscles are most relaxed.

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.



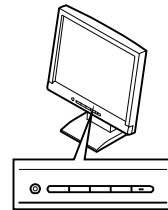
### Adjustment of Display Unit Angles

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.



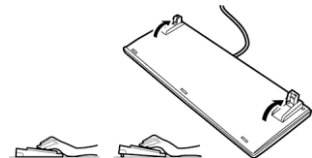
### Adjustment of Screen Brightness and Contrast

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.



---

---

# **Chapter 1 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

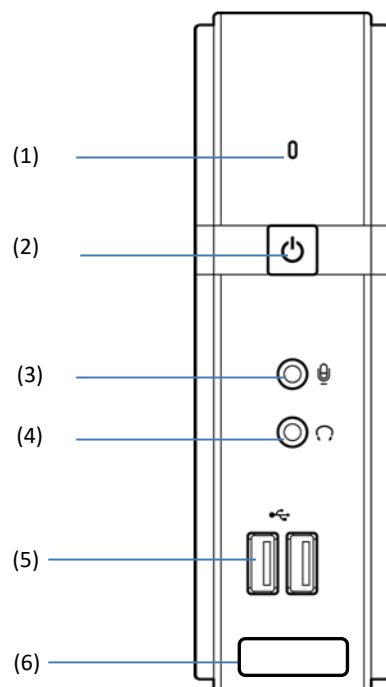
---

This section describes the names and functions of US310e components.

---

### 2.1 Front View

---



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

(2) Power switch

(3) Microphone connector

(4) Headphone connector

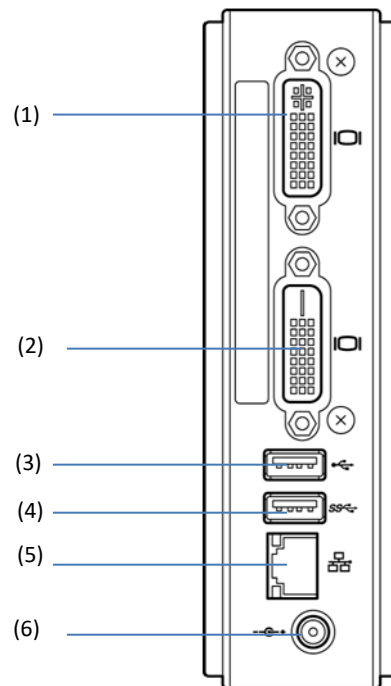
(5) USB 2.0 ports (2 ports)

(6) COA label (\*2)

\*1 US310e does not support standby operations.

\*2 Do not peel off the label stuck on the front of the device.

## 2.2 Rear View



(1) DVI-I port

(2) DVI-D port

(3) USB 2.0 port

(4) USB 3.0 port (\*1)

(5) LAN connector

(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.

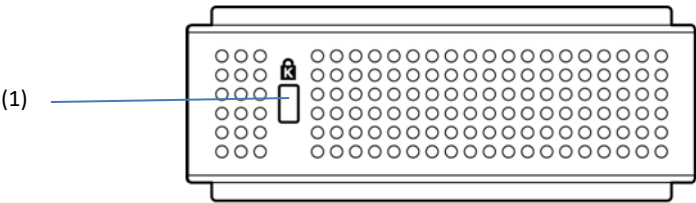
### 2.2.6 Power connector

---

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

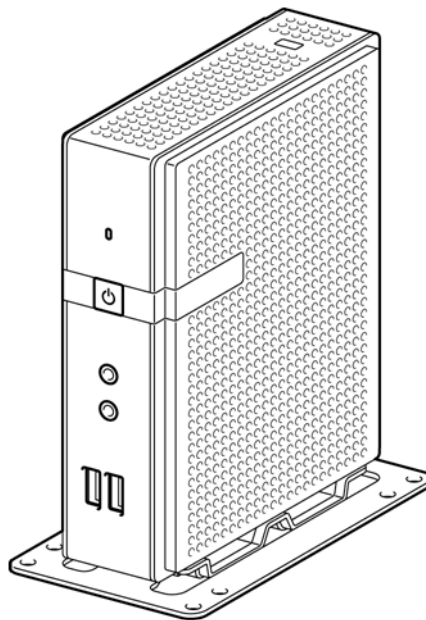
---

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.

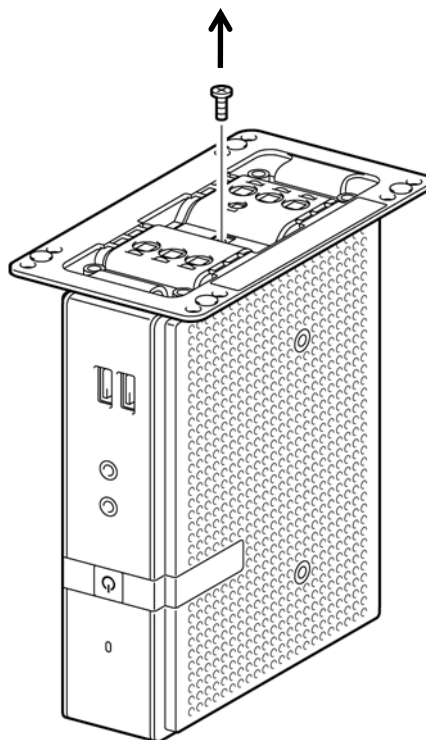


### 3.1.2 Mounting on the back of a monitor

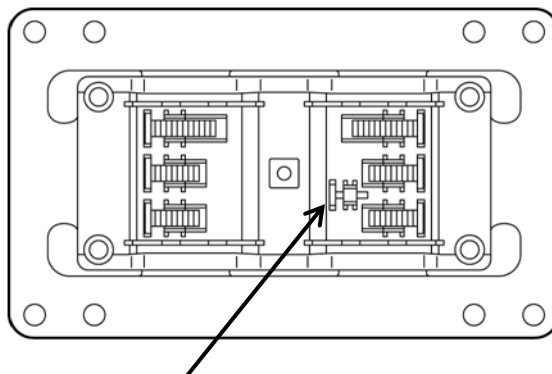
Mount US310e on the back of a monitor by using the stand.

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.



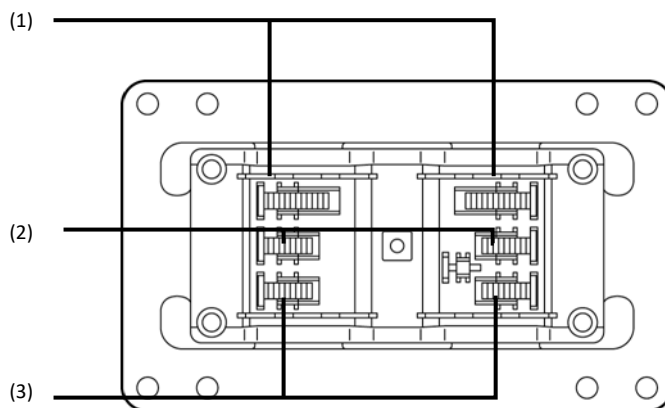
Store the removed screw inside the stand.



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.



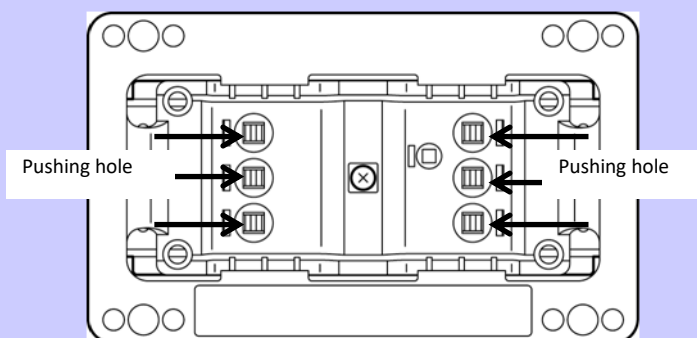
(1) Fixing screw for monitor (long) (Approx. 13 mm)

(3) Fixing screw for body

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

#### Tips

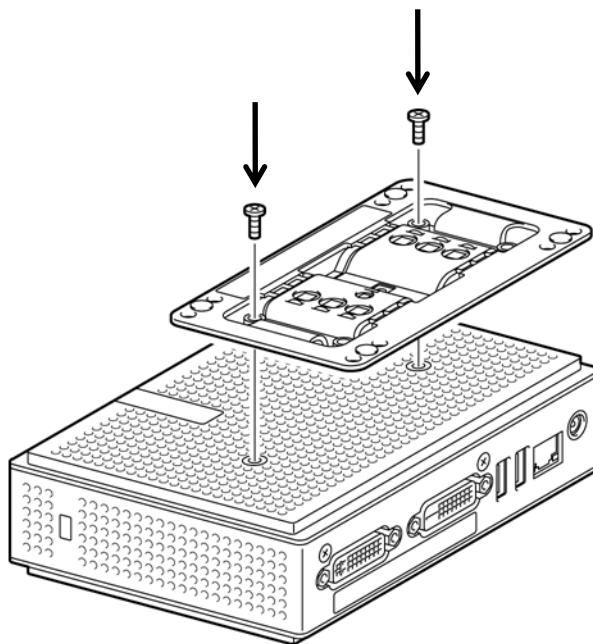
- Use only one type of screw (long or short).
- Select screws having a length appropriate to your monitor according to the instruction manual that comes with your monitor.
- If it is hard to remove the screw, push the screw up from the hole underneath by using a thin screwdriver.



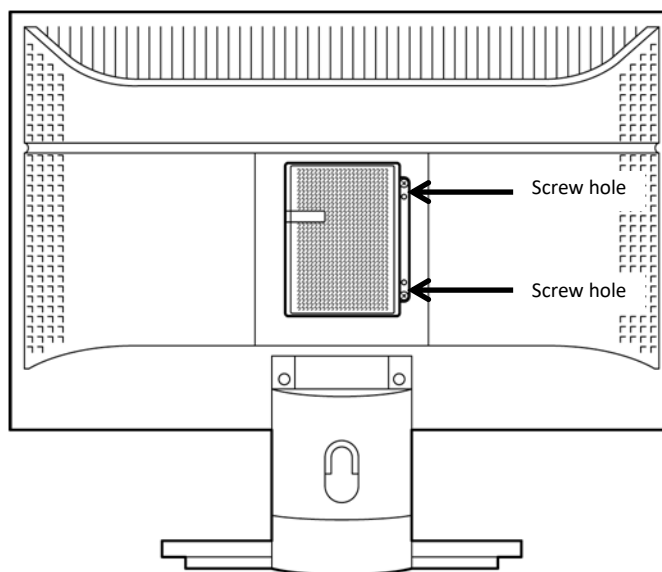
- If the screwdriver is too thin (or too thick) for the screw, the screw thread may be damaged. Use the proper screwdriver.



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**

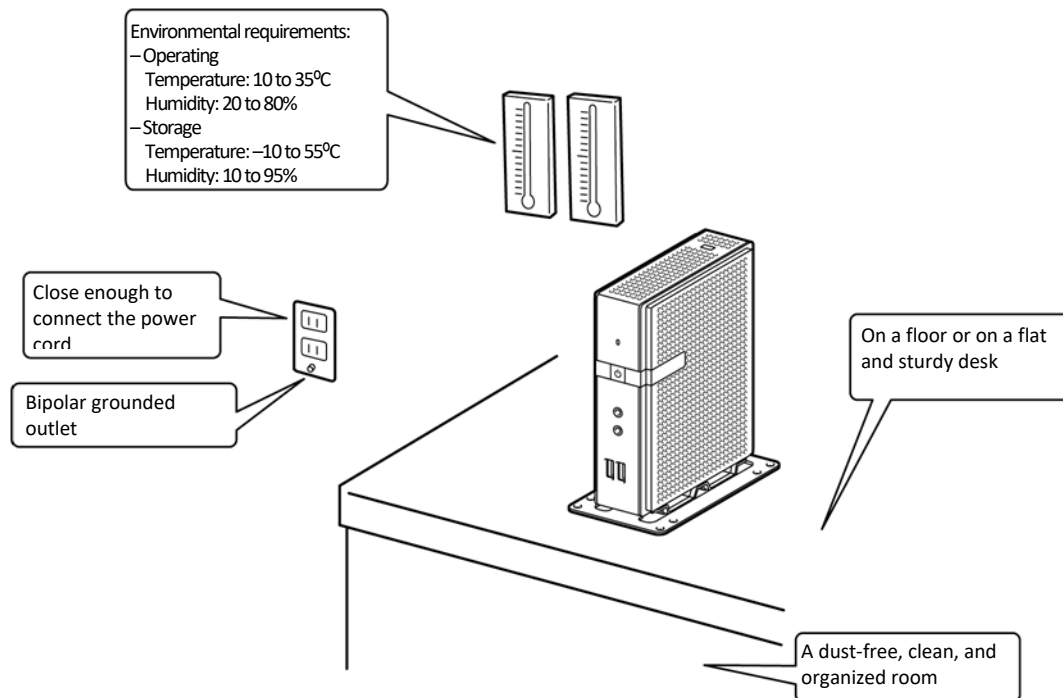
- Do not use US310e with the stand being removed.
- Do not change combination of US310e and the stand.

**⚠ 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.**



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 (for example, 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*.

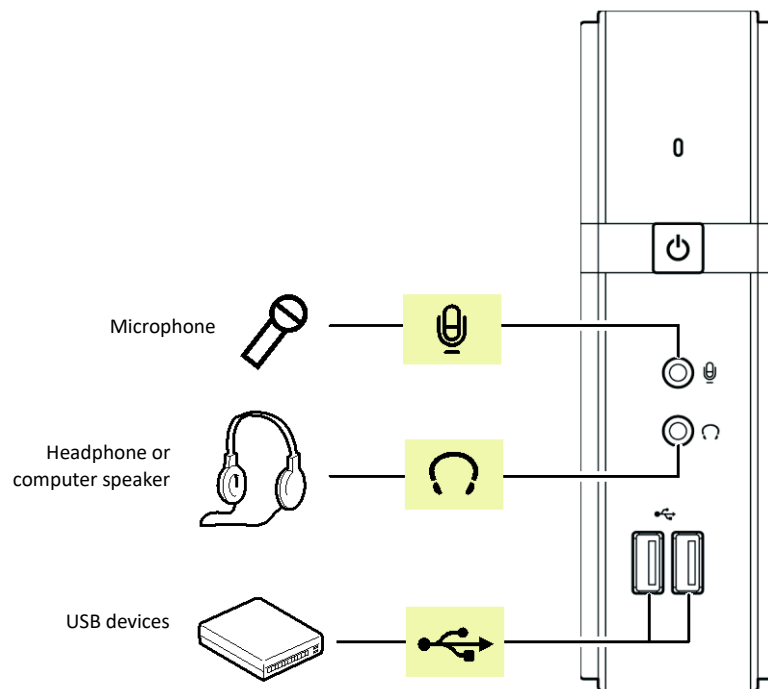
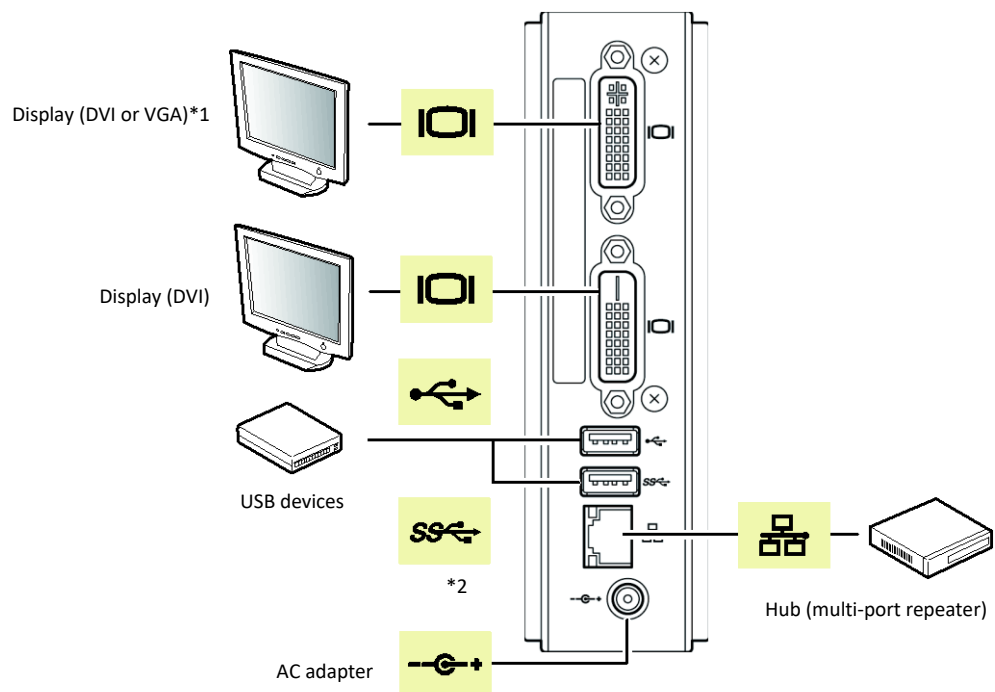
- Plug into a proper power source of the specified voltage.
- Do not connect exceeding number of power cords to a power outlet to prevent excessive electrical load.
- Do not use US310e with any loose interface connection.
- Use the authorized power cord only.
- Do not connect any interface cable with 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****Rear view**

\*1 Use the supplied DVI-VGA adapter to connect a display that uses a VGA interface.

\*2 The USB 3.0 port is disabled by the factory default settings.

---

## 4. Setting up the System BIOS

---

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

Read this section before installing 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

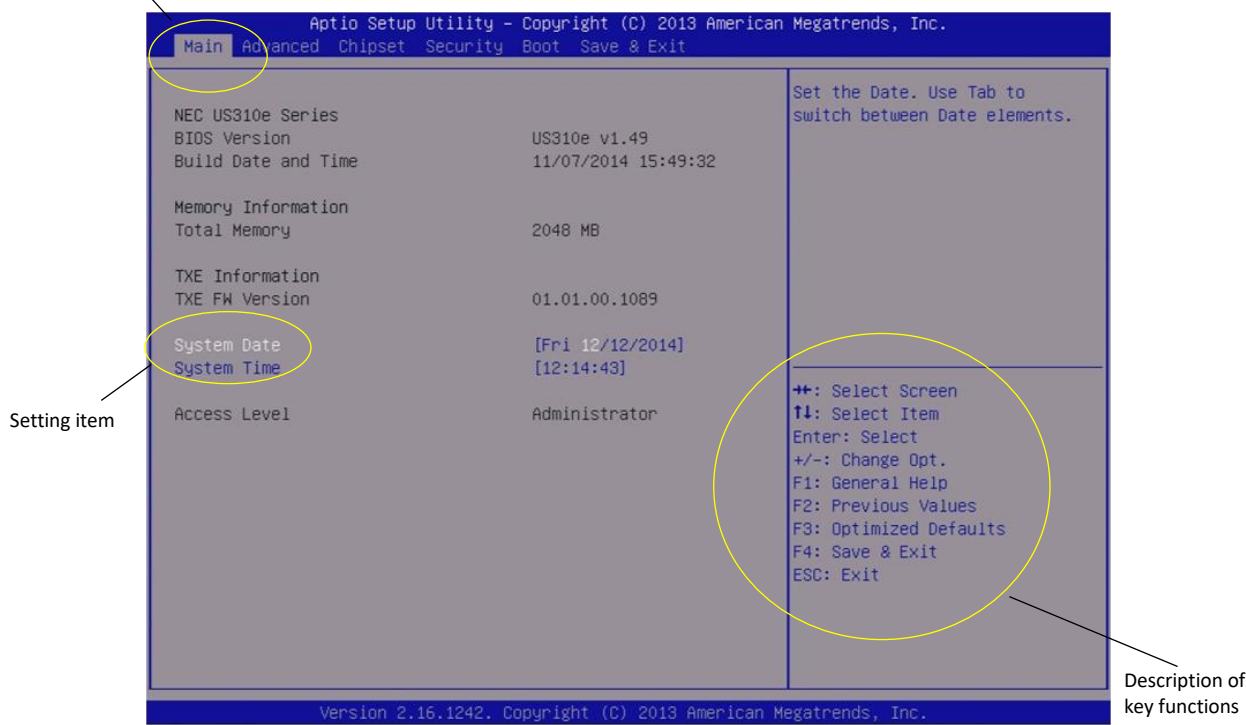
---

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



Cursor keys (←, →)	Used to select the <b>Main</b> , <b>Advanced</b> , <b>Chipset</b> , <b>Security</b> , <b>Boot</b> , or <b>Save &amp; Exit</b> 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 <b>Save &amp; Exit</b> 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.



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

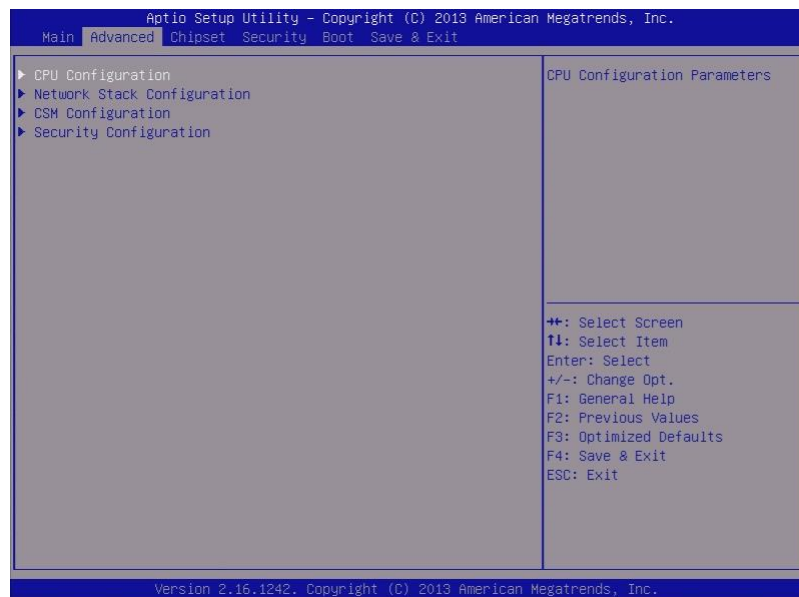
Check the system clock about once a month.

- 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.



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

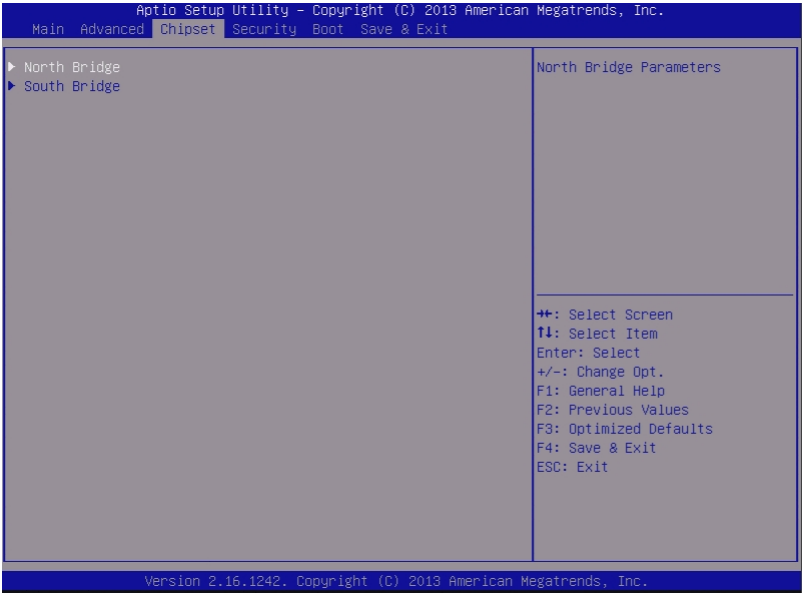
Item	Parameter	Description
CPU Configuration / Power Technology	Disable [Energy Efficient]	Do not change this setting.
Network Stack Configuration / Network Stack	[Disable] Enable	Do not change this setting.
CSM Configuration / Boot option filter	[UEFI and Legacy] Legacy only UEFI only	Do not change 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 HMRFP0	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.



4.4.4 Intel IGD Configuration

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



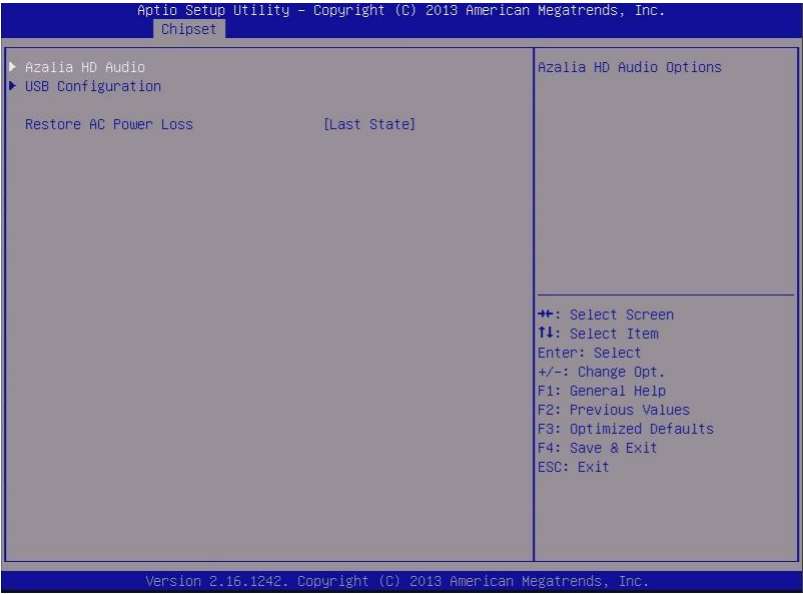
See the table below for each item.

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.



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 <b>XHCI</b> is selected for <b>USB Configuration</b> or <b>USB Mode</b> . 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.



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:



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.



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 <b>F4</b> 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 <b>F2</b> 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 <b>F3</b> key.)
Boot Override	Do not select this item.

---

## Chapter 2 Before Getting Started

Read this section before starting work on US310e.

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

Describes UWF (Unified Writer Filter).

**2. Default User Accounts**

Describes the default user accounts.

**3. the Behavior of System Startup**

Describes the behavior of system startup.

**4. Standard / Customized Desktop Shortcuts**

Describes the standard and customized desktop shortcuts.

**5. Connecting to a Printer**

Describes how to connect US310e to a printer.

**6. Connecting to a Monitor**

Describes how to connect US310e to a monitor.

---

# 1. 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. 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.

### <<< IMPORTANT NOTICE >>>

Using a network controllable product with its default password may raise a serious risk as it may be hacked by some malicious third person. If a product is supplanted by a malware, it will face possibilities of not only information leakages, but also system damages obstructing its availability and/or integrity. Even if it does not cause damage to own system, the product may be used as a botnet to make a cyber-attack to some other systems.

The default password on our product is provided only for the purpose of changing initial setting during its installation service. In first change of initial setting, please be sure to change the password. NEC shall not take any liability and responsibility for any damages arising from illegal access.

If the new password is not strong (too short) or easily guessed (such as "123456789", "abcdefg", "password", "Administrator"), illegal access cannot be prevented. Please be sure to use a strong password (use 8 digits or longer, and including numerals, capital letters and small letters).

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

---

## 3. 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.

---

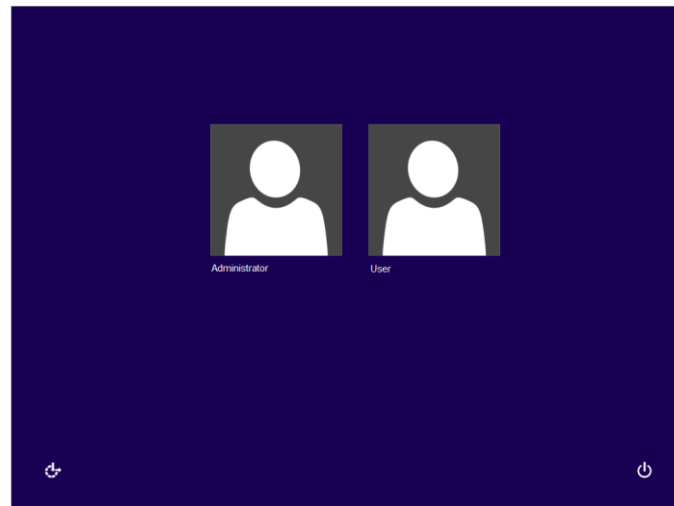
### 3.1 Switching the Sign-In User

---

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

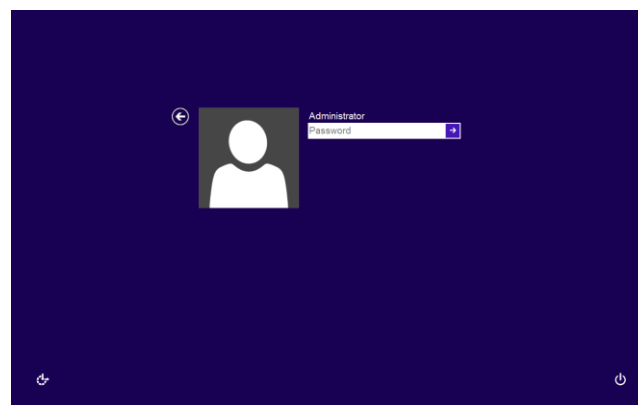
1. Sign in automatically by default user account.
2. Press and hold the **Shift** key on the keyboard until the screen to select the sign-in user appears.

3. 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.

4. Select the user account to sign in with, enter your password, and then click **OK**.



---

## 4. Standard / Customized Desktop Shortcuts

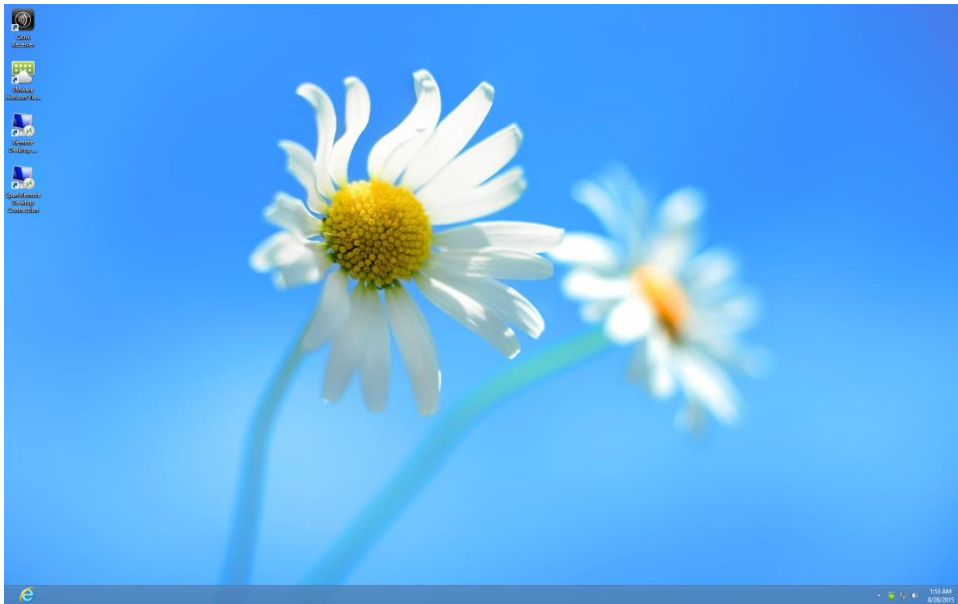
---

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.

---

---

## **Chapter 3 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.

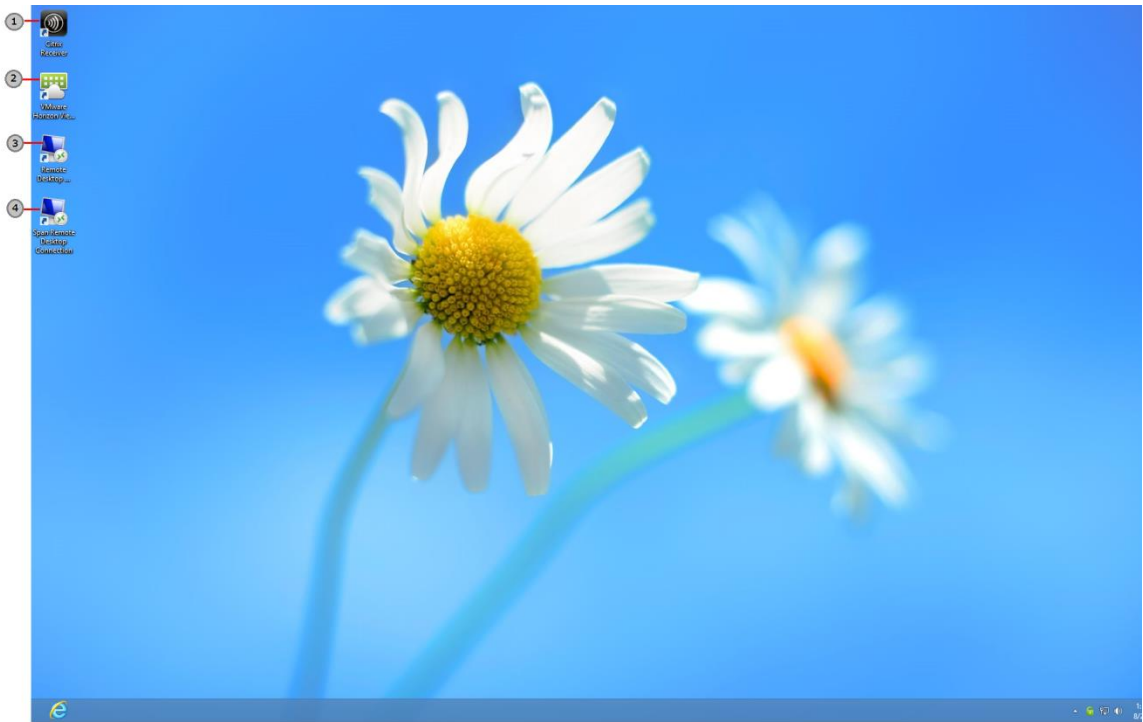
**6. Browsing the Internet by Using Internet Explorer**

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.
4	Remote Desktop Connection (Span mode)	Double click to access Microsoft Remote Desktop services in the span mode.

**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

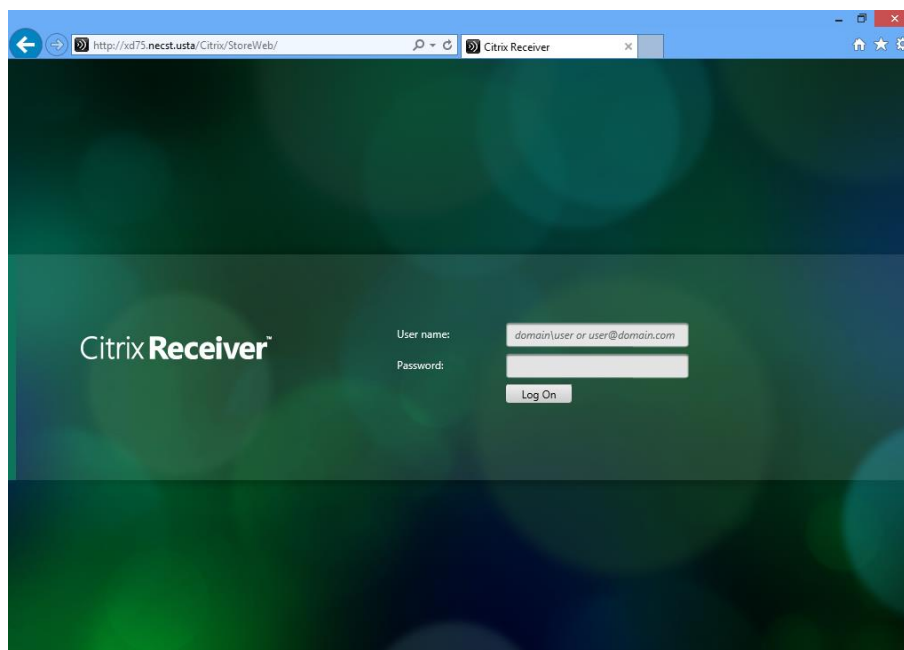
---

### 2.1 Accessing Citrix Service with Internet Explorer

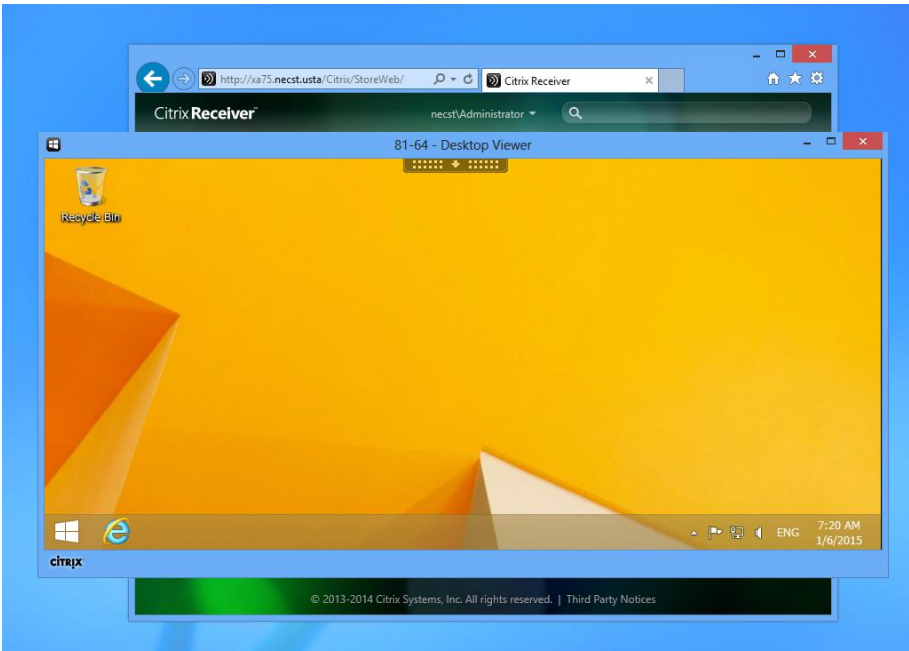
---

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

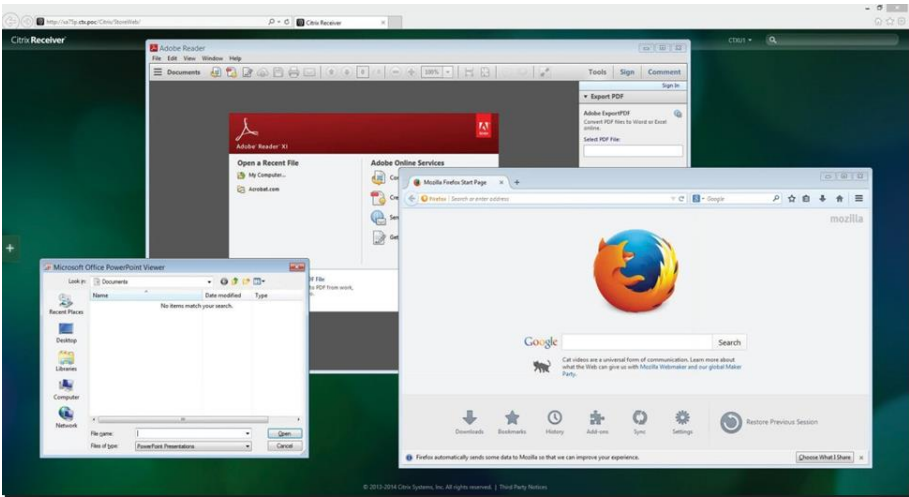
1. Open the Internet Explorer by clicking its icon on the Start screen or the desktop taskbar.
2. Enter the IP address / URL / FQDN of the server through which Citrix services are accessible.
3. Follow the on-line instructions to provide the required data and access Citrix services.



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

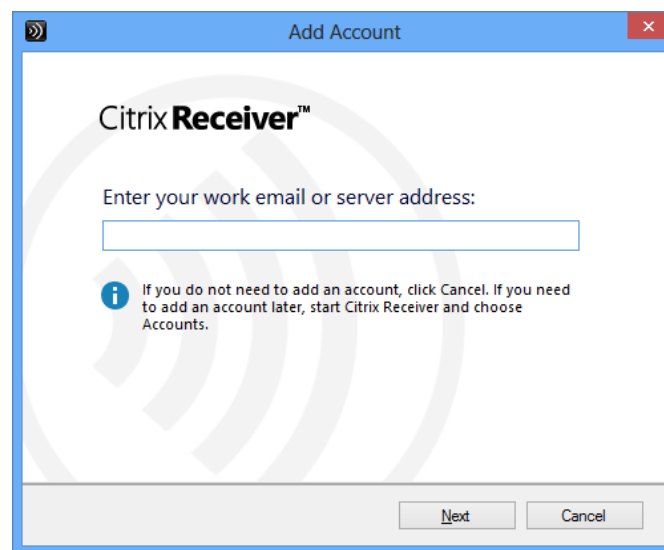
To access Citrix services through the Citrix Receiver shortcut, do the following:

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.

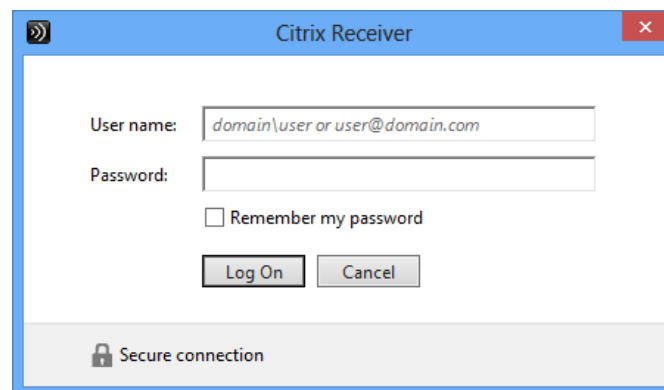
**Note**

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.



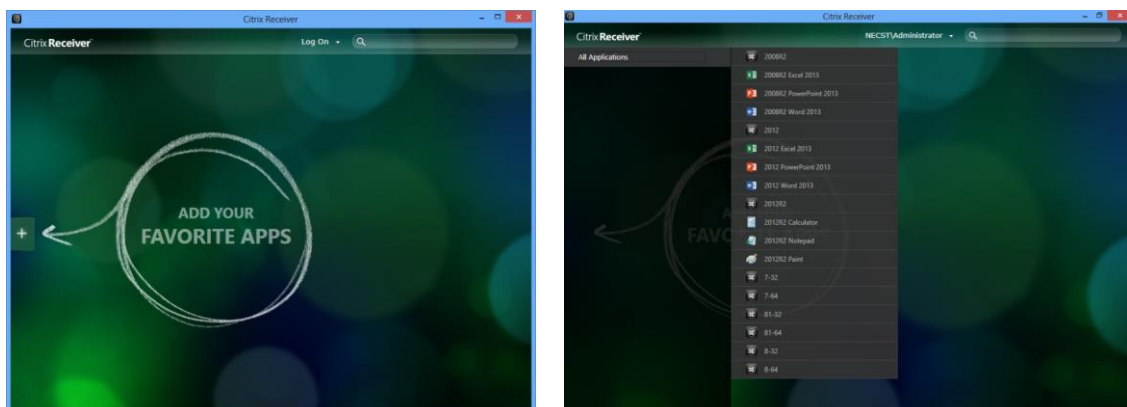
5. Click **Yes** to optimize your Citrix access.



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

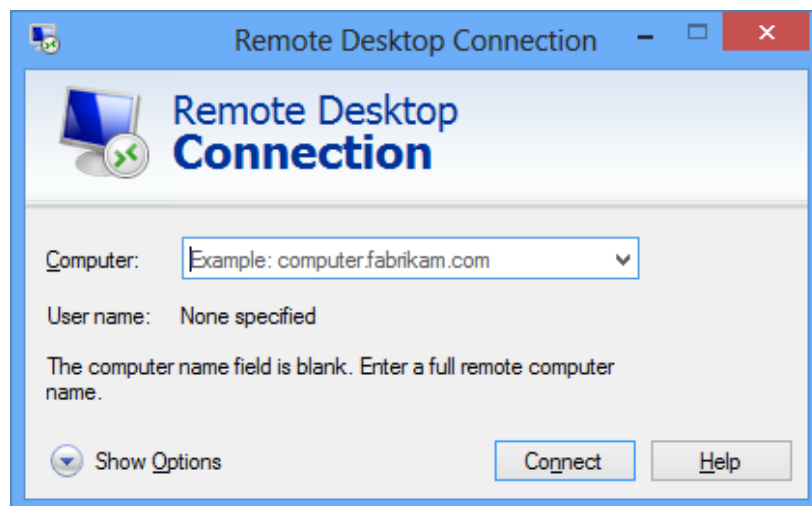
---

### 3.1 Accessing Microsoft Remote Desktop Services by Using Remote Desktop Connection

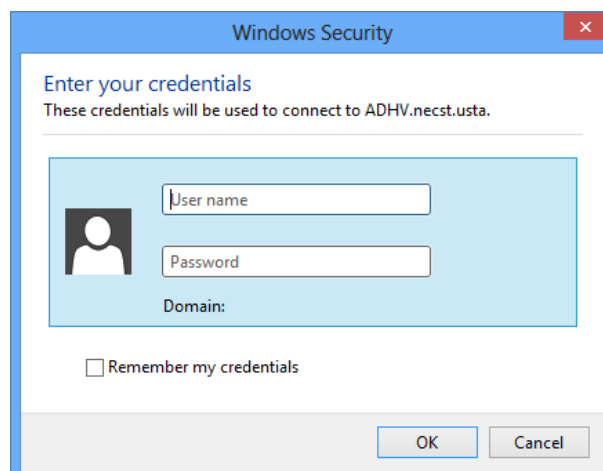
---

To access Remote Desktop services, do the following:

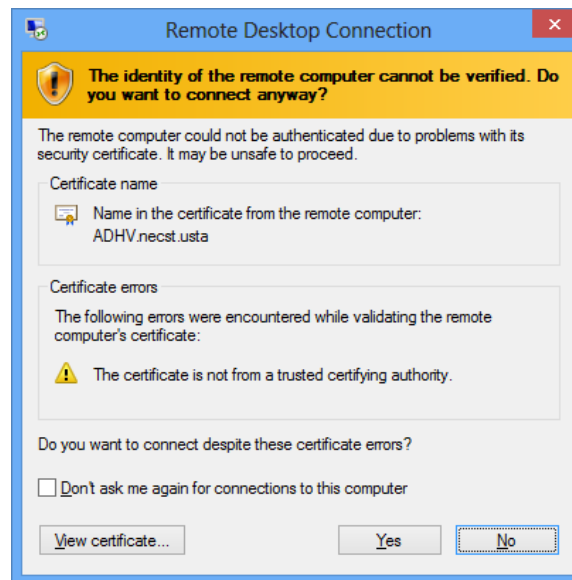
1. Double click **Remote Desktop Connection** on the desktop.
2. Enter the name or IP address of the remote computer on the Remote Desktop Connection window, and then click **Connect**.



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

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

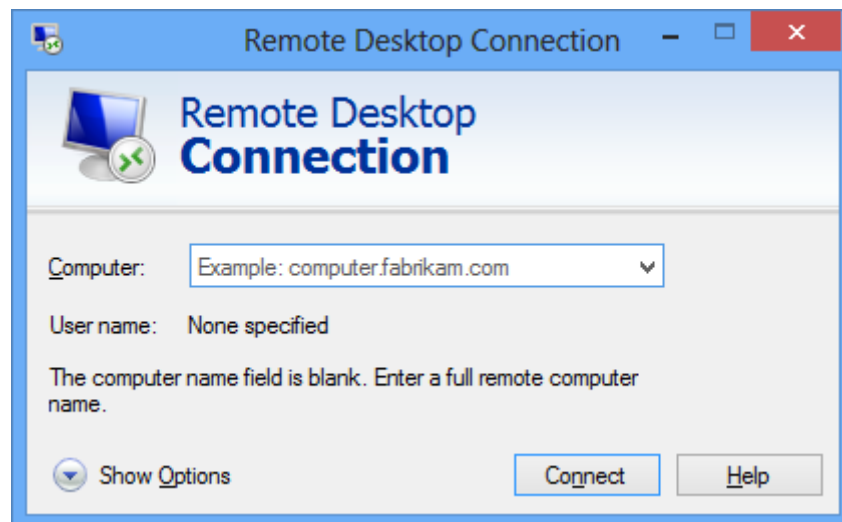
**Note**

To establish a connection in the span mode, connect the primary and secondary monitors to US310e. In addition, open Control Panel and click **Display** -> **Change the appearance of your display** to properly configure your display settings. (For details, see documentation available from Microsoft at <http://www.microsoft.com>.)

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

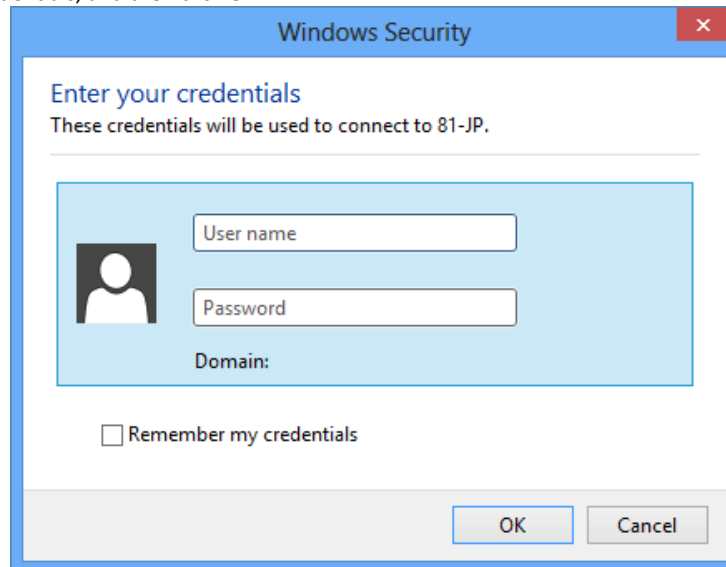
**Note**

If you select **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).

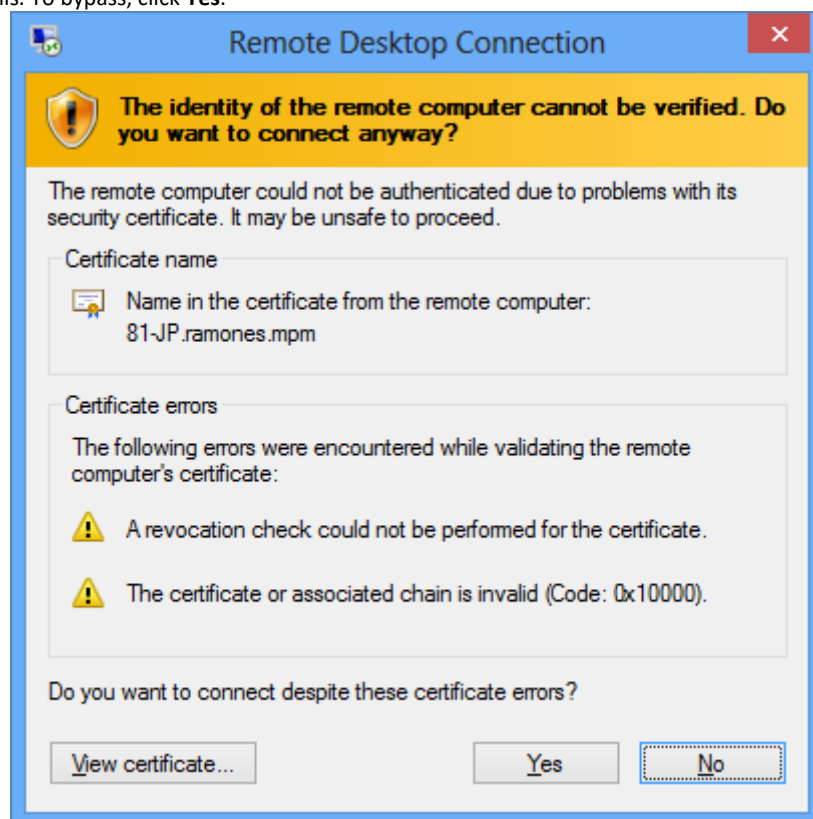




3. Enter your credentials, and then click **OK**.



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



5. US310e is connected to the remote desktop, and the virtual desktop will be displayed on the screen.
6. After logging on to the virtual desktop, check that US310e is connected in the span mode.
- \* When US310e is connected to the remote desktop in the span mode, applications such as NotePad are displayed across two screens when maximized.

## 3.3 Accessing Remote Desktop Services by Using RemoteApp and Desktop Connection

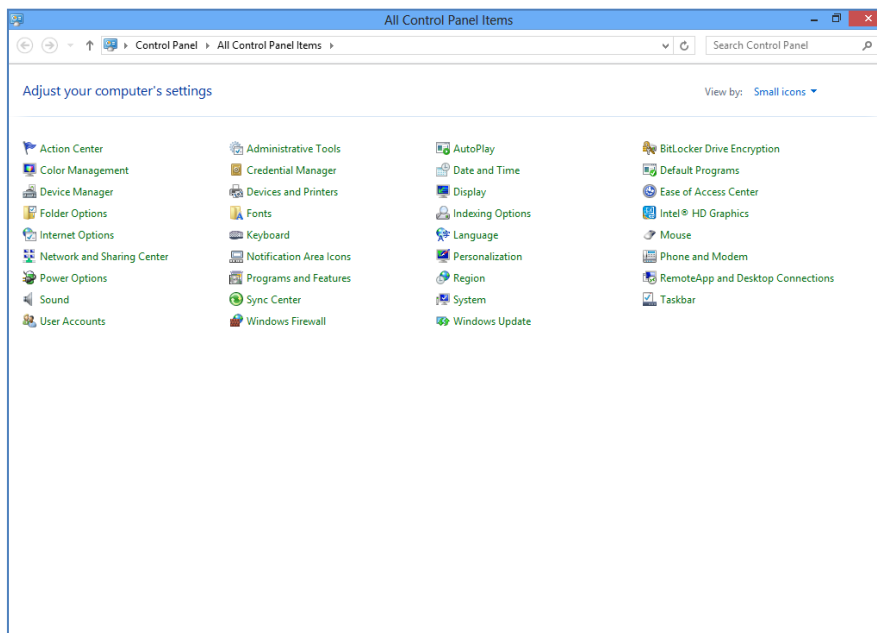
Access Remote Desktop services by using RemoteApp and Desktop Connection as follows:

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

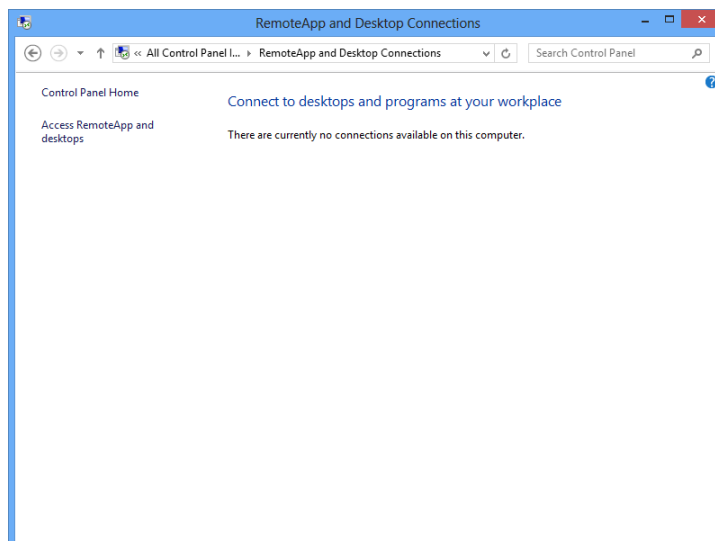
### Note

For how to import a certificate, see Chapter 5, "16. Saving the Certificate".

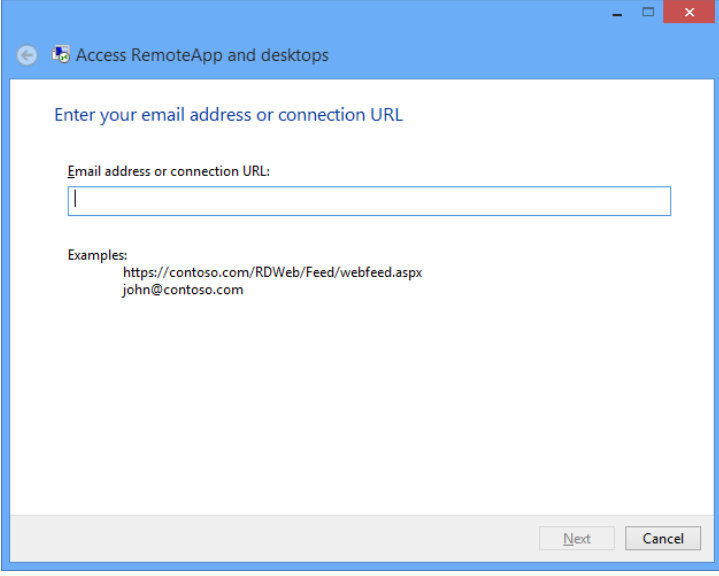
2. On your desktop, move the mouse pointer to the bottom-left corner, and right-click **Start** to open the popup menu.
3. Click **Control Panel**.
4. Select **RemoteApp and Desktop Connections**.



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.



Access RemoteApp and desktops

Enter your email address or connection URL

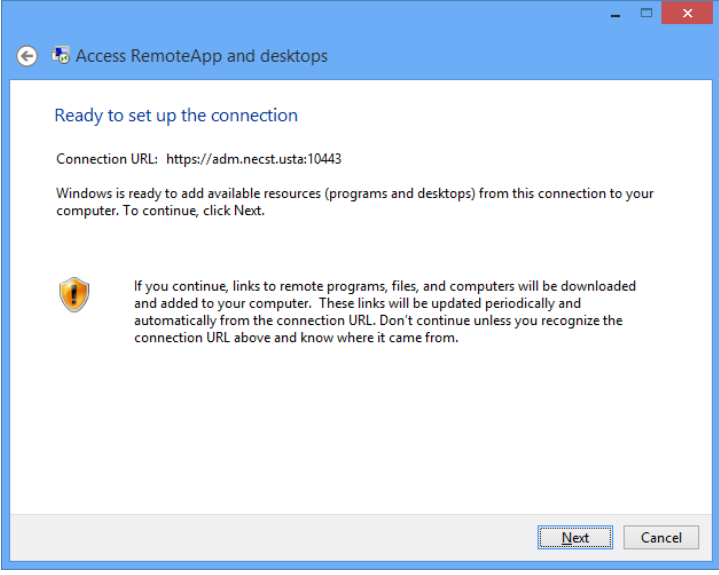
Email address or connection URL:

Examples:

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

Next Cancel

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



Access RemoteApp and desktops

Ready to set up the connection

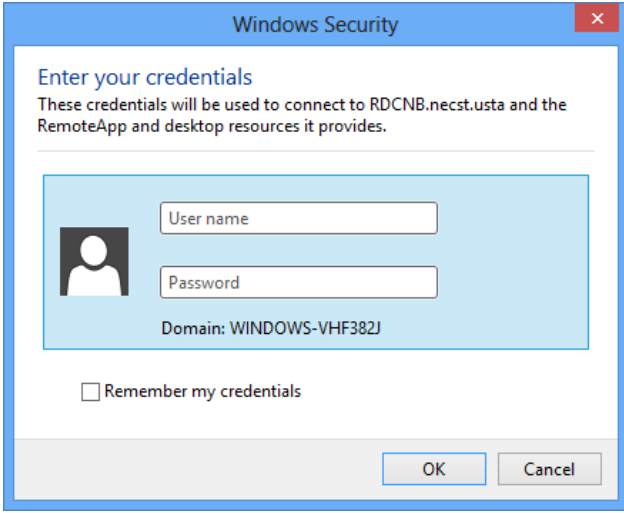
Connection URL: https://adm.necst.usta:10443

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

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

Next Cancel

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



Windows Security

Enter your credentials

These credentials will be used to connect to RDCNB.necst.usta and the RemoteApp and desktop resources it provides.

User name

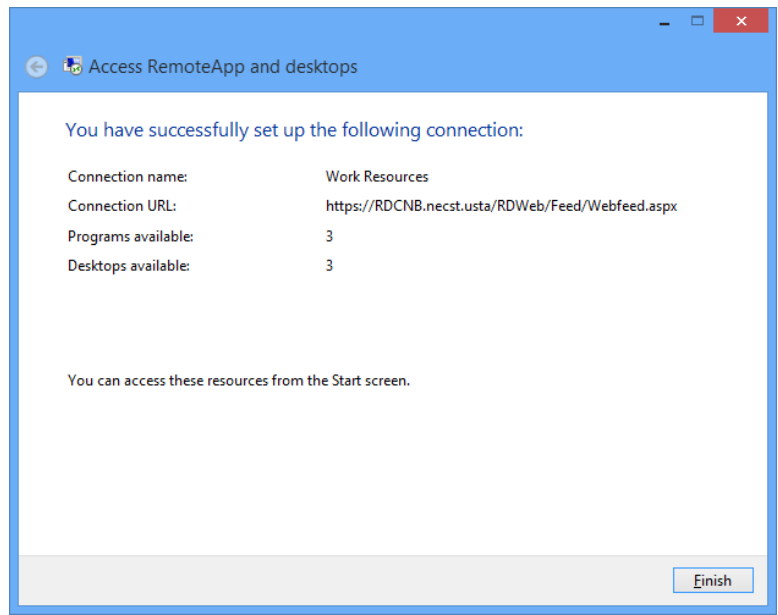
Password

Domain: WINDOWS-VHF382J

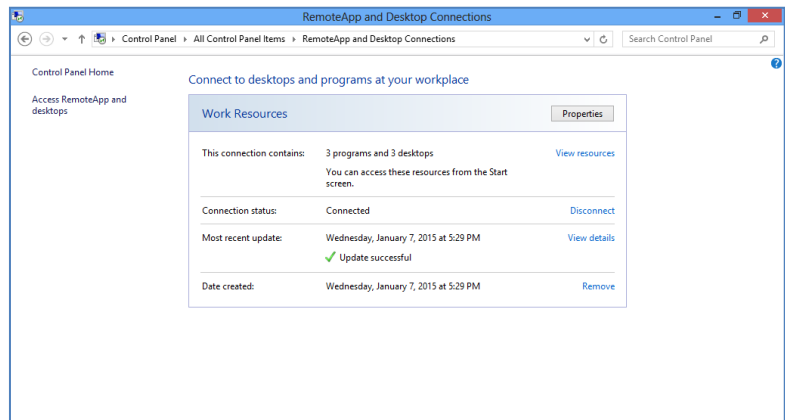
☐ Remember my credentials

OK Cancel

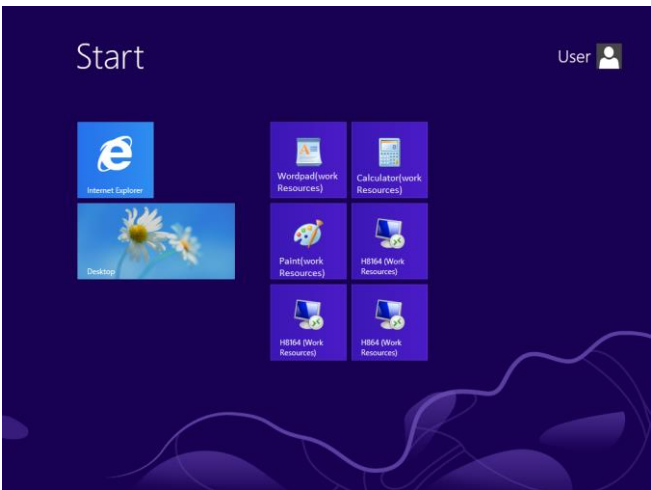
9. A window indicating that connection is properly set up appears. Click **Finish**.



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.

## 3.4 Accessing Remote Desktop Services by Using Internet Explorer

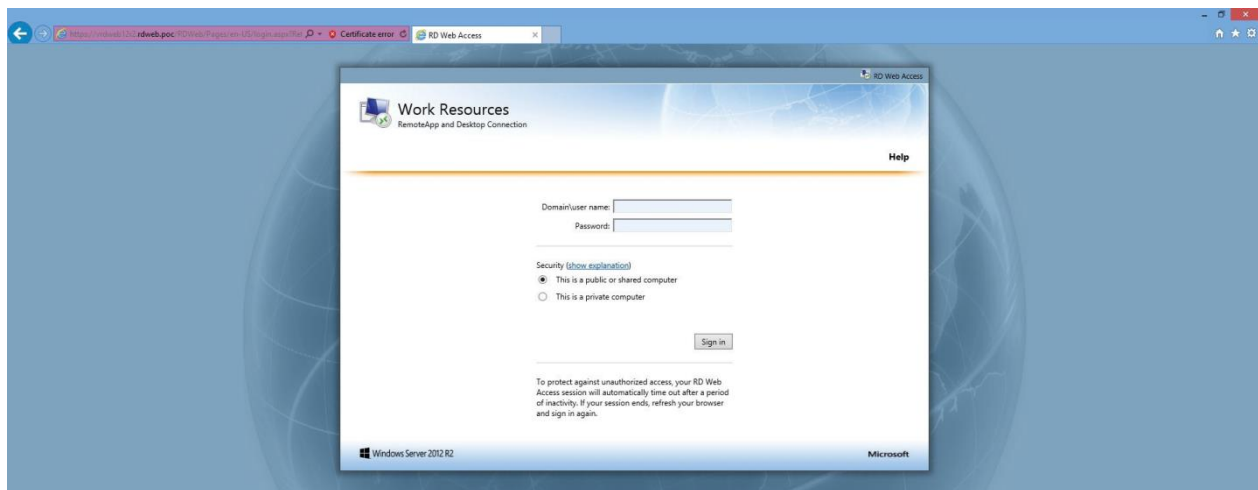
Access Remote Desktop services by using Internet Explorer as follows:

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

### Note

For how to import a certificate, see Chapter 5, "16. Saving the Certificate".

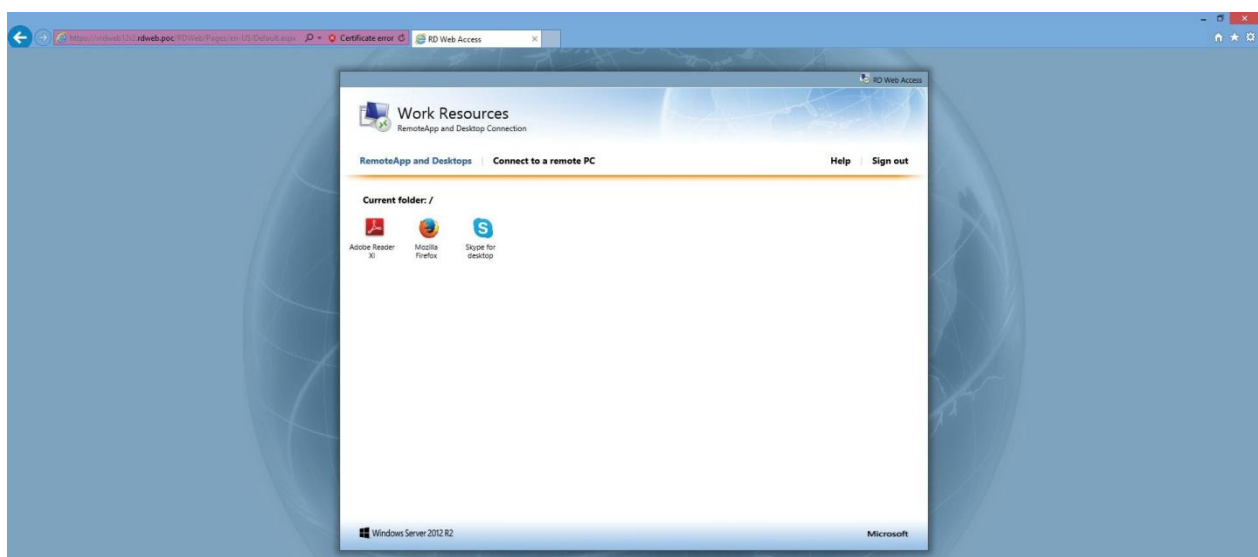
2. Click the Internet Explorer icon on the **Start** screen or taskbar on your desktop to launch Internet Explorer.
3. Enter the IP address, URL, or FQDN of the server through which Remote Desktop Services will be accessed.
4. Enter your credentials, and then click **Sign in**.



### 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)

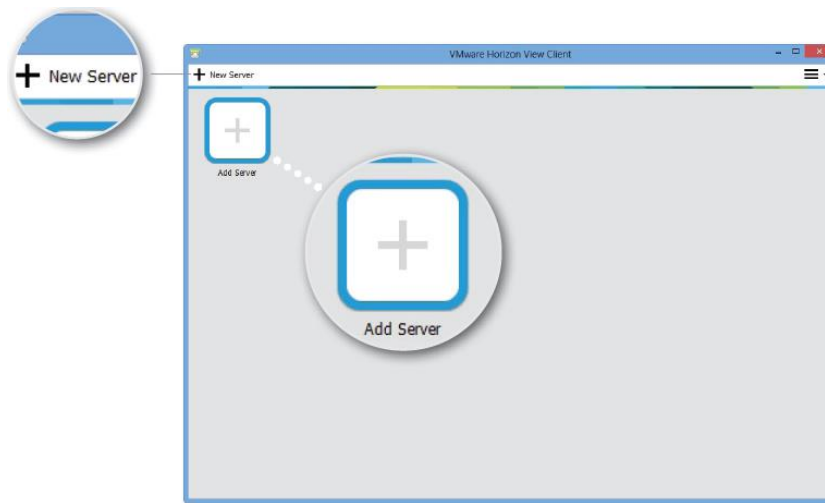
### Note

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.

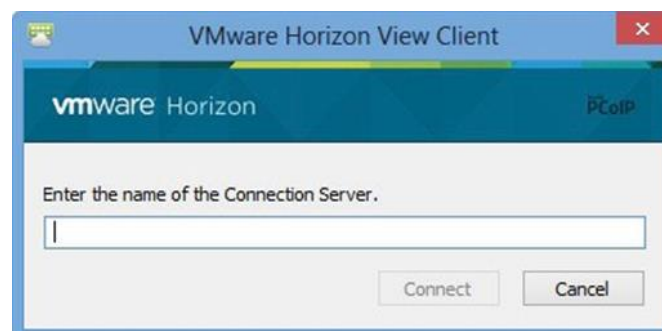
### 4.1 Accessing VMware View and Horizon View Services by Using VMware Horizon View Client

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**.

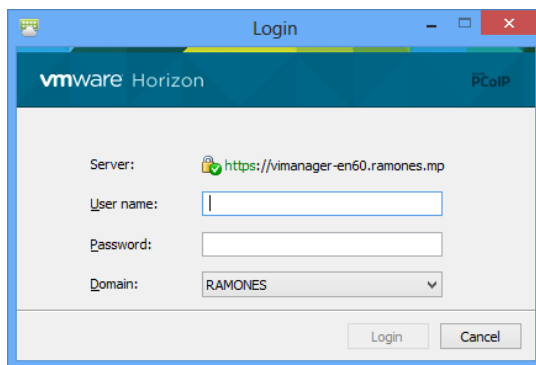


5. By default, a secure connection (HTTPS) is required to connect to the View Connection server. You therefore need to import a certificate.

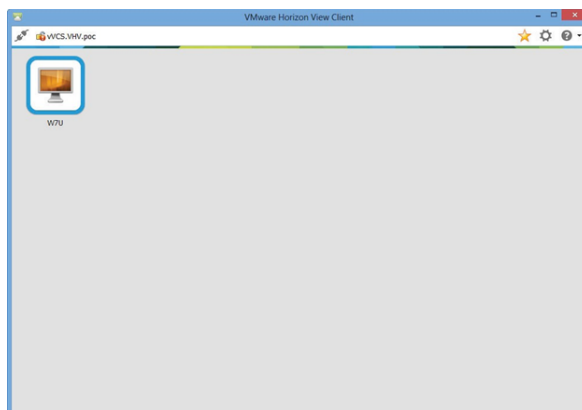
**Note**

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

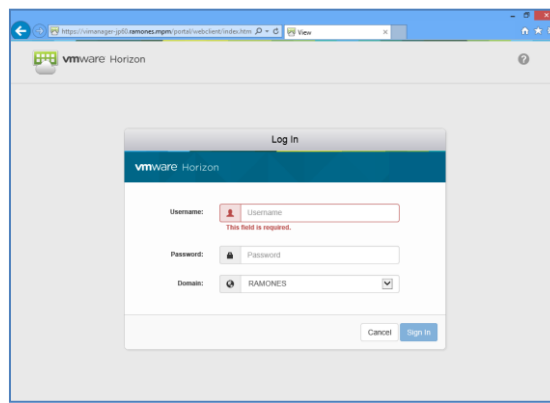
Access VMware View and Horizon View Services by using Internet Explorer as follows:

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.

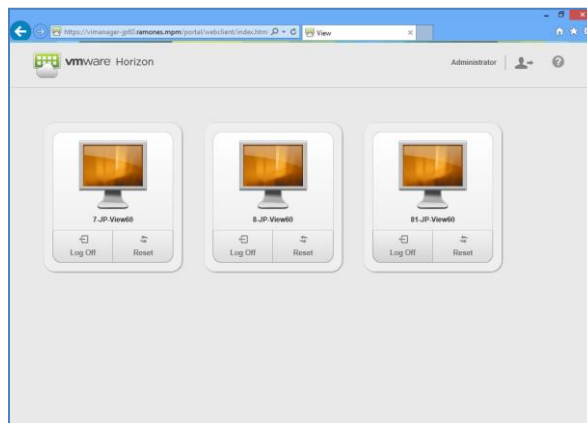
**Note**

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**

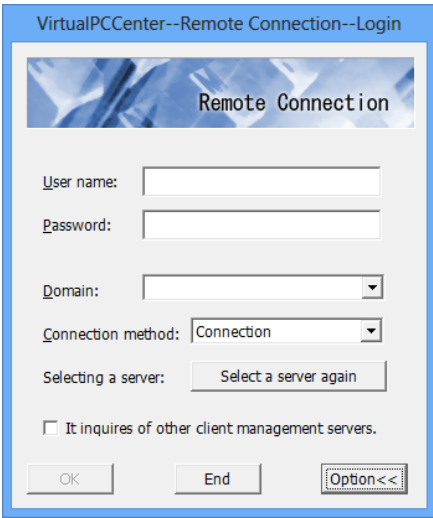
To access NEC Client Management Option (CMO) Services, CMO Terminal Agent must be installed on your US310e (it is not installed by default).

Your US310e contains a CMO Terminal Agent installer. See Chapter 5, "13. Installing CMO Terminal Agent" for how to install this software.

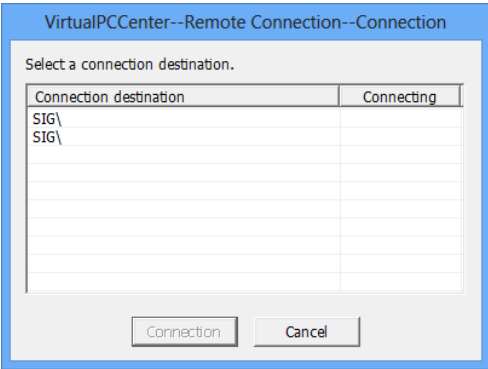
## 5.1 Accessing NEC Client Management Option (CMO) Services by Using CMO Terminal Agent

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

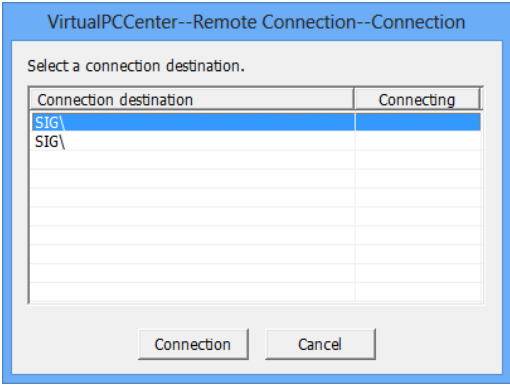
1. On your desktop, double-click the **Remote Connection** icon.
2. Enter your credentials, and then click **OK**.



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**.



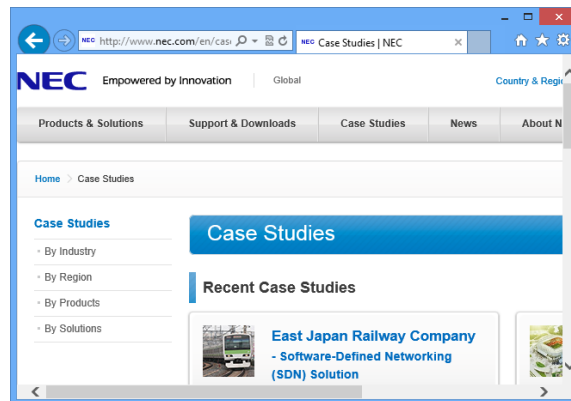
- 5. The client is connected to the selected virtual desktop.

---

## 6. 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

---

## Chapter 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

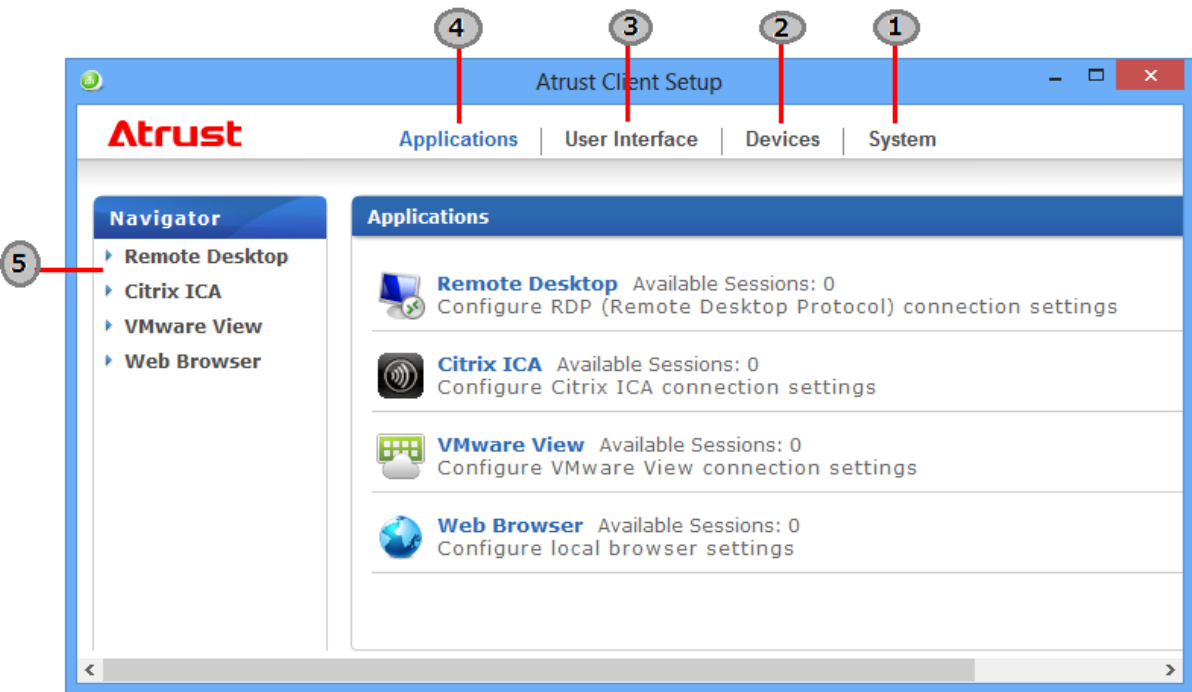
Describes how to configure service access settings using Atrust Client Setup.

# 1. Atrust Client Setup (ACS)

## 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. 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

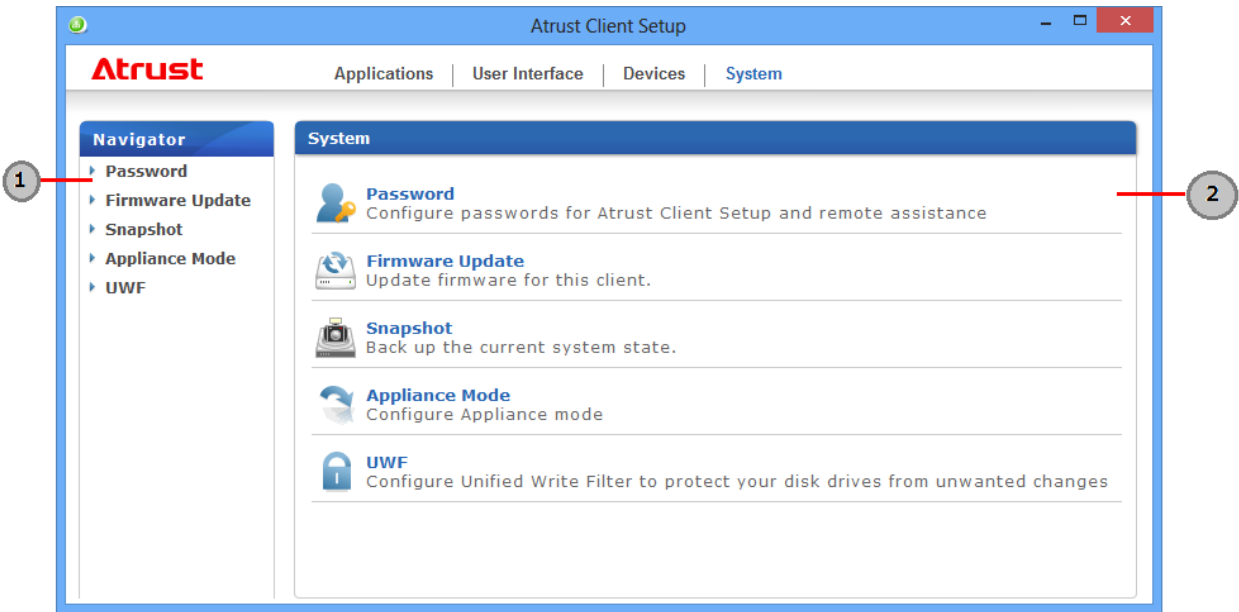
The following table provides a brief description of each setting item under four main setting categories.

Tab	Setting item	Section page
<b>System</b>	<ul style="list-style-type: none"> <li>• Configuring whether a password is required to access Atrust Client Setup and setting a password</li> <li>• Enabling/disabling remote assistance and setting a password</li> <li>• Updating firmware</li> <li>• Taking snapshots</li> <li>• Enabling/disabling the Appliance mode</li> <li>• Configuring UWF (Unified Writer Filter)</li> </ul>	Chapter 4, "2. Configuring System Settings".
<b>Devices</b>	<ul style="list-style-type: none"> <li>• Configuring settings for USB storage devices</li> <li>• Configuring settings for audio devices</li> </ul>	Chapter 4, "3. Configuring External Device Settings".
<b>User Interface</b>	<ul style="list-style-type: none"> <li>• Configuring whether to display or hide the service access shortcut</li> </ul>	Chapter 4, "4. Configuring User Interface Settings".
<b>Applications</b>	<ul style="list-style-type: none"> <li>• Configuring Microsoft RDP connection settings</li> <li>• Configuring Citrix ICA connection settings</li> <li>• Configuring VMware View connection settings</li> <li>• Configuring Web browser session settings</li> </ul>	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 <b>System</b> tab.
2	Configuration area	Configures setting values when a setting item is selected.

## 2.2 Available Settings

Tab	Setting	Icon	Description	Section page
System	Password		Click to set a password to access Atrust Client Setup. You can enable or disable remote assistance and set a password here.	<ul style="list-style-type: none"> <li>Chapter 4 "2.3. Setting a Password to Access Atrust Client Setup"</li> <li>Chapter 4 "2.4. Configuring Shadow Settings for Remote Assistance"</li> </ul>
	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.	<ul style="list-style-type: none"> <li>Chapter 4, "2.5 Updating Firmware from the Management Computer".</li> </ul>
	Snapshot		Click to take a snapshot (system image) of the client for mass deployment.	<ul style="list-style-type: none"> <li>Chapter 4, "2.6 Taking Snapshots for Mass Deployment".</li> </ul>
	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.	<ul style="list-style-type: none"> <li>Chapter 4, "2.8 Enabling or Disabling the Appliance Mode".</li> </ul>
	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.	<ul style="list-style-type: none"> <li>Chapter 4, "2.9 Configuring UWF (Unified Write Filter)".</li> </ul>

### Note

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



## 2.3 Setting a Password to Access Atrust Client Setup

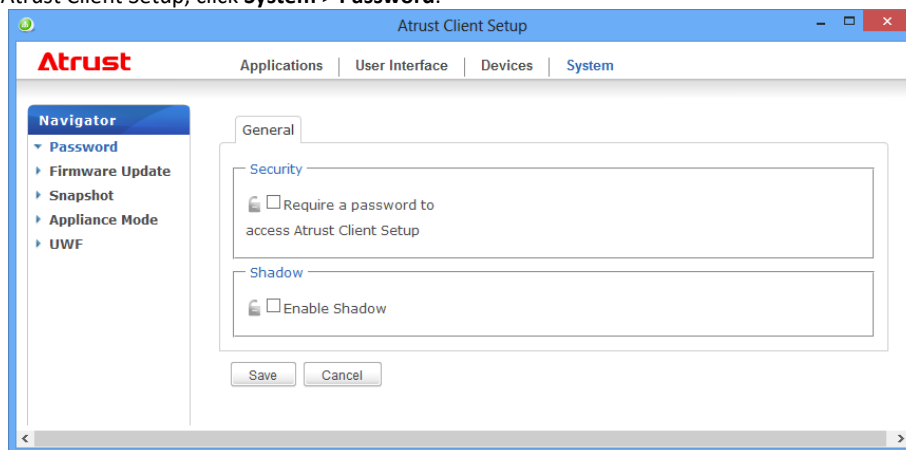
You can set a password to access Atrust Client Setup.

### Note

- Only the system administrator and manager are allowed to access Atrust Client Setup by default. So, if you do not set a password, system administrator privileges are sufficient to access Atrust Client Setup. If you set a password, that password must be entered to launch Atrust Client Setup.
- If a password to access Atrust Client Setup is set, the standard US310e user needs the following two passwords to access Atrust Client Setup: the password for the administrator account in Windows Embedded 8 Standard and the password to access Atrust Client Setup.

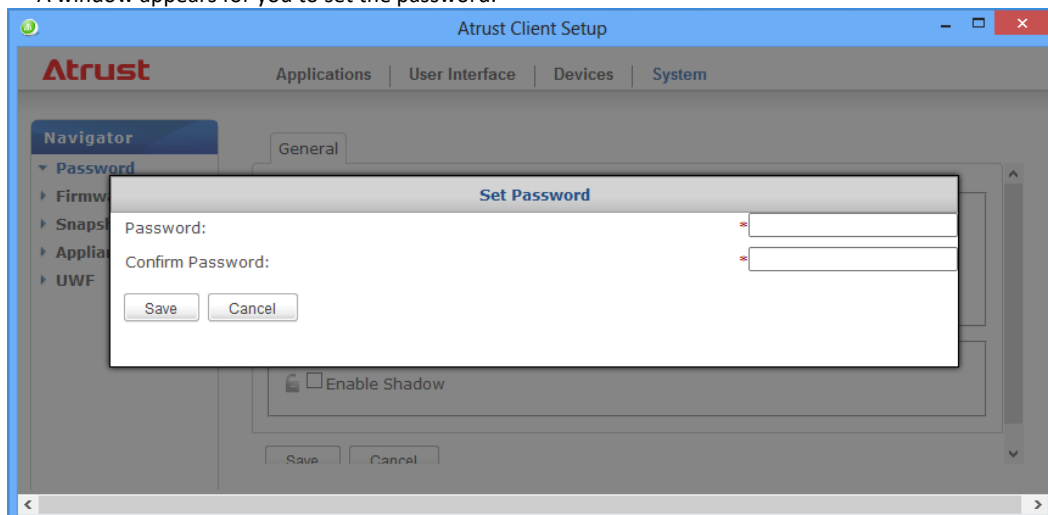
To set a password to access Atrust Client Setup, do the following:

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



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

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



4. Enter an arbitrary password and click **Save** to apply it.
5. Click **Save** to save all the changes.

## 2.4 Configuring Shadow Settings for Remote Assistance

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

### Important

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.

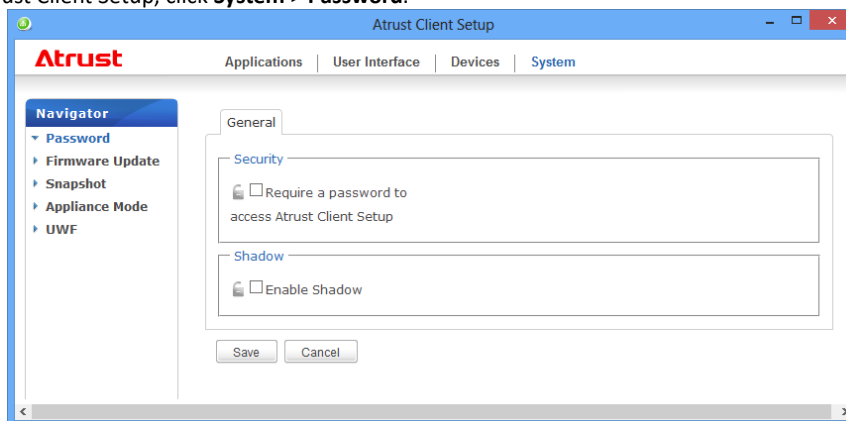
It is therefore important to implement security measures (such as using VNC only within the firewall or disabling VNC when it is not being used) when using this feature.

### 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.

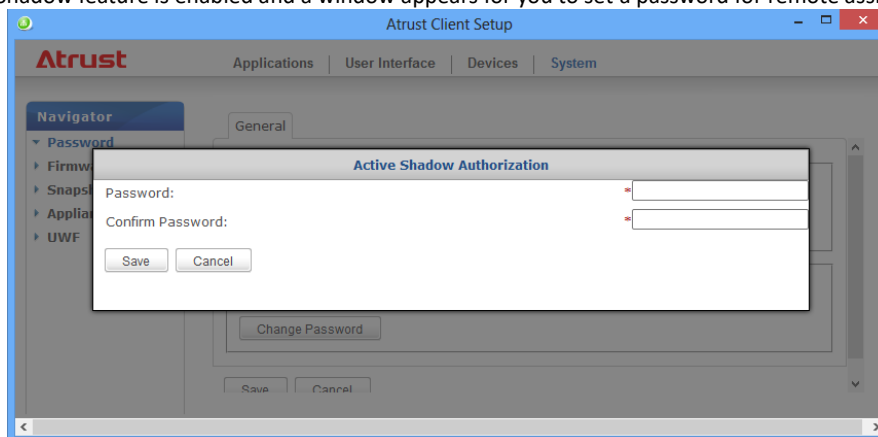
To enable the Shadow feature and set a password for remote assistance, do the following:

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

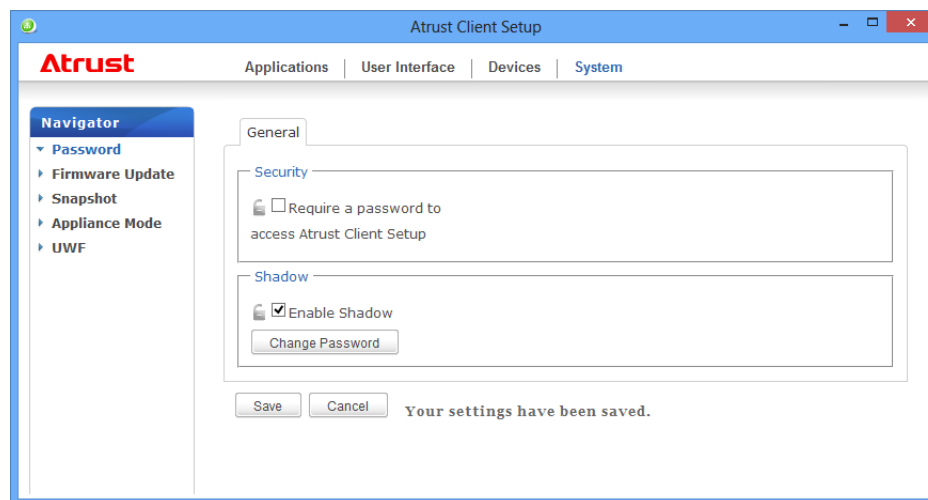




2. Check **Shadow > Enable Shadow**.

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



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

**Note**

When the Shadow feature is enabled, the  icon is displayed on the Notification area of the Taskbar in US310e. When this feature is being executed from the remote computer, the icon color changes to yellow .

## 2.5 Updating Firmware from the Management Computer

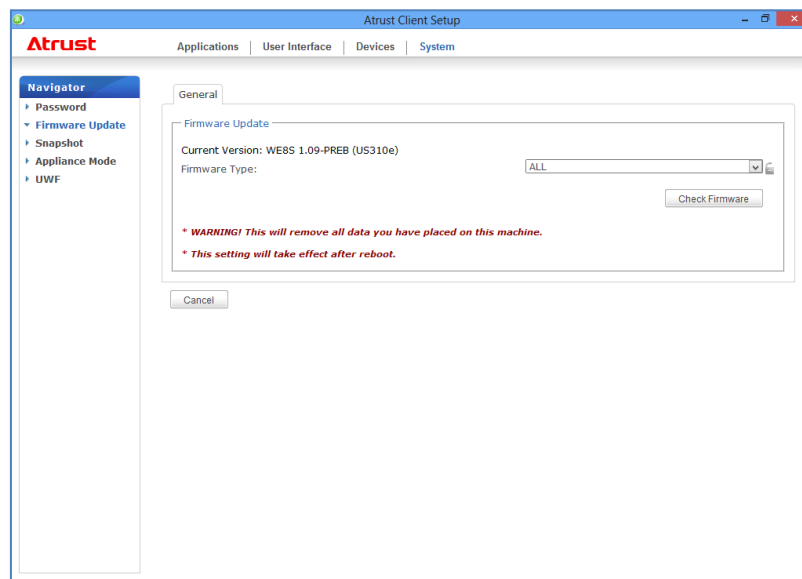
**Update Firmware** allows users to update client firmware from the remote management computer to get the client device up-to-date.

### Note

Ensure that your client has been added into a managed group under Atrust Device Manager installed on a remote computer, and that you have imported client firmware files into Atrust Device Manager. These are prerequisites of this feature.

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

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



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

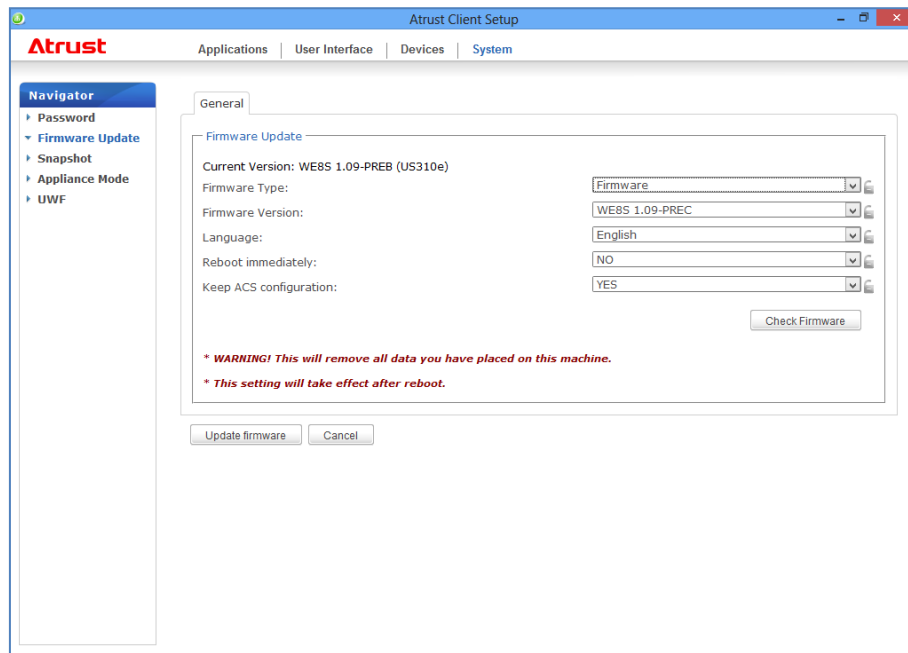
You can also update the firmware of a client with a snapshot (the system image of a client) which is coming from another client of the same model and is with a newer firmware version. For detailed information, see Chapter 4, "2.6 Taking Snapshots for Mass Deployment" about the snapshot.

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.								
	<table><tr><th>Type</th><th>Description</th></tr><tr><td>ALL</td><td>All firmware types, <b>Firmware</b> and <b>Snapshot</b>.</td></tr><tr><td>Firmware</td><td>The system image of a client.</td></tr><tr><td>Snapshot</td><td>The system image of a client coming from another client of the same model.</td></tr></table>	Type	Description	ALL	All firmware types, <b>Firmware</b> and <b>Snapshot</b> .	Firmware	The system image of a client.	Snapshot	The system image of a client coming from another client of the same model.
	Type	Description							
	ALL	All firmware types, <b>Firmware</b> and <b>Snapshot</b> .							
	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.  <b>NOTE:</b> 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.  <b>NOTE:</b> If <b>Yes</b> is selected, all client settings under Atrust Client Setup will remain unchanged after firmware update. If <b>No</b> is selected, all settings will be restored to the factory default.  <b>NOTE:</b> If the client is managed by Atrust Device Manager and here <b>No</b> is selected, Atrust Device Manager will fail to manage the client after firmware update. For more information on Atrust Device Manager, refer to the User's Guide of Atrust Device Manager.								

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

## 2.6 Taking Snapshots for Mass Deployment

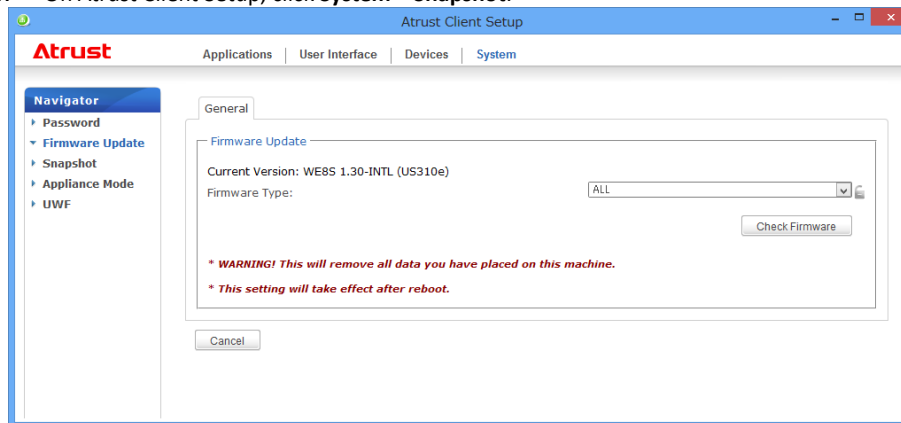
A snapshot is the system image of a client, allowing you to use that image for mass deployment. This system image can be stored on a remote management computer or a locally attached USB flash drive.

### Note

- To store the system image on a remote computer, ensure that Atrust Device Manager has been installed on that computer, and that the client has been added into a managed group under Atrust Device Manager.
- When taking a snapshot, all system specific information, including the Computer Security Identifier (SID) and computer name, will be reset or removed from the system image by performing the System Preparation (Sysprep) tool automatically.
- Taking a snapshot will reset the startup behavior to the default (auto-sign-in with the default standard user account). For details, see Chapter 2, "3. the Behavior of System Startup".

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

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



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

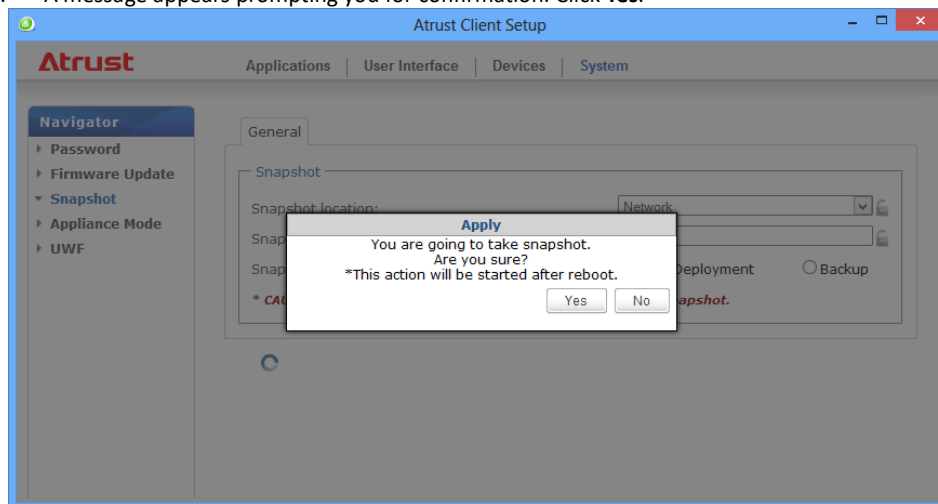
**Note**

- Select **Network** to save the snapshot image on a remote computer.
- Select **USB** to save the snapshot image in a locally connected USB flash memory.

**Important**

- In case of getting snapshot in a USB flash drive on ACS, you need enabling USB flash drives on security options of ACS. After deploying snapshot image, special care must be taken that USB flash devices are enabled because the snapshot image is taken with the state of enabling USB flash devices.

3. Fill in **Snapshot description**.
4. Click **Apply**.
5. A message appears prompting you for confirmation. Click **Yes**.



6. The system automatically restarts to complete the process.

**Note**

Wait until the process is automatically completed. It takes several minutes to create a snapshot and the system restarts several times. The Sysprep process is not displayed on the desktop. It always executes in the background.



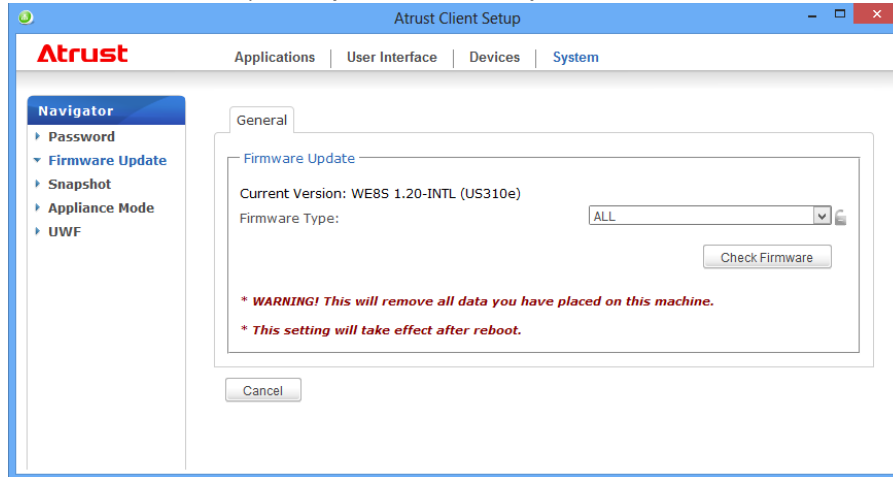
## 2.7 Deploying a System Image Using a Taken Snapshot

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

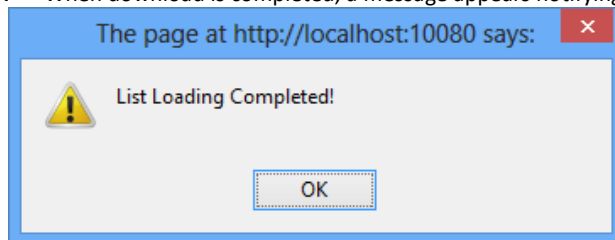
### 2.7.1 Deploying a Snapshot System Image via Network

To deploy a system image to US310e by using a snapshot on a remote computer, do the following:

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



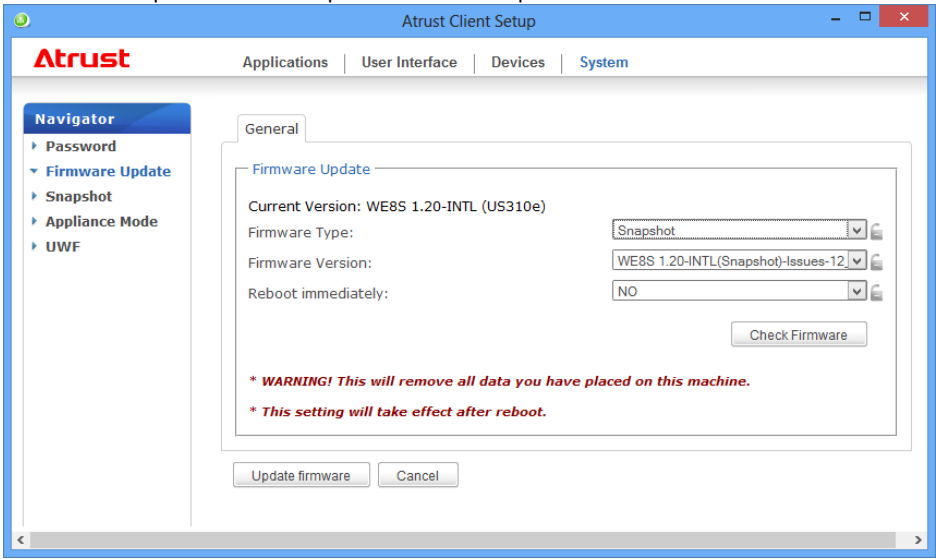
2. Select **Snapshot** from **Firmware Type** in the **Firmware Update** section. A list of snapshots is automatically downloaded from the remote computer.
3. When download is completed, a message appears notifying you that the snapshot list has been loaded. Click **OK**.



#### Note

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

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



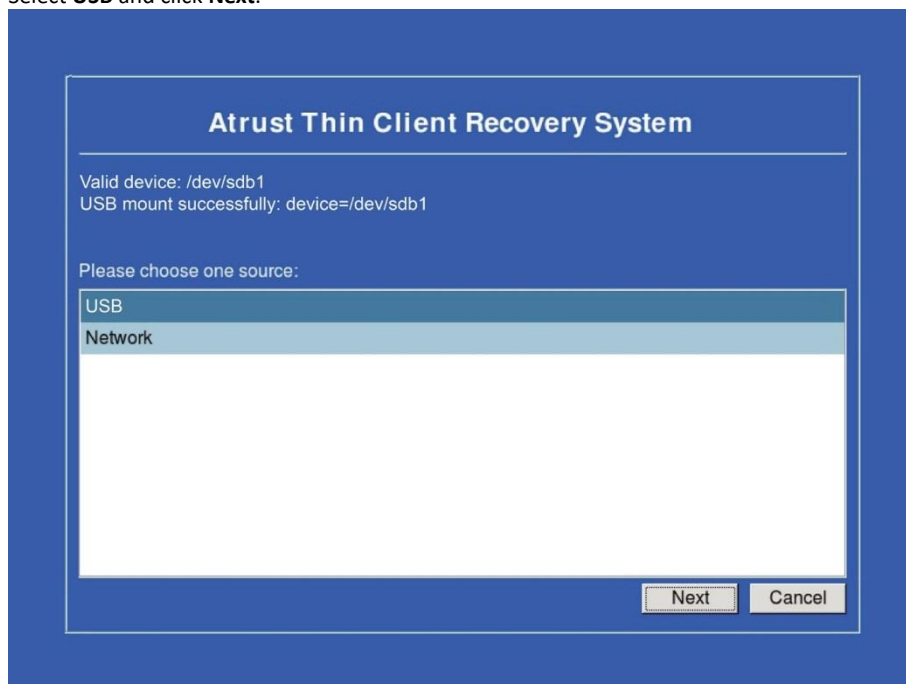
Snapshot deployment options	
Item	Description
Firmware Version	Select a snapshot from the snapshot list.
Reboot immediately	Select whether to immediately restart the system or to manually restart the system later to update firmware.

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

### 2.7.2 Deploying a Snapshot System Image from a USB Flash Memory

To deploy a system image to US310e by using a snapshot in the USB flash memory, do the following:

1. Insert the USB flash memory into an empty USB port on the client.
2. Start or restart the client.
3. Press the F7 key on the keyboard during POST (Power-On Self-Test) to open the **Boot Device** menu.
4. Select to boot from the connected USB flash memory.
5. Select **USB** and click **Next**.



6. The recovery system starts deploying the snapshot to the client.
7. When the process is completed, click **Finish** to restart the client.

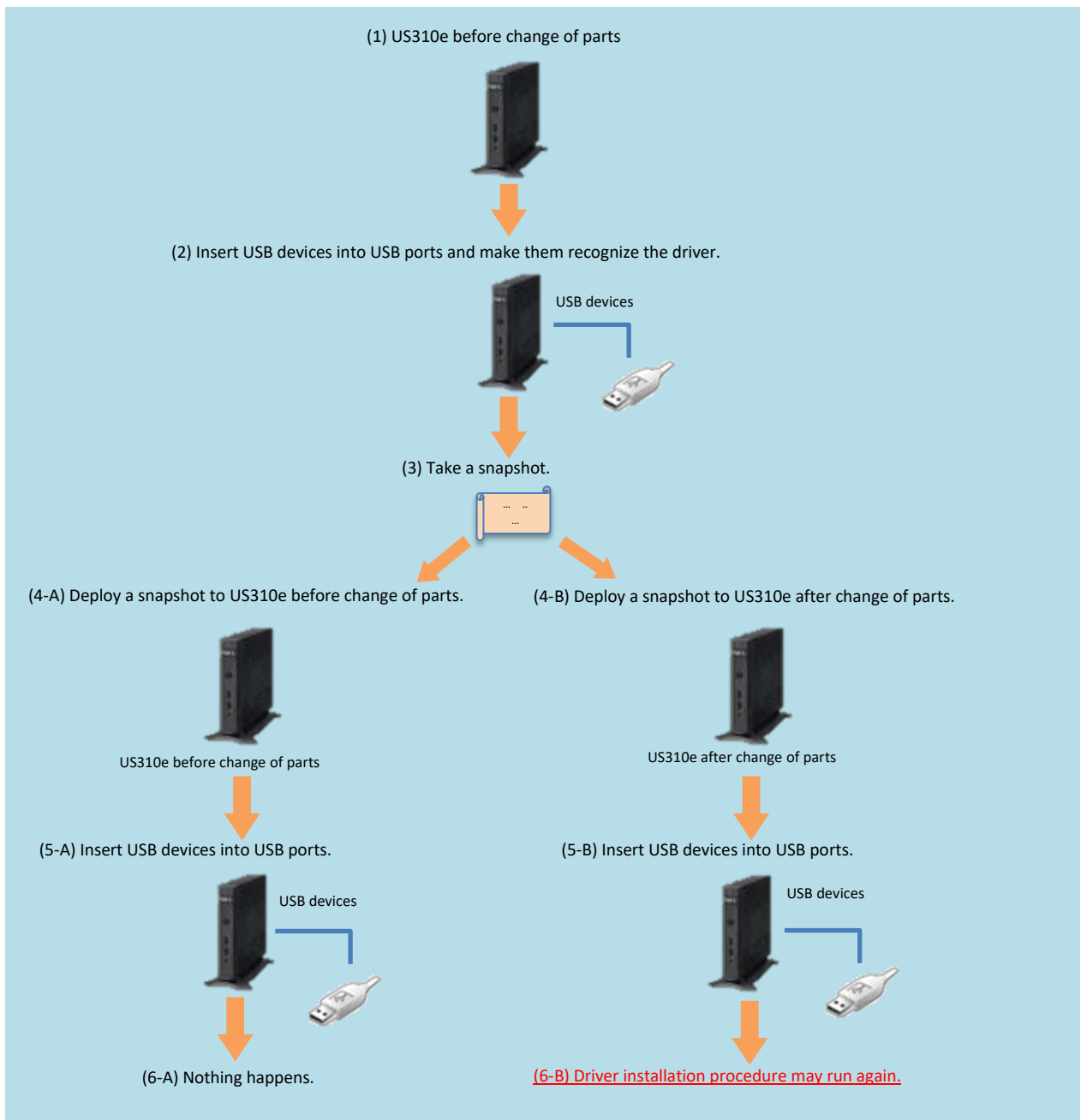
### 2.7.3 About snapshot diversion restriction by change of parts.

Some parts which are used in US310e have been changed because the parts were discontinued.

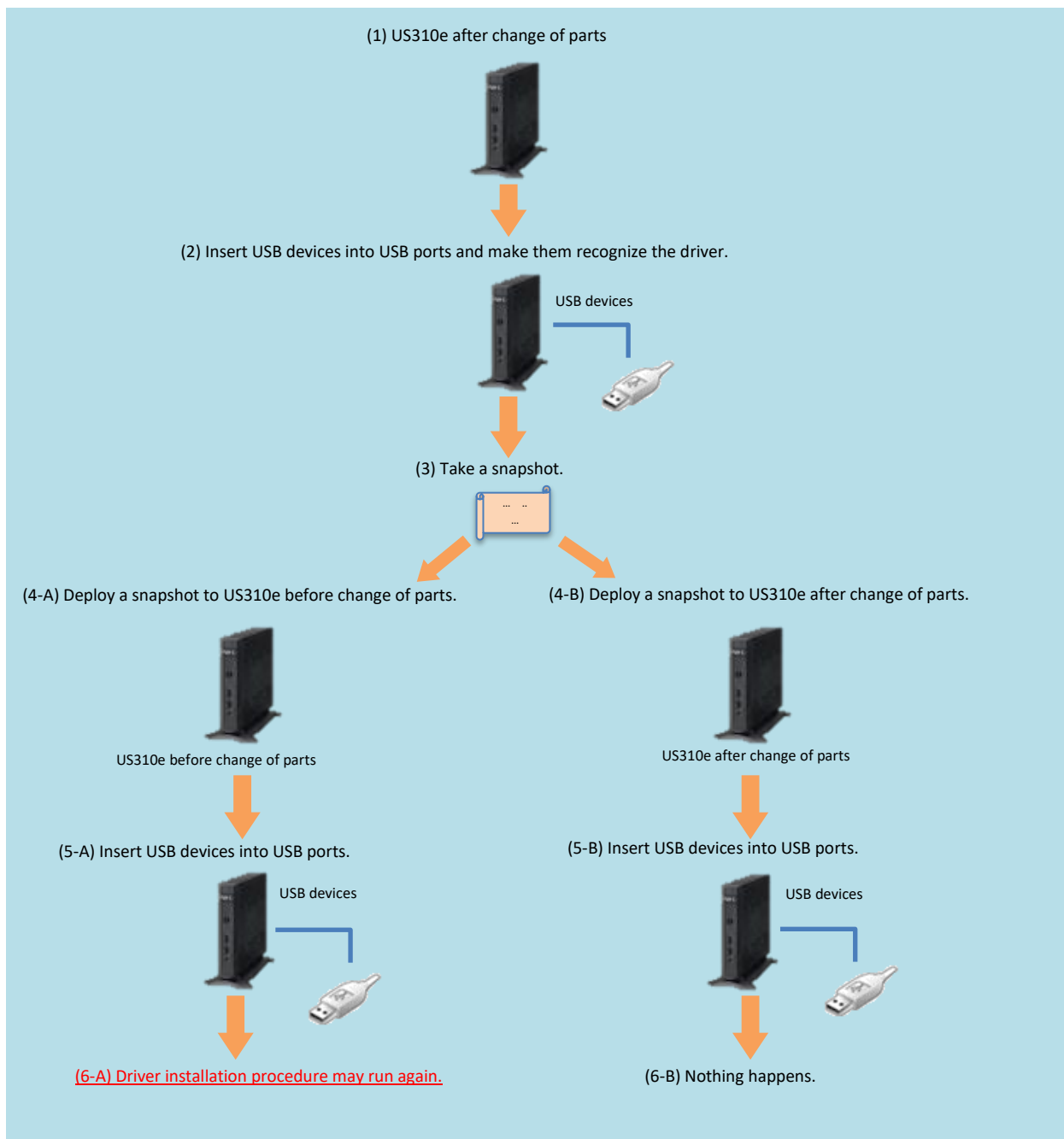
This change has been applied to US310e whose S/N is ST180WH210001 or later.

Snapshot can be used for both old and new US310e, however, USB hardware may be detected by firmware and driver installation procedure may run after firmware boot up. This is the same behavior as the time when a USB device is connected newly and is no problem in actual use.

**The case which took a snapshot from US310e before change of parts.**



The case which took a snapshot from US310e after change of parts.



Driver installation procedure does not run again, by the following steps.

1. Disable Unified Write Filter (hereinafter called UWF).
2. Insert USB devices into USB ports and make them recognize the driver.
3. Enable UWF.

## 2.8 Enabling or Disabling the Appliance Mode

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

### Note

There are two modes for your thin client:

No.	Mode	Description
1	Appliance	The client will automatically start up with the RDP / ICA / View session launched and is shut down after the session ends.
2	Autostart	<p>The client will start up directly with the desired RDP / ICA / View session and perform the configured action after exiting the session.</p> <p>Available actions include:</p> <ul style="list-style-type: none"> <li>• Returning to the local desktop</li> <li>• Re-launching a new session</li> <li>• Restarting the thin client</li> <li>• Turning off the thin client</li> </ul>

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

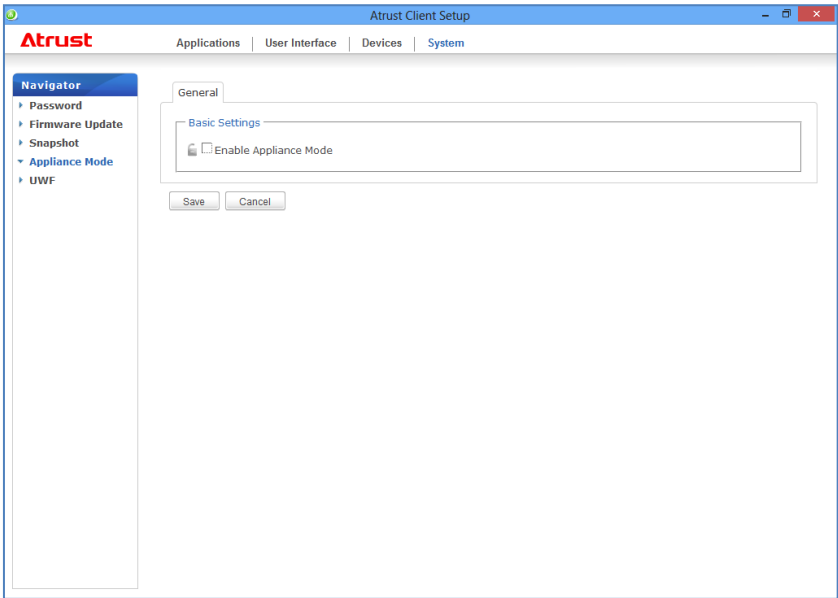
To enable the Appliance mode, do the following:

### Note

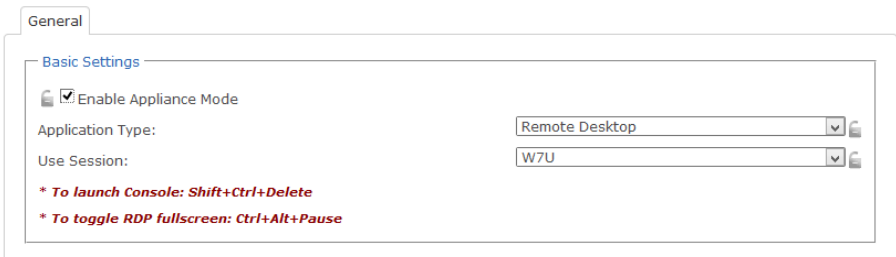
Ensure that you have configured the connection settings for the desired Microsoft Remote Desktop, Citrix ICA, VMware View, or Horizon View session under **Applications** tab. You need to specify which service type and connection settings entry will be used under the Appliance mode. For detailed instructions, 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"

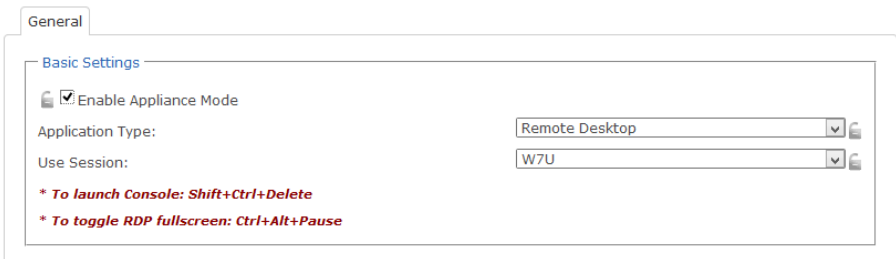
1. On Atrust Client Setup, click **System > Appliance Mode**.



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.





The screenshot shows the 'General' tab of the Atrust Client Setup utility. Under the 'Basic Settings' section, the 'Enable Appliance Mode' checkbox is checked. The 'Application Type' dropdown menu is set to 'VMware View', and the 'Use Session' dropdown menu is set to 'VMH6'. A red note at the bottom of the settings area states: '\* To launch Console: Shift+Ctrl+Delete'.

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

**Note**

To disable the Appliance mode or to access Atrust Client Setup under the Appliance mode, see Chapter 4, "2.8.2 Disabling the Appliance Mode".



## 2.8.2 Disabling the Appliance Mode

To disable the Appliance mode, do the following:

1. In the Appliance mode, exit the Full Screen mode of the RDP / ICA session, or release the keyboard and mouse from the View session (virtual desktop).
  - To exit the Full Screen mode of the RDP session, press Ctrl + Alt + Pause.
  - To exit the Full Screen mode of the ICA session, use the XenDesktop toolbar at the top. (Note that you may not be in the Full Screen mode.)
  - To release the keyboard and mouse from the View session (virtual desktop), press Ctrl + Alt.

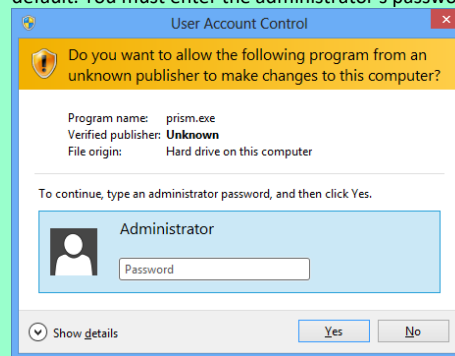
### Note

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

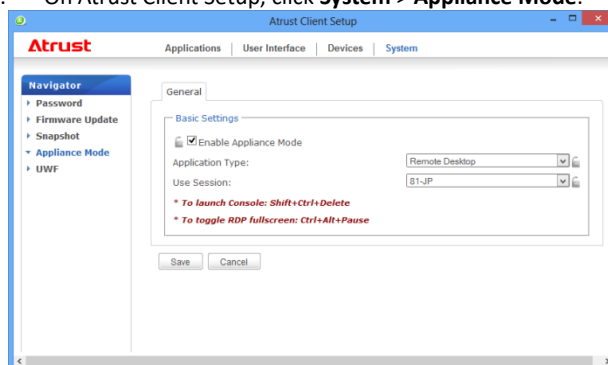
2. Click Shift + Ctrl + A to launch Atrust Client Setup.

### Note

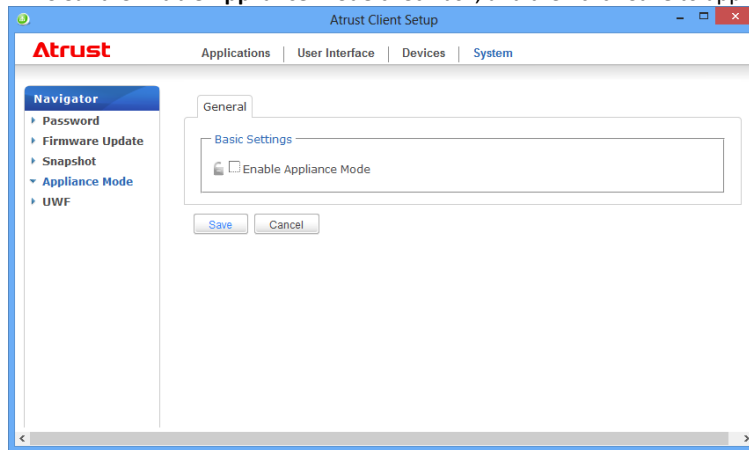
- You cannot access the Taskbar of the client operating system in the Appliance mode.
- When you are using the standard user account, the User Account Control screen appears by default. You must enter the administrator's password to launch Atrust Client Setup.



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



4. Clear the **Enable Appliance Mode** check box, 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 on the View session (virtual desktop) in the background.
6. Sign out from the current RDP / ICA / View session.
7. When you sign out from the session, the client will automatically shut down.
8. Next time, the system starts up with the Appliance mode disabled.

## 2.9    Configuring UWF (Unified Write Filter)

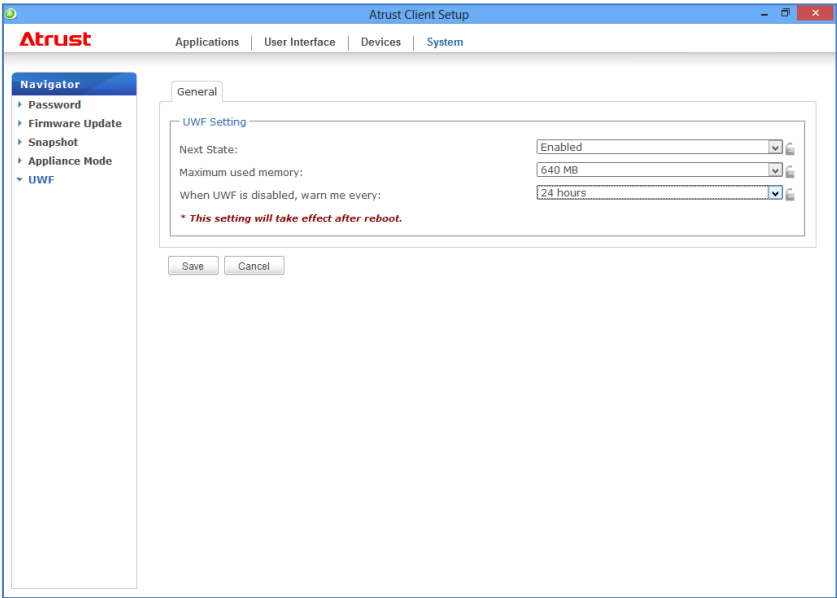
Your US310e is UWF-enabled by default. Unified Write Filter (UWF) is a sector-based write filter intercepting all write attempts to a protected volume and redirecting those write attempts to a RAM cache. With UWF, all system changes will only affect the session where the changes are made. After restart, all changes will be discarded.

Important

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

To configure the UWF settings, do the following:

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






3. Click to select other options if needed.

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

Important

- The maximum memory used recommends 640MB of default value.
- There is a possibility that cash of UWF overlays is used by various factors, and when cash exceeds the maximum memory used, there is a fear that the system becomes unstable.

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

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

**Important**

In case that you need to copy a file to the protected volume, ensure that its size is smaller than the free memory (overlay) space. Otherwise, your system may have unexpected results or become unresponsive.

**Note**

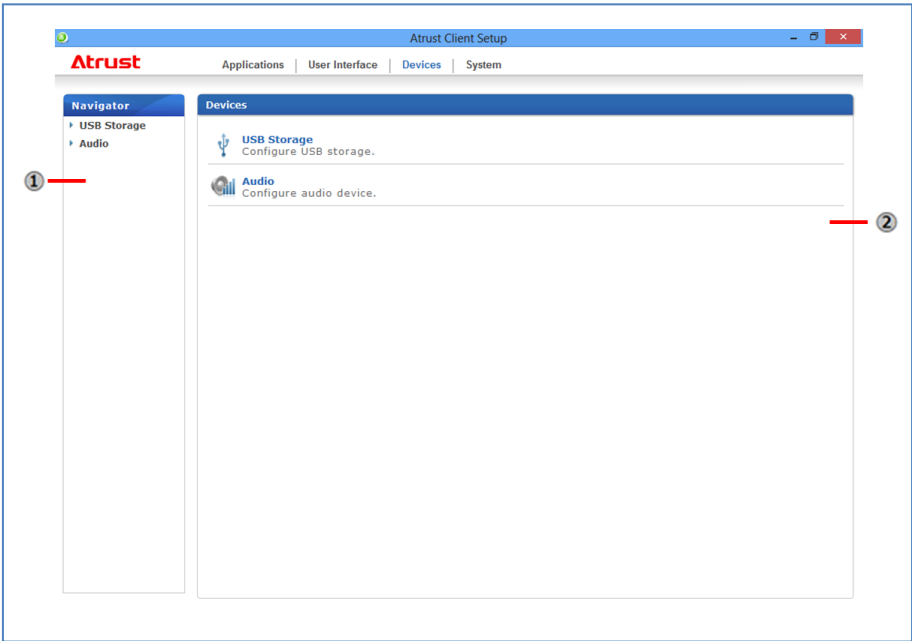
As a thin client device, your US310e is mainly for access to remote or virtual desktops on servers. Because the hard disk space is limited and protected (UWF-enabled), it is *not* recommended to save data on your US310e. Instead, you can use storage space on remote or virtual desktops, removable storage 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.



Devices Tab Overview



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

### 3.2 Available Settings

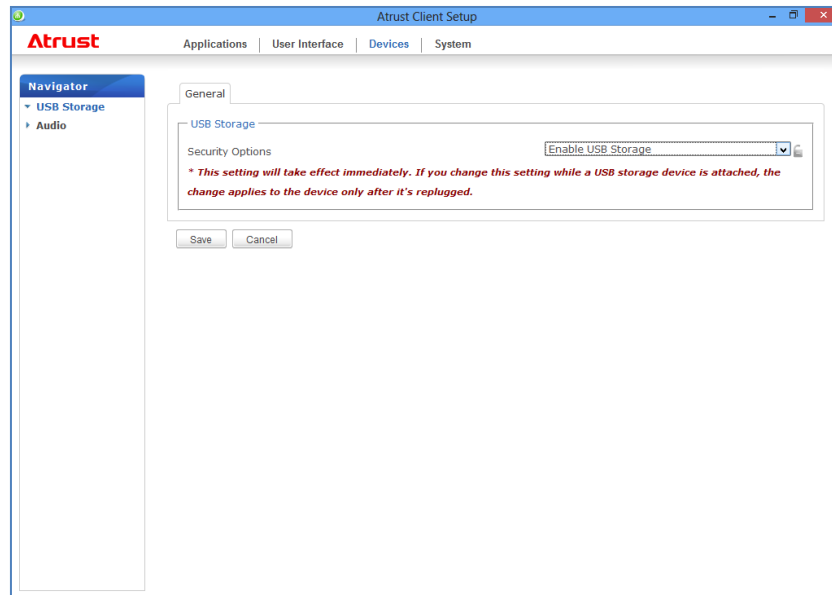
Available settings are shown below:

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**.



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

### Note

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

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

### Important

Even if you select **Disable USB Storage**, the user can use a locally connected USB storage device through redirection in a Citrix ICA and VMware View / Horizon View session. To completely prevent USB storage devices from being used in a virtual desktop session, setup in the Citrix and VMware service delivery environment is required.

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

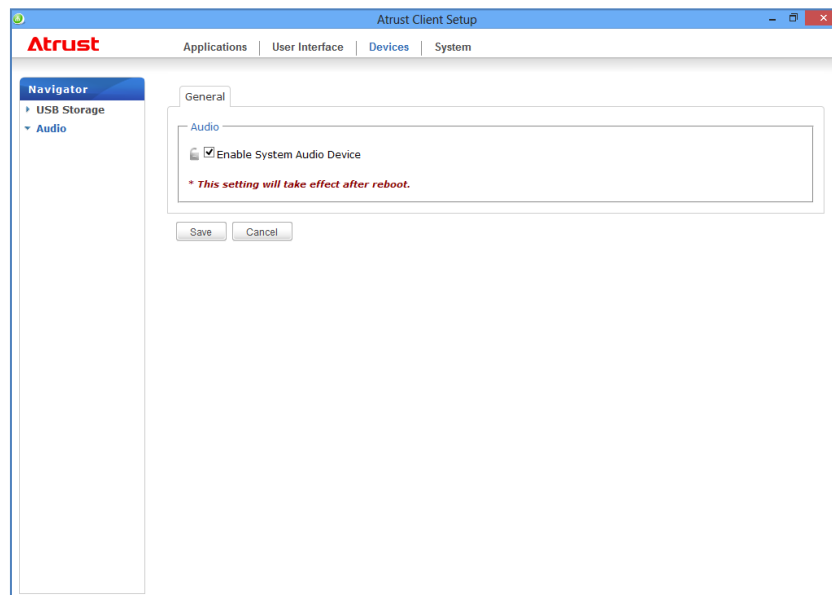
## 3.4 Disabling or Enabling Attached Audio Devices

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

### Note

- If you disable locally attached audio devices, client users are not allowed to perform audio playback or recording with these devices in an RDP / ICA / View session.
- To perform audio playback or recording with local audio devices in an RDP / ICA / View session, you need to enable locally attached audio devices here (the **Audio** setting item under **Devices** tab) and configure audio related settings (if any) in the RDP / ICA / View connection settings. For detailed instructions, see sections:
  - Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"
  - Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"
  - Chapter 4, "5.11 Configuring Advanced View Connection Settings"

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



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

### Note

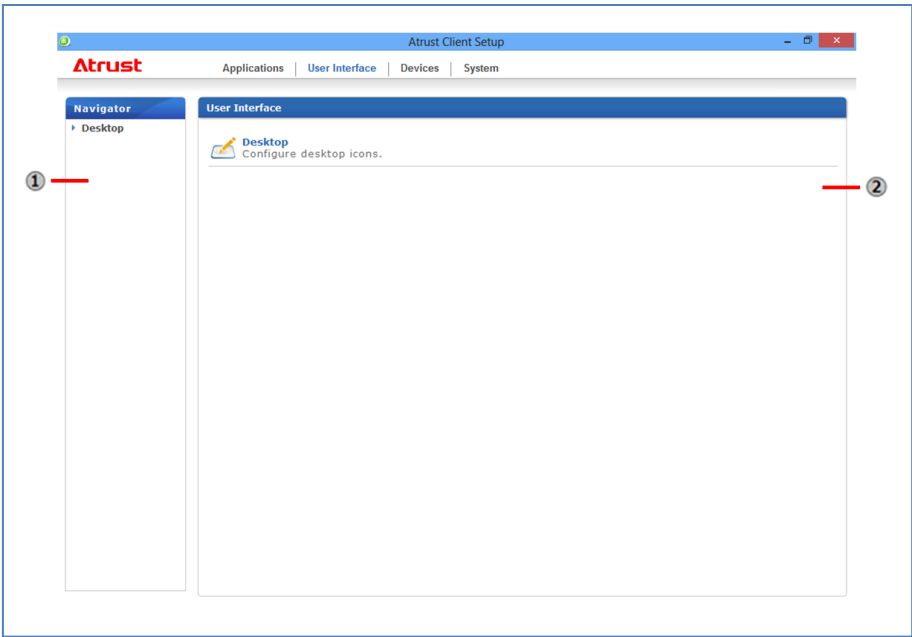
The change will take effect after the client has been restarted.

# 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 <b>User Interface</b> tab.
2	Configuration area	Configures setting values when a setting item is selected.

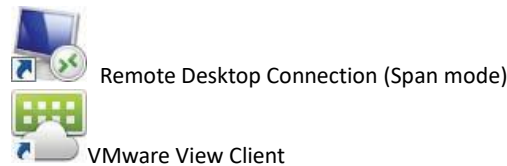
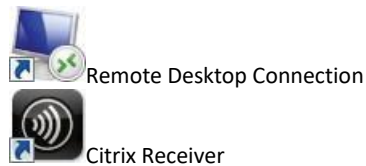
## 4.2 Available Settings

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



## 4.3 Configuring the Display of Standard Desktop Shortcuts for Quick Access

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



### Tip

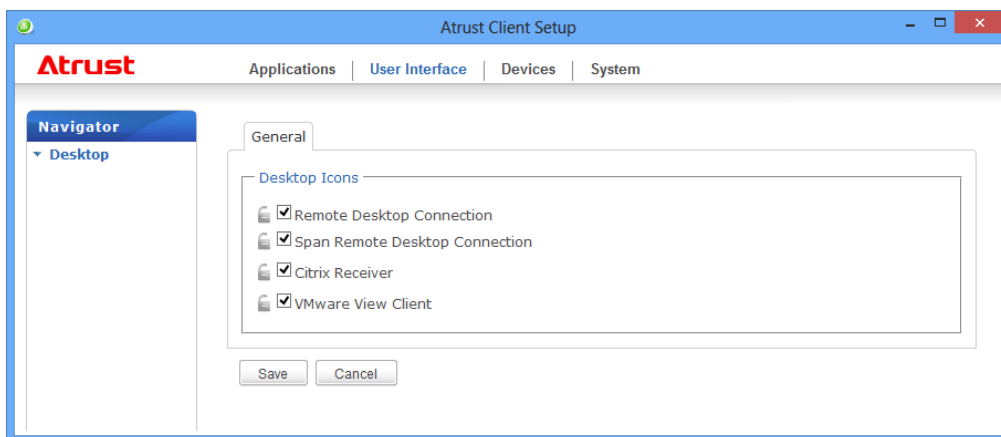
You can use these standard desktop shortcuts to quickly access services. For detailed instructions, see Chapter 3, "1. Standard Shortcuts".

### 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**.

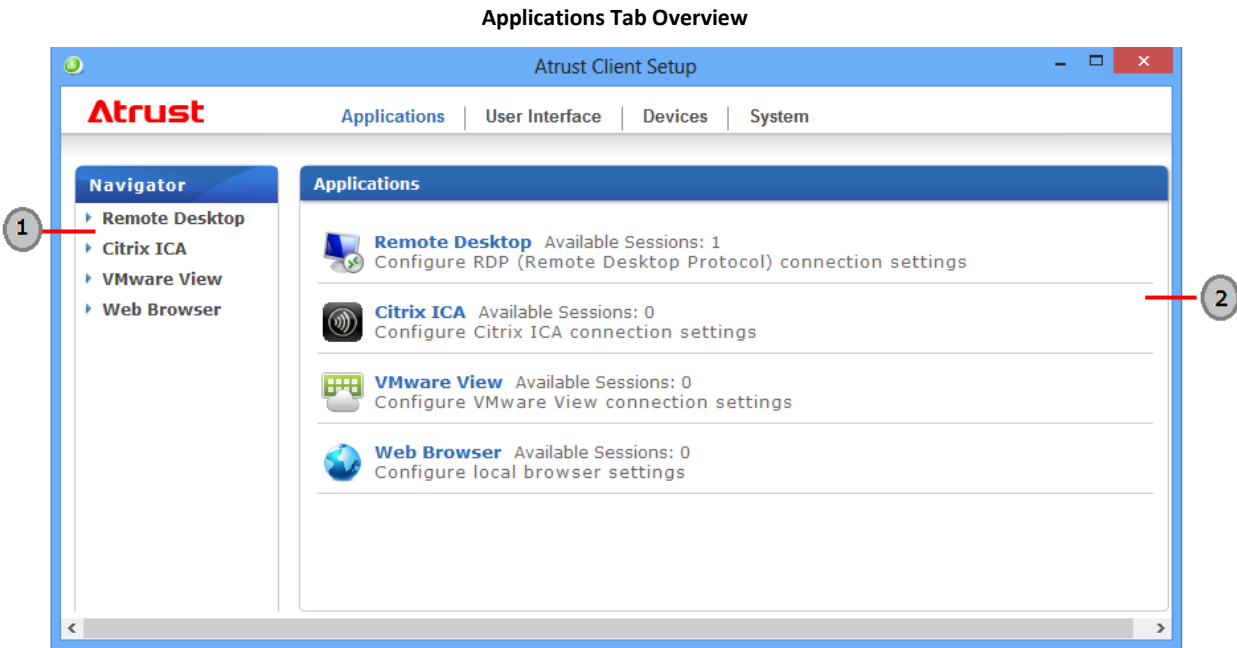


2. Select or clear the **Remote Desktop Connection**, **Span Remote Desktop Connection**, **Citrix Receiver**, and **VMware View Client** check boxes as appropriate.
3. Click **Save** to apply.

# 5. Configuring Service Access Settings





## 5.1 Applications Tab Overview

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



No.	Name	Description
1	Navigation area	Click to select a setting item under <b>Applications</b> 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.	<ul style="list-style-type: none"> <li>Chapter 4, "5.3 Configuring Basic RDP Connection Settings"</li> <li>Chapter 4, "5.4 Accessing Remote Desktop Services"</li> <li>Chapter 4, "5.5 Configuring Advanced RDP Connection Settings"</li> </ul>
	Citrix ICA		Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create access shortcuts on the desktop for ICA sessions.	<ul style="list-style-type: none"> <li>Chapter 4, "5.6 Configuring Basic ICA Connection Settings"</li> <li>Chapter 4, "5.7 Accessing Citrix Services"</li> <li>Chapter 4, "5.8 Configuring Advanced ICA Connection Settings"</li> </ul>
	VMware View		Click to configure VMware View connection settings and create access shortcuts on the desktop for View sessions.	<ul style="list-style-type: none"> <li>Chapter 4, "5.9 Configuring Basic VMware View Connection Settings"</li> <li>Chapter 4, "5.10 Accessing VMware View or Horizon View Services"</li> <li>Chapter 4, "5.11 Configuring Advanced View Connection Settings"</li> </ul>
	Web Browser		Click to configure browser session settings and create access shortcuts on the desktop for browser sessions.	<ul style="list-style-type: none"> <li>Chapter 4, "5.12 Configuring Web Browser Settings"</li> </ul>

## 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](http://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

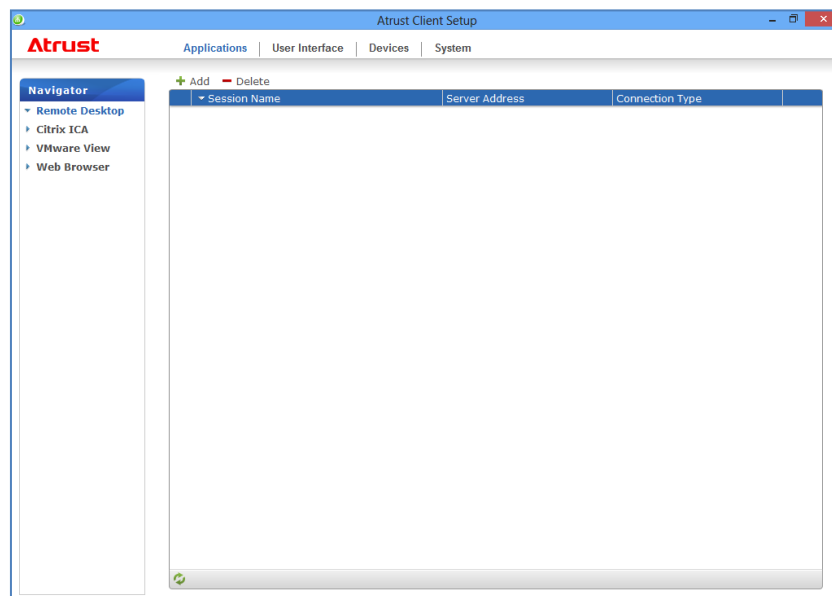
To configure RDP connection settings for Remote Desktop connection type, do the following:

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.

The screenshot shows the Atrust Client Setup window with the General tab selected. The left sidebar contains a Navigator with options: Remote Desktop, Citrix ICA, VMware View, and Web Browser. The main area is divided into three sections: Server Settings, Login Settings, and Common Settings. The Server Settings section includes fields for Session Name, Server Address, Connection Type (set to Remote Desktop), Connection Quality (set to Very Fast (LAN)), and Server Authentication (set to Connect and don't warn me). The Login Settings section includes fields for Username, Password, and Domain. The Common Settings section includes fields for Autostart When Startup (set to No) and On Application Exit (set to Do Nothing). Red asterisks are placed next to the Session Name and Server Address fields, indicating they are required. At the bottom of the window are Save and Cancel buttons.

**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](http://www.microsoft.com) or [support.microsoft.com](http://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**

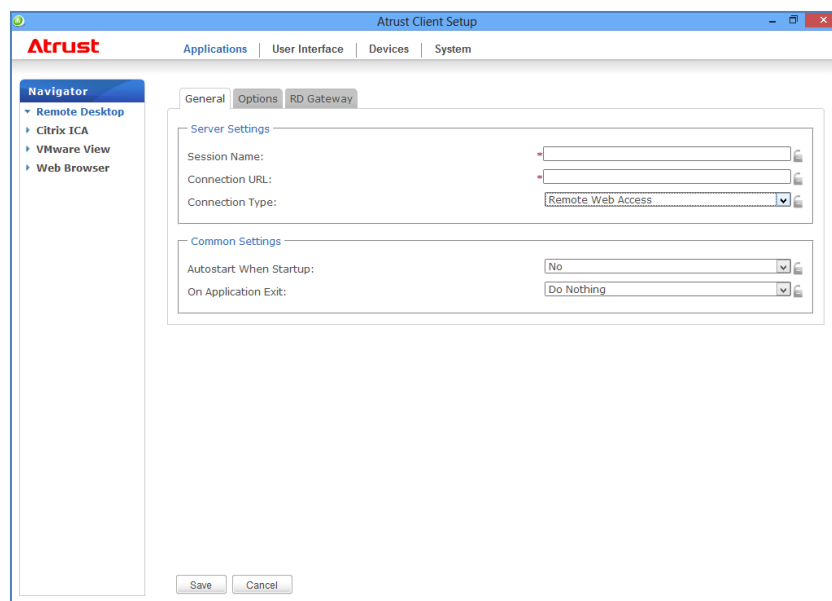
Your US310e supports only RD Web Access based on Windows Server 2012 R2; Windows Server 2008 R2 based is not supported.

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".



## 5.4 Accessing Remote Desktop Services

### 5.4.1 Connection Type: Remote Desktop

To access Remote Desktop services, do the following:

**Note**

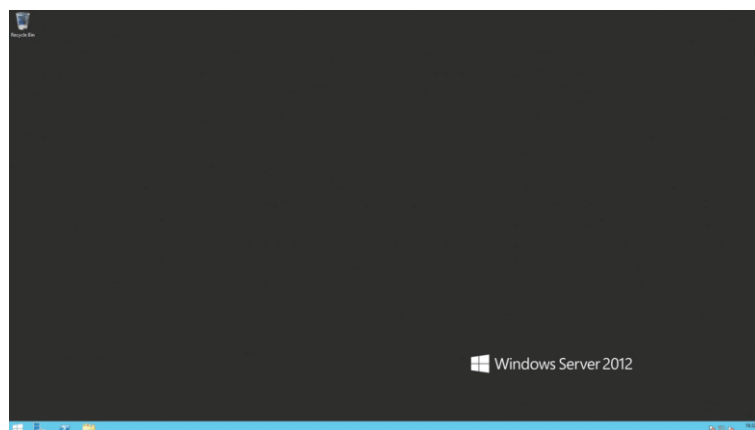
You can also access Remote Desktop services through the standard desktop shortcut **Remote Desktop Connection**. For detailed instructions on how to access services via this standard shortcut, see Chapter 3, "3. Accessing Microsoft Remote Desktop Services".

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).

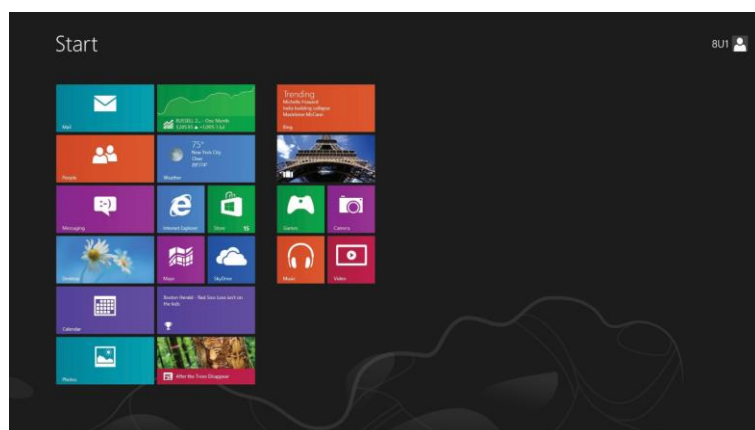
**Note**

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**



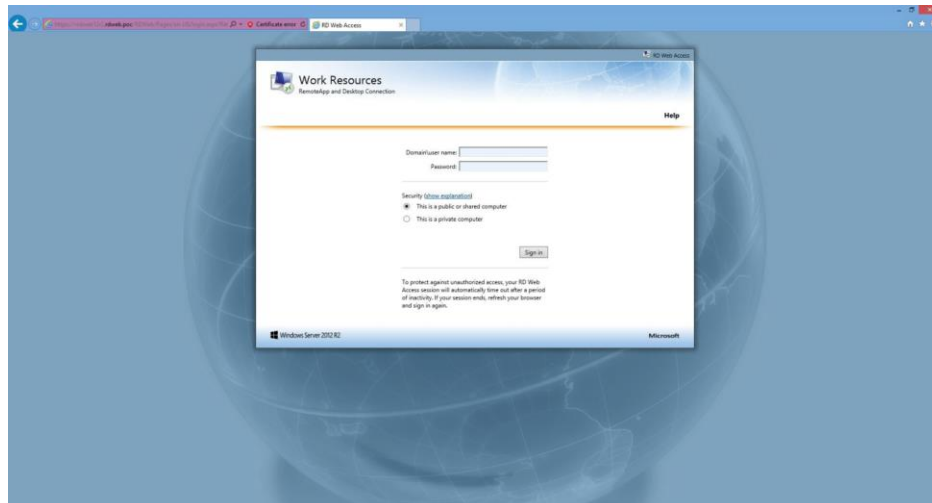
**Example: Windows 8 Enterprise**



### 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.

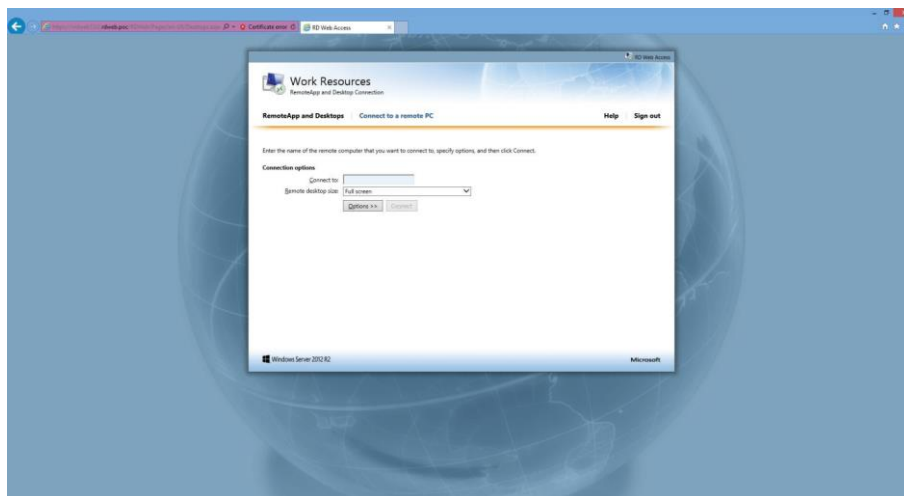
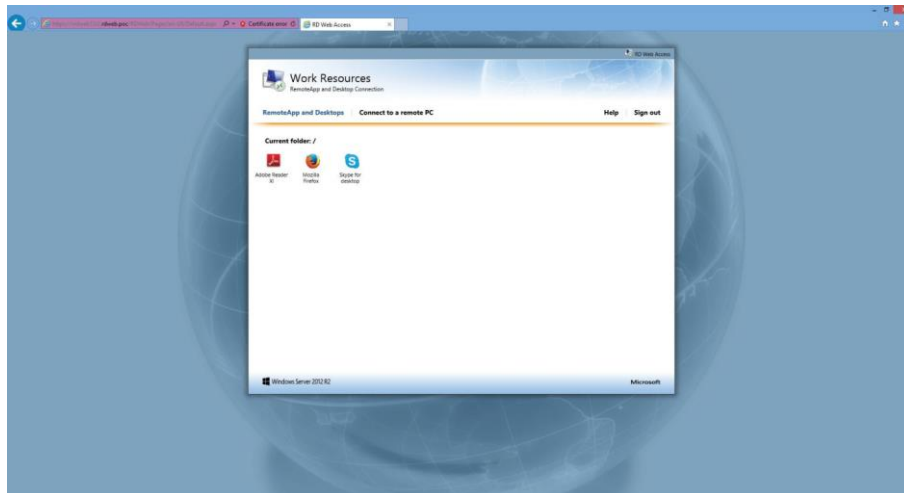


#### Note

- 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**.

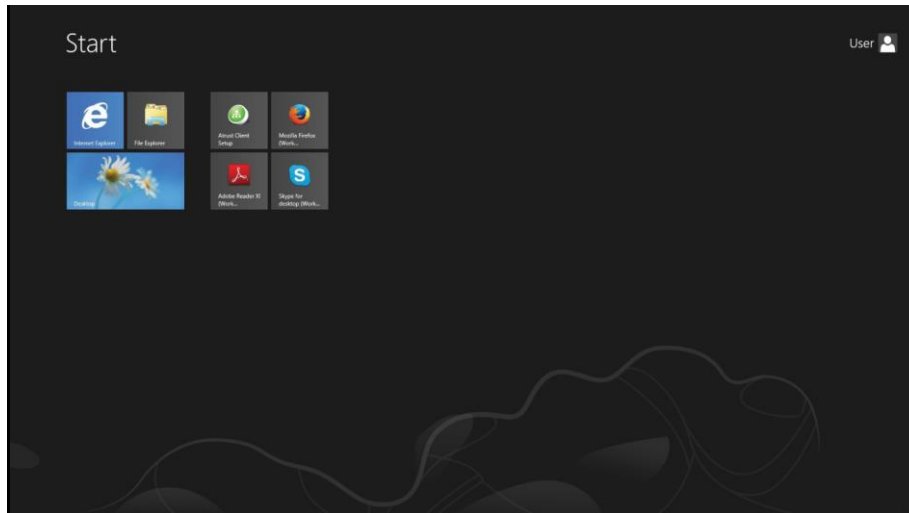
4. Click to select **RemoteApp and Desktops** or **Connect to a remote PC**.



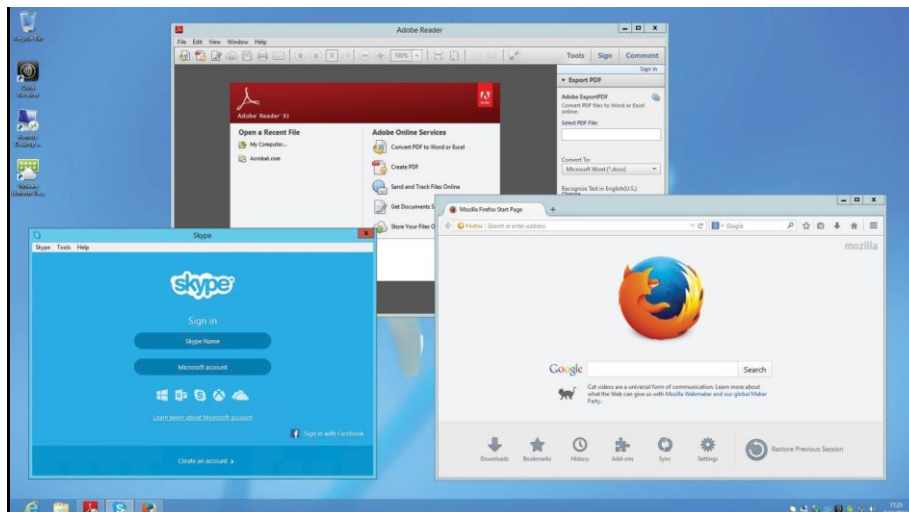
### 5.4.3 Connection Type: Web Feed

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

Common Settings											
Item	Description										
<b>Autostart When Startup</b>	Select whether to open a Remote Desktop session automatically or not when Windows Embedded starts. If <b>Yes</b> is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.										
<b>On Application Exit</b>	<p>Select what to do when a Remote Desktop session is ended. Four options are available: <b>Do Nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.</p> <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>Do Nothing</b></td><td>Does not perform any processing after exiting the session.</td></tr> <tr> <td><b>Restart Application</b></td><td>Opens a Remote Desktop session again.</td></tr> <tr> <td><b>Reboot</b></td><td>Restarts your thin client.</td></tr> <tr> <td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr> </tbody> </table>	Option	Description	<b>Do Nothing</b>	Does not perform any processing after exiting the session.	<b>Restart Application</b>	Opens a Remote Desktop session again.	<b>Reboot</b>	Restarts your thin client.	<b>Shutdown</b>	Turns off your thin client.
Option	Description										
<b>Do Nothing</b>	Does not perform any processing after exiting the session.										
<b>Restart Application</b>	Opens a Remote Desktop session again.										
<b>Reboot</b>	Restarts your thin client.										
<b>Shutdown</b>	Turns off your thin client.										

## Options Sub-tab

Programs							
Item	Description						
<b>Start the following program on connection</b>	<p>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:</p> <ul style="list-style-type: none"> <li>Remote Desktop (when the Application mode is disabled)</li> <li>Remote Application (when the Application mode is enabled)</li> </ul> <p><b>NOTE:</b> Remote Application sessions are Remote sessions used to access only specific applications rather than full desktops.</p> <p><b>NOTE:</b> Before you can open a Remote Application session, you need to add the desired application to the RemoteApp Programs list with RemoteApp Manager on the application hosted server. For detailed instructions on how to add a desired application to the RemoteApp Programs list on the server, visit Microsoft Support website at <a href="http://support.microsoft.com">support.microsoft.com</a>.</p>						
<b>Start in the following folder</b>	<p>Type in the location of the desired application (on the host server) if <b>Start the following program on connection</b> is enabled.</p> <p><b>NOTE:</b> You can type in the location/path of the desired application in this field, and specify only the name of the application in <b>Program path and file name</b> (the next field). Or, you can type in the full path and name of the application in <b>Program path and file name</b>, and leave this field empty.</p>						
<b>Program path and file name</b>	<p>Type in the path and name of the desired application if <b>Start the following program on connection</b> is enabled.</p> <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>Windows Media Player</b></td><td>C:\Programs Files (x86)\Windows Media Player\wmplayer.exe</td></tr> <tr> <td><b>Adobe Reader X</b></td><td>C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32</td></tr> </tbody> </table> <p><b>NOTE:</b> The file extension can be omitted.</p>	Option	Description	<b>Windows Media Player</b>	C:\Programs Files (x86)\Windows Media Player\wmplayer.exe	<b>Adobe Reader X</b>	C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32
Option	Description						
<b>Windows Media Player</b>	C:\Programs Files (x86)\Windows Media Player\wmplayer.exe						
<b>Adobe Reader X</b>	C:\Programs Files (x86)\Adobe\Reader 10.0\Reader\ArcoRd32						

Window Settings	
Item	Description
<b>Color Depth</b>	<p>Click the drop-down menu to select the desired color depth for a Remote Desktop session. Four options are available: <b>15 Bit</b>, <b>16 Bit</b>, <b>24 Bit</b>, and <b>32 Bit</b>.</p> <p><b>NOTE:</b> If RemoteFX is enabled, then no matter which color depth you choose here, 32 bit per pixel will be applied.</p> <p><b>NOTE:</b> 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.</p>
<b>Resolution</b>	<p>Click the drop-down menu to select the desired display resolution on a Remote Desktop session. Twelve options are available: <b>Full Screen</b>, <b>1920x1200</b>, <b>1920x1080</b>, <b>1680x1050</b>, <b>1400x1050</b>, <b>1440x900</b>, <b>1280x1024</b>, <b>1280x768</b>, <b>1280x720</b>, <b>1024x768</b>, <b>800x600</b>, and <b>640x480</b>.</p>
<b>Multi-Monitor</b>	Click the drop-down menu to enable/disable multiple displays in a Remote Desktop session.
<b>Display the connection bar when I use the full screen</b>	Click the drop-down menu to select if the Connection bar is displayed or not in full-screen mode.
Connection Settings	
Item	Description
<b>Printer Mapping</b>	<p>Click the drop-down menu to enable/disable printer mapping. When <b>Enable</b> is selected, users can access a local or network printer in a Remote Desktop session.</p> <p><b>NOTE:</b> 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.</p> <p><b>NOTE:</b> To add a local or network printer for your Windows Embedded-based thin client, go to Control Panel, click <b>Hardware and Sound &gt; Devices and Printers &gt; Add a printer</b>, and then follow the on-screen instructions to add the desired local or network printer.</p>
<b>Clipboard Redirection</b>	<p>Click the drop-down menu to enable/disable Clipboard redirection.</p> <p><b>NOTE:</b> When <b>Enable</b> is selected, Clipboard can be used across local and remote desktops (in both directions).</p> <p><b>NOTE:</b> To use a local or network printer in a Remote Desktop session, you need to add the printer to your thin client, then enable <b>Clipboard Redirection</b>.</p> <p><b>NOTE:</b> To add a local or network printer to a Windows Embedded based thin client, open <b>Control Panel</b> and select <b>Hardware and Sound &gt; Devices and Printers &gt; Add Printer</b>, then follow the on-screen instructions.</p>
<b>Smart Card Mapping</b>	<p>Click the drop-down menu to enable/disable smart card mapping.</p> <p>When <b>Enable</b> is selected, users can access smart cards through a smart card reader in a Remote Desktop session.</p>
<b>Port Mapping</b>	<p>Click the drop-down menu to enable/disable port mapping.</p> <p>When <b>Enable</b> is selected, users can access attached devices using locally available ports, in a Remote Desktop session.</p> <p><b>NOTE:</b> The types and availability of device ports on thin clients may vary, depending on your product models.</p>

Local Resources Settings									
Item	Description								
<b>Remote Audio Playback</b>	<p>Click the drop-down menu to configure the computer sounds and audio playback setting in a Remote Desktop session. Three options are available: <b>Bring to this computer</b>, <b>Do not play</b>, and <b>Leave at remote computer</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Bring to this computer</b></td><td>Allows computer sounds and audio playback in a Remote Desktop session using locally attached audio devices.</td></tr> <tr> <td><b>Do not play</b></td><td>Disables computer sounds and audio playback in a Remote Desktop session.</td></tr> <tr> <td><b>Leave at remote computer</b></td><td>Leave computer sounds and audio playback at the remote computer.</td></tr> </table>	Option	Description	<b>Bring to this computer</b>	Allows computer sounds and audio playback in a Remote Desktop session using locally attached audio devices.	<b>Do not play</b>	Disables computer sounds and audio playback in a Remote Desktop session.	<b>Leave at remote computer</b>	Leave computer sounds and audio playback at the remote computer.
Option	Description								
<b>Bring to this computer</b>	Allows computer sounds and audio playback in a Remote Desktop session using locally attached audio devices.								
<b>Do not play</b>	Disables computer sounds and audio playback in a Remote Desktop session.								
<b>Leave at remote computer</b>	Leave computer sounds and audio playback at the remote computer.								
<b>Remote Audio Recording</b>	<p>Click the drop-down menu to configure the audio recording setting in a Remote Desktop session. Two options are available: <b>Recording from this computer</b> and <b>Do not record</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Recording from this computer</b></td><td>Allows audio recording in a Remote Desktop session using locally attached audio devices.</td></tr> <tr> <td><b>Do not record</b></td><td>Disables audio recording in a Remote Desktop session using locally attached audio devices.</td></tr> </table> <p><b>NOTE:</b> When <b>Leave at remote computer</b> is selected on the drop-down menu of <b>Remote Audio Playback</b>, this setting item will be grayed out.</p>	Option	Description	<b>Recording from this computer</b>	Allows audio recording in a Remote Desktop session using locally attached audio devices.	<b>Do not record</b>	Disables audio recording in a Remote Desktop session using locally attached audio devices.		
Option	Description								
<b>Recording from this computer</b>	Allows audio recording in a Remote Desktop session using locally attached audio devices.								
<b>Do not record</b>	Disables audio recording in a Remote Desktop session using locally attached audio devices.								
<b>Apply Windows key combinations</b>	Click the drop-down menu to select where to apply Windows key combinations. Three options are available: <b>On this computer</b> , <b>On the remote computer</b> , <b>Only when using the full screen</b> .								
<b>Drives</b>	Click the drop-down menu to enable/disable locally attached drives in a Remote Desktop session.								
<b>Supported plug and play devices</b>	Click the drop-down menu to enable/disable the supported plug and play devices in a Remote Desktop session.								
<b>RemoteFX USB redirection</b>	<p>Click to enable/disable locally attached RemoteFX USB devices.</p> <p><b>NOTE:</b> To use RemoteFX USB devices in remote desktops, you need to configure the policy setting about device redirection to allow RemoteFX USB Device Redirection as well. To do so, follow the steps below:</p> <ol style="list-style-type: none"> <li>1. Sign in to your US310e with an administrative account.</li> <li>2. Disable UWF (Unified Write Filter) through Atrust Client Setup (See Chapter 4, "2.9 Configuring UWF (Unified Write Filter)").</li> <li>3. On the <b>desktop</b> or <b>Start screen</b>, move your mouse to the bottom-right corner. The charms appear.</li> <li>4. Click <b>Search</b> to select the Search charm.</li> <li>5. Type <b>group policy</b> in the Search charm, and then click <b>Settings</b>. <b>Edit group policy</b> appears on the left.</li> <li>6. Click to select <b>Edit group policy</b>.</li> <li>7. On the opened window, select <b>Computer Configuration &gt; Administrative Templates &gt; Windows Components &gt; Remote Desktop Services &gt; Remote Desktop Connection Client &gt; RemoteFX USB Device Redirection &gt; Allow RDP redirection of other supported RemoteFX USB devices from this computer</b>.</li> <li>8. Select <b>Enabled</b> and to which users this setting applies: <b>Administrators Only</b> or <b>Administrators and Users</b>, and then click <b>OK</b>.</li> <li>9. Enable UWF through Atrust Client Setup.</li> </ol>								



## RD Gateway Sub-tab

Connection Settings									
Item	Description								
<b>RD Gateway Server Settings</b>	Click the drop-down menu to choose if a RD Gateway server is used, automatically detected, or manually configured. Three options are available: <b>Automatically detect RD Gateway server settings</b> , <b>Use these RD Gateway server settings</b> , and <b>Do not use an RD Gateway server</b> .								
<b>Server Name</b>	Type the IP address / URL / FQDN of the RD Gateway server. <b>NOTE:</b> Consult your network administrator for details.								
<b>Logon method</b>	Click the drop-down menu to select the logon method. Three options are available: <b>Allow me to select later</b> , <b>Ask for password (NTLM)</b> , and <b>Smart card</b> . <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>Allow me to select later</b></td><td>Users can select a logon method while connecting to the server.</td></tr> <tr> <td><b>Ask for password (NTLM)</b></td><td>Users will be prompted for a password while connecting to the server.</td></tr> <tr> <td><b>Smart card</b></td><td>Users will be prompted for a smart card while connecting to the server.</td></tr> </tbody> </table>	Option	Description	<b>Allow me to select later</b>	Users can select a logon method while connecting to the server.	<b>Ask for password (NTLM)</b>	Users will be prompted for a password while connecting to the server.	<b>Smart card</b>	Users will be prompted for a smart card while connecting to the server.
Option	Description								
<b>Allow me to select later</b>	Users can select a logon method while connecting to the server.								
<b>Ask for password (NTLM)</b>	Users will be prompted for a password while connecting to the server.								
<b>Smart card</b>	Users will be prompted for a smart card while connecting to the server.								
<b>Bypass RD Gateway server for local addresses</b>	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								
<b>Use my RD Gateway credentials for the remote computer</b>	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										
<b>Session Name</b>	Type in the name for Remote Web Access sessions.										
<b>Connection URL</b>	Type in the connection URL through which RD Web Access is available.										
<b>Connection Type</b>	<p>This table only provides descriptions for available settings when <b>Remote Web Access</b> is selected. Three connection types are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Remote Desktop</b></td><td>Does not perform any processing after exiting the session.</td></tr> <tr> <td><b>Remote Web Access</b></td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr> <tr> <td><b>Web Feed</b></td><td>Provides access to remote applications through published Start screen tiles.</td></tr> </table>	Option	Description	<b>Remote Desktop</b>	Does not perform any processing after exiting the session.	<b>Remote Web Access</b>	Provides access to remote desktops/applications through a Web browser (Internet Explorer).	<b>Web Feed</b>	Provides access to remote applications through published Start screen tiles.		
Option	Description										
<b>Remote Desktop</b>	Does not perform any processing after exiting the session.										
<b>Remote Web Access</b>	Provides access to remote desktops/applications through a Web browser (Internet Explorer).										
<b>Web Feed</b>	Provides access to remote applications through published Start screen tiles.										
Common Settings											
Item	Description										
<b>Autostart When Startup</b>	Select whether to open a Remote Desktop session automatically or not when Windows Embedded starts. If <b>Yes</b> is selected, every time when you log in to the system, the Remote Desktop session will be opened automatically.										
<b>On Application Exit</b>	<p>Select what to do when a Remote Desktop session is ended. Four options are available: <b>Do Nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Do Nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr> <tr> <td><b>Restart Application</b></td><td>Opens a Remote Desktop session again.</td></tr> <tr> <td><b>Reboot</b></td><td>Restarts your thin client.</td></tr> <tr> <td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr> </table>	Option	Description	<b>Do Nothing</b>	Returns to the Windows Embedded desktop.	<b>Restart Application</b>	Opens a Remote Desktop session again.	<b>Reboot</b>	Restarts your thin client.	<b>Shutdown</b>	Turns off your thin client.
Option	Description										
<b>Do Nothing</b>	Returns to the Windows Embedded desktop.										
<b>Restart Application</b>	Opens a Remote Desktop session again.										
<b>Reboot</b>	Restarts your thin client.										
<b>Shutdown</b>	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								
<b>Session Name</b>	Type in the name for Web Feed sessions.								
<b>Web Feed URL</b>	Type in the computer name or IP address of the server/virtual machine where to deliver a Web Feed session.								
<b>Connection Type</b>	<p>This table only provides descriptions for available settings when <b>Web Feed</b> is selected. Three connection types are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Remote Desktop</b></td><td>Provides access to remote desktops/applications.</td></tr> <tr> <td><b>Remote Web Access</b></td><td>Provides access to remote desktops/applications through a Web browser (Internet Explorer).</td></tr> <tr> <td><b>Web Feed</b></td><td>Provides access to remote applications through published Start screen tiles.</td></tr> </table>	Option	Description	<b>Remote Desktop</b>	Provides access to remote desktops/applications.	<b>Remote Web Access</b>	Provides access to remote desktops/applications through a Web browser (Internet Explorer).	<b>Web Feed</b>	Provides access to remote applications through published Start screen tiles.
Option	Description								
<b>Remote Desktop</b>	Provides access to remote desktops/applications.								
<b>Remote Web Access</b>	Provides access to remote desktops/applications through a Web browser (Internet Explorer).								
<b>Web Feed</b>	Provides access to remote applications through published Start screen tiles.								
Login Settings									
Item	Description								
<b>Username</b>	Type in the user/account name used for authentication.								
<b>Password</b>	Type in the password of the user account used for authentication.								
<b>Domain</b>	<p>Type in the domain of the server.</p> <p><b>NOTE:</b> Leave this field blank if the server doesn't belong to any domain.</p>								
RemoteApp and Desktop Connection									
Item	Description								
<b>Update Now</b>	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.

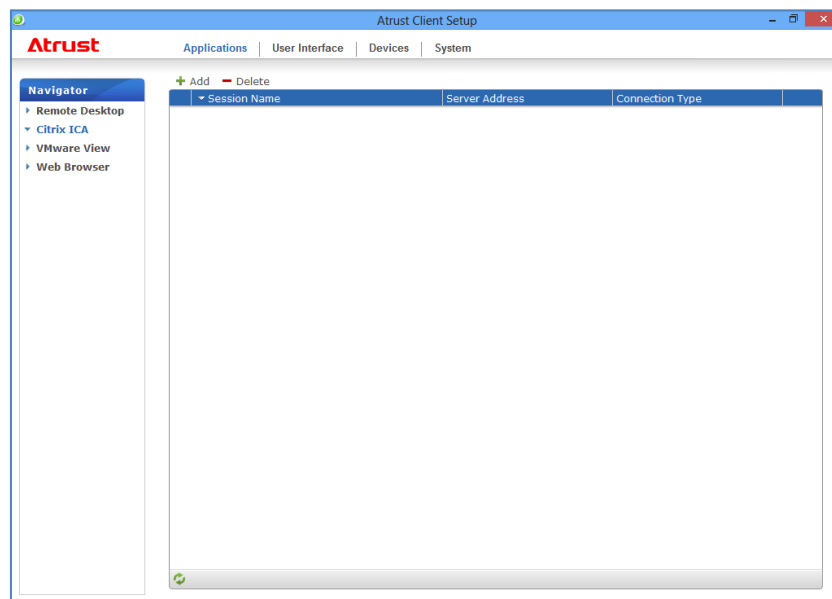
### Note

- For more information on Citrix desktop virtualization solutions, visit Citrix website at [www.citrix.com](http://www.citrix.com) or Citrix Knowledge Center at [support.citrix.com](http://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.

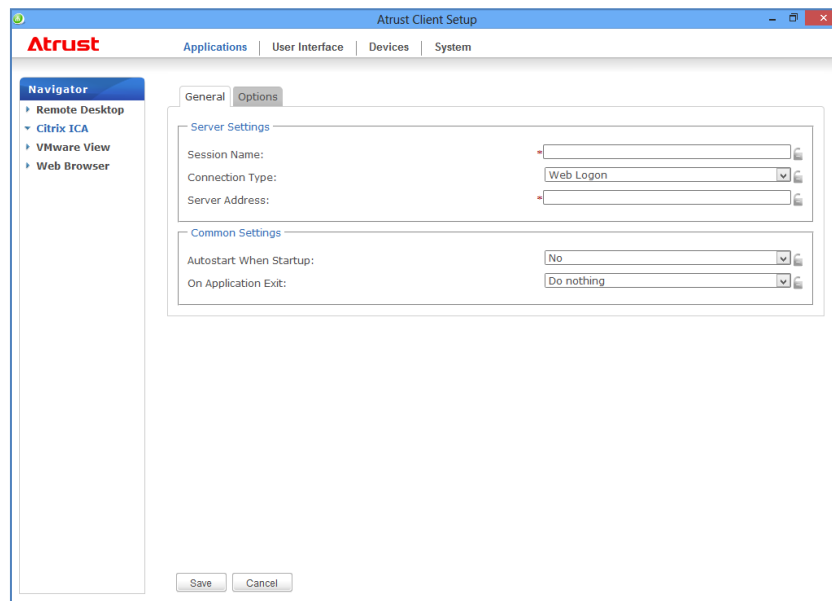


### Note

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.

- 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.

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

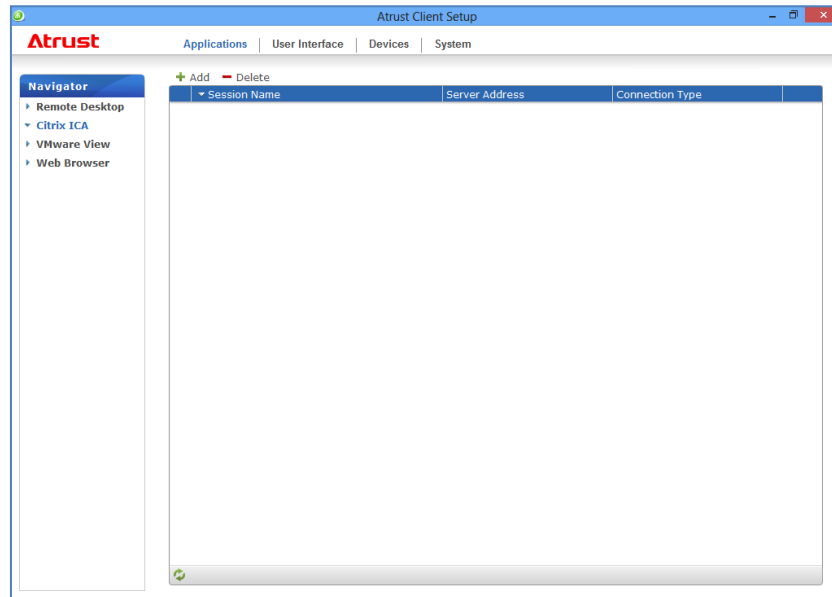
**Note**

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:

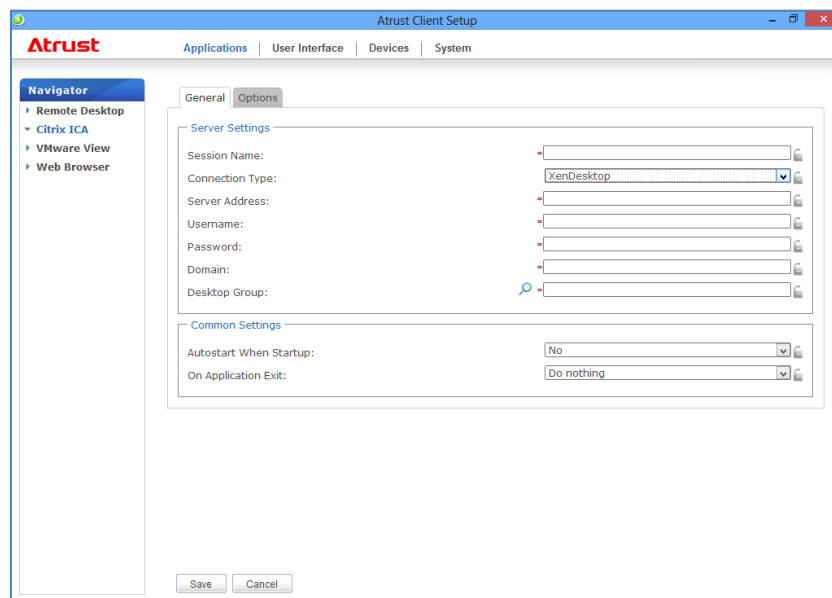
1. On Atrust Client Setup, click **Applications > Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.




#### 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**.

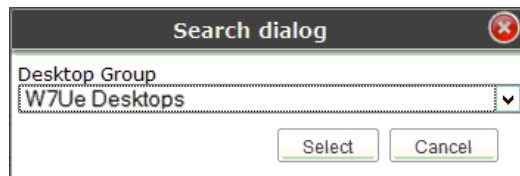


5. Type the session name, the IP address / FQDN of the server through which XenDesktop is accessible, user credentials, the domain of the server, and then click the Search icon (  ) to discover available desktop groups.

**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.

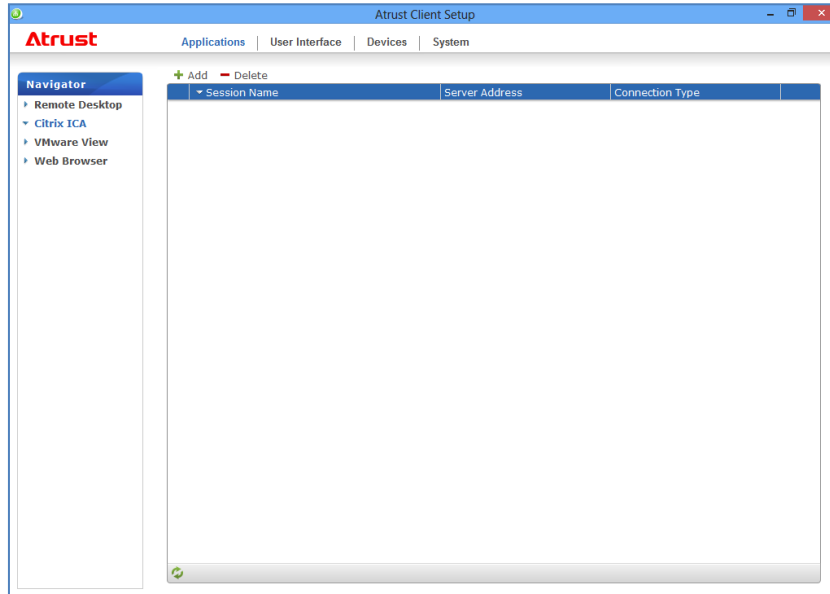
**Note**

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:

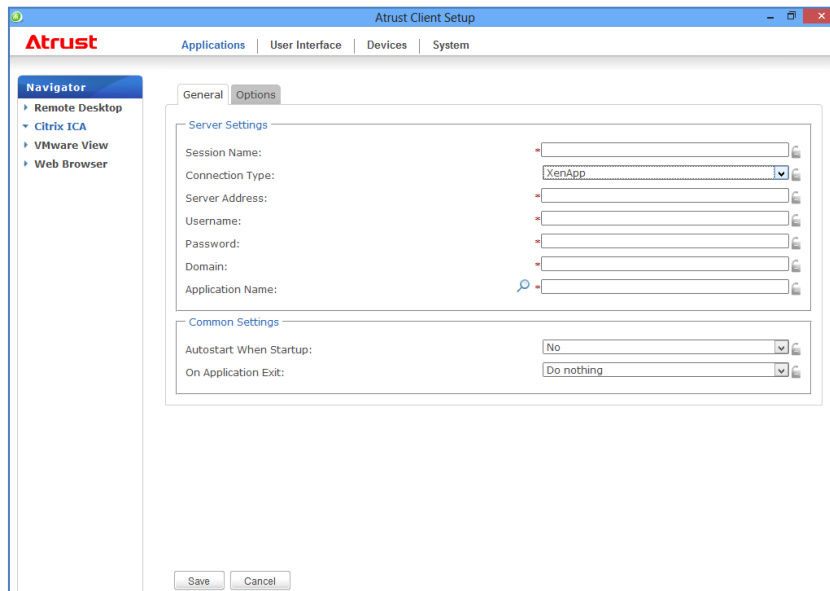
1. On Atrust Client Setup, click **Applications > Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.




#### 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.

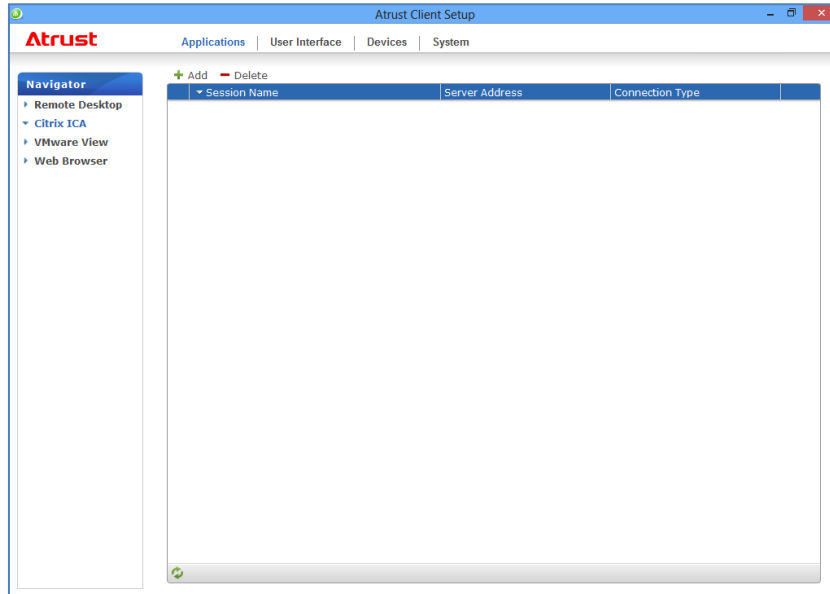
**Note**

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:

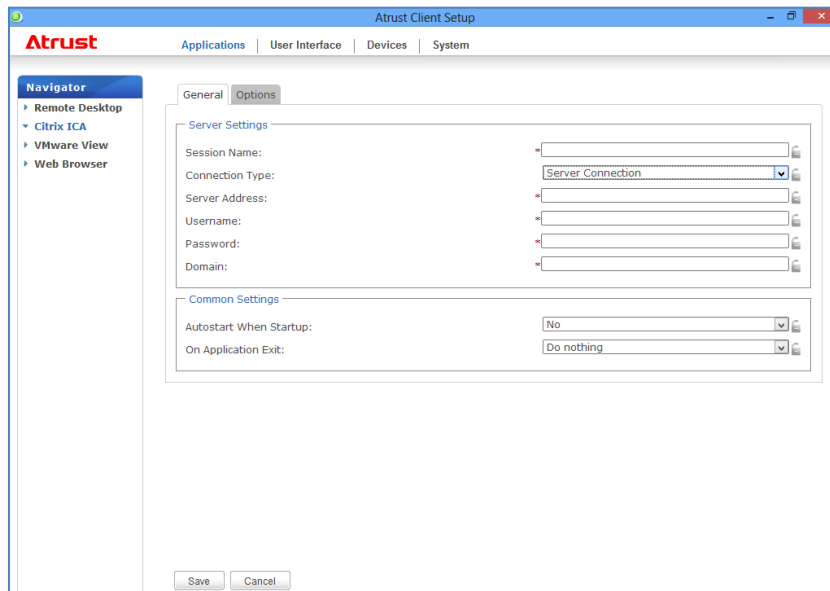
1. On Atrust Client Setup, click **Applications > Citrix ICA**.
2. The available ICA Connection list appears in the Configuration area.



#### 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

---

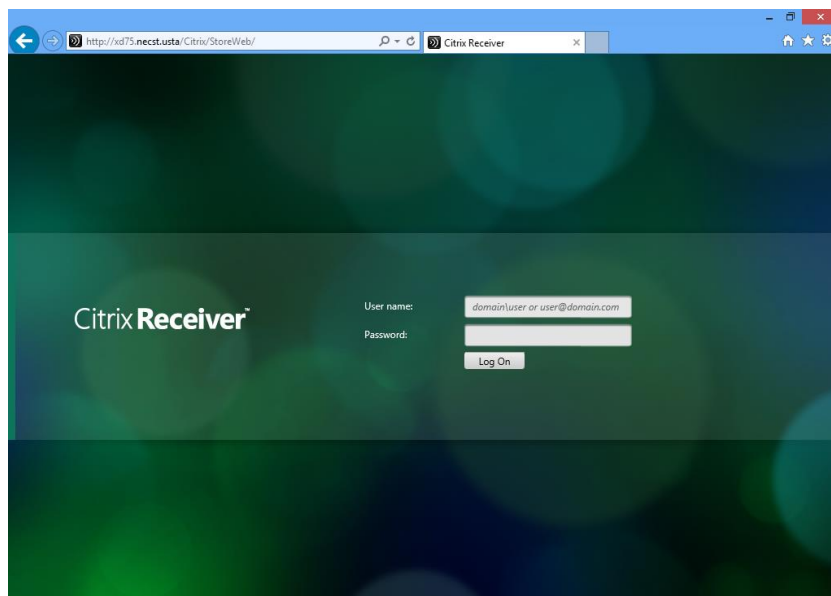
To access Citrix services, do the following:

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.

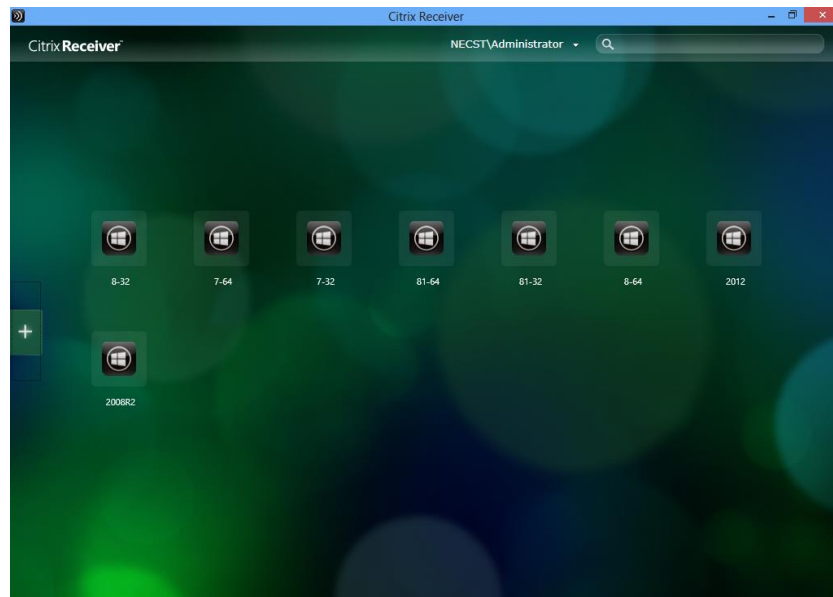


3. Type in the required credentials and domain name, and then click **Log On**.

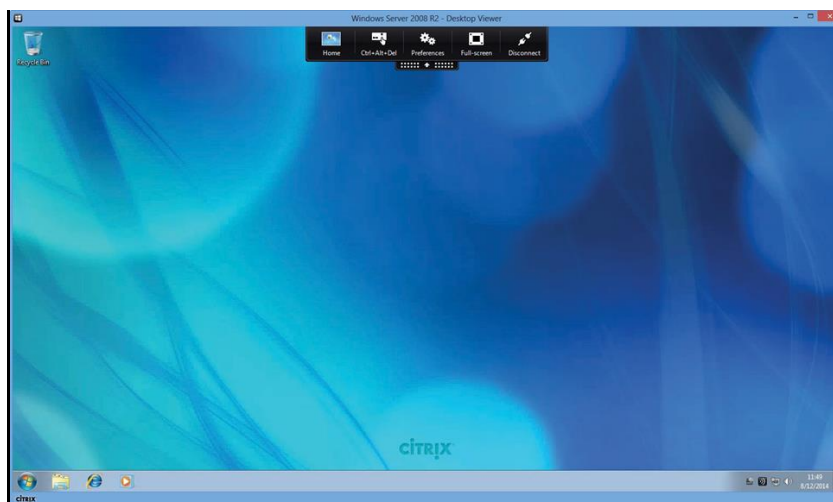
**Note**

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										
<b>Session Name</b>	Type in the name for Web Logon sessions.										
<b>Connection Type</b>	<p>This table only provides descriptions for available settings when <b>Web Logon</b> is selected. Four connection types are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr> <tr> <td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr> <tr> <td><b>XenApp</b></td><td>Provides application delivery services.</td></tr> <tr> <td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr> </table> <p><b>NOTE:</b> When <b>Web Logon</b> 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.</p> <p>For more details, see Chapter 4, "5.7 Accessing Citrix Services".</p>	Option	Description	<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).	<b>XenDesktop</b>	Provides desktop delivery services.	<b>XenApp</b>	Provides application delivery services.	<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).
Option	Description										
<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).										
<b>XenDesktop</b>	Provides desktop delivery services.										
<b>XenApp</b>	Provides application delivery services.										
<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).										
<b>Server Address</b>	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										
<b>Autostart When Startup</b>	Select whether to open a Citrix ICA session automatically or not when US310e starts. If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.										
<b>On Application Exit</b>	<p>Select what to do when a Citrix ICA session is ended. Four options are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Do nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr> <tr> <td><b>Restart Application</b></td><td>Opens a Citrix ICA session again.</td></tr> <tr> <td><b>Reboot</b></td><td>Restarts your thin client.</td></tr> <tr> <td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr> </table>	Option	Description	<b>Do nothing</b>	Returns to the Windows Embedded desktop.	<b>Restart Application</b>	Opens a Citrix ICA session again.	<b>Reboot</b>	Restarts your thin client.	<b>Shutdown</b>	Turns off your thin client.
Option	Description										
<b>Do nothing</b>	Returns to the Windows Embedded desktop.										
<b>Restart Application</b>	Opens a Citrix ICA session again.										
<b>Reboot</b>	Restarts your thin client.										
<b>Shutdown</b>	Turns off your thin client.										

## Options Sub-tab


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

## 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										
<b>Session Name</b>	Type in the name for Citrix ICA sessions.										
<b>Connection Type</b>	<p>This table only provides descriptions for available settings when <b>XenDesktop</b> is selected. Four connection types are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr> <tr> <td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr> <tr> <td><b>XenApp</b></td><td>Provides application delivery services.</td></tr> <tr> <td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr> </table>	Option	Description	<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).	<b>XenDesktop</b>	Provides desktop delivery services.	<b>XenApp</b>	Provides application delivery services.	<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).
Option	Description										
<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).										
<b>XenDesktop</b>	Provides desktop delivery services.										
<b>XenApp</b>	Provides application delivery services.										
<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).										
<b>Server Address</b>	Type in the IP address / FQDN of the server through which XenDesktop is accessible.										
<b>Username</b>	Type in the user/account name used for authentication.										
<b>Password</b>	Type in the password of the user account used for authentication.										
<b>Domain</b>	Type in the domain of the server.										
<b>Desktop Group</b>	<p>Type in the desktop group.</p> <p><b>NOTE:</b> You can use the Search icon (  ) in front of the field to discover available desktop groups. For detailed instructions, see Chapter 4, "5.6.2 Connection Type: XenDesktop".</p>										
Common Settings											
Item	Description										
<b>Autostart When Startup</b>	<p>Select whether to open a Citrix ICA session automatically or not when US310e starts.</p> <p>If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.</p>										
<b>On Application Exit</b>	<p>Select what to do when a Citrix ICA session is ended. Four options are available: <b>Do nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Do nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr> <tr> <td><b>Restart Application</b></td><td>Opens a Citrix ICA session again.</td></tr> <tr> <td><b>Reboot</b></td><td>Restarts your thin client.</td></tr> <tr> <td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr> </table>	Option	Description	<b>Do nothing</b>	Returns to the Windows Embedded desktop.	<b>Restart Application</b>	Opens a Citrix ICA session again.	<b>Reboot</b>	Restarts your thin client.	<b>Shutdown</b>	Turns off your thin client.
Option	Description										
<b>Do nothing</b>	Returns to the Windows Embedded desktop.										
<b>Restart Application</b>	Opens a Citrix ICA session again.										
<b>Reboot</b>	Restarts your thin client.										
<b>Shutdown</b>	Turns off your thin client.										



## Options Sub-tab


Window Settings											
Item	Description										
<b>Requested Color Quality</b>	<p>Click the drop-down menu to select the desired color quality for a Citrix ICA session.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>No preference</b></td><td>No preference for a specific color quality.</td></tr> <tr> <td><b>Better Speed (16-bit)</b></td><td>The 16-bit color quality is used for better display speed.</td></tr> <tr> <td><b>Better Appearance (32-bit)</b></td><td>The 32-bit color quality is used for better desktop appearance.</td></tr> </table>	Option	Description	<b>No preference</b>	No preference for a specific color quality.	<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.	<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.		
Option	Description										
<b>No preference</b>	No preference for a specific color quality.										
<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.										
<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.										
<b>Window Size</b>	<p>Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: <b>Default</b>, <b>Seamless</b>, <b>Full Screen</b>, <b>640 x 480</b>, <b>800 x 600</b>, <b>1024 x 768</b>, <b>1280 x 1024</b>, and <b>1600 x 1200</b>.</p> <p><b>NOTE:</b> When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size.</p> <p><b>NOTE:</b> For more information about how to disable the XenDesktop toolbar, visit Citrix websites at <a href="http://support.citrix.com">support.citrix.com</a> or <a href="http://www.citrix.com">www.citrix.com</a> for online help.</p> <p><b>NOTE:</b> In case that you don't want to disable the toolbar, you can use the toolbar or your mouse to resize the launched window if needed.</p>										
Device Mapping											
Item	Description										
<b>Mapping Local Drive</b>	Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions.										
<b>Mapping Local Serial Ports</b>	<p>Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions.</p> <p><b>NOTE:</b> <b>Mapping Local Serial Ports</b> is not available because US310e has no serial port.</p>										
<b>Mapping local Printers</b>	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions.										
Connection Settings											
Item	Description										
<b>Network Protocol</b>	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: <b>TCP/IP</b> , <b>TCP/IP + HTTP server location</b> , and <b>SSL/TLS + HTTPS server location</b> .										
<b>Audio Quality</b>	<p>Click the drop-down menu to disable audio playback or to configure the quality setting for audio playback in a Citrix ICA session. Four options are available: <b>High - high definition audio</b>, <b>Medium - optimized for speech</b>, <b>Low - for low-speed connections</b>, and <b>Off</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>High - high definition audio</b></td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr> <tr> <td><b>Medium - optimized for speech</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr> <tr> <td><b>Low - for low-speed connections</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr> <tr> <td><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr> </table>	Option	Description	<b>High - high definition audio</b>	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.	<b>Medium - optimized for speech</b>	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.	<b>Low - for low-speed connections</b>	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.	<b>Off</b>	Disables audio playback in opened ICA sessions.
Option	Description										
<b>High - high definition audio</b>	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.										
<b>Medium - optimized for speech</b>	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.										
<b>Low - for low-speed connections</b>	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.										
<b>Off</b>	Disables audio playback in opened ICA sessions.										
<b>Encryption</b>	Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic</b> , <b>RC5 128 bit (login only)</b> , <b>RC5 40 bit</b> , <b>RC5 56 bit</b> , <b>RC5 128 bit</b> .										
<b>Apply Windows key combinations (Ex. Alt + Tab keys)</b>	<p>Click the drop-down menu to select where to apply Windows key combinations.</p> <p>Three options are available: <b>On the local desktop</b>, <b>On the remote desktop</b>, <b>In full screen desktops only</b>.</p>										

### 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										
<b>Session Name</b>	Type in the name for Citrix ICA sessions.										
<b>Connection Type</b>	<p>This table only provides descriptions for available settings when <b>XenApp</b> is selected. Four connection types are available:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Web Logon</b></td><td>Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).</td></tr> <tr> <td><b>XenDesktop</b></td><td>Provides desktop delivery services.</td></tr> <tr> <td><b>XenApp</b></td><td>Provides application delivery services.</td></tr> <tr> <td><b>Server Connection</b></td><td>Provides full server access services for administrators (XenApp servers only).</td></tr> </table>	Option	Description	<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).	<b>XenDesktop</b>	Provides desktop delivery services.	<b>XenApp</b>	Provides application delivery services.	<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).
Option	Description										
<b>Web Logon</b>	Provides application, desktop, and content access services through the interface of a Web browser (Internet Explorer).										
<b>XenDesktop</b>	Provides desktop delivery services.										
<b>XenApp</b>	Provides application delivery services.										
<b>Server Connection</b>	Provides full server access services for administrators (XenApp servers only).										
<b>Server Address</b>	Type in the IP address and FQDN of the server through which XenApp is accessible.										
<b>Username</b>	Type in the user/account name used for authentication.										
<b>Password</b>	Type in the password of the user account used for authentication.										
<b>Domain</b>	<p>Type in the domain of the server.</p> <p><b>NOTE:</b> Type in the full computer/server name if your XenApp server doesn't belong to any domain.</p>										
<b>Application Name</b>	<p>Type in the application name.</p> <p><b>NOTE:</b> You can use the Search icon (  ) in front of the field to discover available applications. For detailed instructions, see Chapter 4, "5.6.3 Connection Type: XenApp".</p>										
Common Settings											
Item	Description										
<b>Autostart When Startup</b>	<p>Select whether to open a Citrix ICA session automatically or not when US310e starts.</p> <p>If <b>Yes</b> is selected, every time when you log in to the system, the Citrix ICA session will be opened automatically.</p>										
<b>On Application Exit</b>	<p>Select what to do when a Citrix ICA session is ended. Four options are available: <b>Do nothing</b>, <b>Restart Application</b>, <b>Reboot</b>, and <b>Shutdown</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>Do nothing</b></td><td>Returns to the Windows Embedded desktop.</td></tr> <tr> <td><b>Restart Application</b></td><td>Opens a Citrix ICA session again.</td></tr> <tr> <td><b>Reboot</b></td><td>Restarts your thin client.</td></tr> <tr> <td><b>Shutdown</b></td><td>Turns off your thin client.</td></tr> </table>	Option	Description	<b>Do nothing</b>	Returns to the Windows Embedded desktop.	<b>Restart Application</b>	Opens a Citrix ICA session again.	<b>Reboot</b>	Restarts your thin client.	<b>Shutdown</b>	Turns off your thin client.
Option	Description										
<b>Do nothing</b>	Returns to the Windows Embedded desktop.										
<b>Restart Application</b>	Opens a Citrix ICA session again.										
<b>Reboot</b>	Restarts your thin client.										
<b>Shutdown</b>	Turns off your thin client.										

## Options Sub-tab

Window Settings											
Item	Description										
<b>Requested Color Quality</b>	<p>Click the drop-down menu to select the desired color quality for a Citrix ICA session.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>No preference</b></td><td>No preference for a specific color quality.</td></tr> <tr> <td><b>Better Speed (16-bit)</b></td><td>The 16-bit color quality is used for better display speed.</td></tr> <tr> <td><b>Better Appearance (32-bit)</b></td><td>The 32-bit color quality is used for better desktop appearance.</td></tr> </table>	Option	Description	<b>No preference</b>	No preference for a specific color quality.	<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.	<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.		
Option	Description										
<b>No preference</b>	No preference for a specific color quality.										
<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.										
<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.										
<b>Window Size</b>	<p>Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: <b>Default</b>, <b>Seamless</b>, <b>Full Screen</b>, <b>640 x 480</b>, <b>800 x 600</b>, <b>1024 x 768</b>, <b>1280 x 1024</b>, and <b>1600 x 1200</b>.</p> <p><b>NOTE:</b> When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size.</p> <p><b>NOTE:</b> For more information about how to disable the XenDesktop toolbar, visit Citrix websites at <a href="http://support.citrix.com">support.citrix.com</a> or <a href="http://www.citrix.com">www.citrix.com</a> for online help.</p> <p><b>NOTE:</b> In case that you don't want to disable the toolbar, you can use the toolbar or your mouse to resize the launched window if needed.</p>										
Device Mapping											
Item	Description										
<b>Mapping Local Drive</b>	Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.										
<b>Mapping Local Serial Ports</b>	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. <b>NOTE: Mapping Local Serial Ports</b> is not available because US310e has no serial port.										
<b>Mapping local Printers</b>	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions through this connection.										
Connection Settings											
Item	Description										
<b>Network Protocol</b>	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: <b>TCP/IP</b> , <b>TCP/IP + HTTP server location</b> , and <b>SSL/TLS + HTTPS server location</b> .										
<b>Audio Quality</b>	<p>Click the drop-down menu to disable audio playback or to configure the quality setting for audio playback in a Citrix ICA session. Four options are available: <b>High - high definition audio</b>, <b>Medium - optimized for speech</b>, <b>Low - for low-speed connections</b>, and <b>Off</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>High - high definition audio</b></td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr> <tr> <td><b>Medium - optimized for speech</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr> <tr> <td><b>Low - for low-speed connections</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr> <tr> <td><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr> </table>	Option	Description	<b>High - high definition audio</b>	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.	<b>Medium - optimized for speech</b>	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.	<b>Low - for low-speed connections</b>	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.	<b>Off</b>	Disables audio playback in opened ICA sessions.
Option	Description										
<b>High - high definition audio</b>	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.										
<b>Medium - optimized for speech</b>	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.										
<b>Low - for low-speed connections</b>	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.										
<b>Off</b>	Disables audio playback in opened ICA sessions.										
<b>Encryption</b>	Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic</b> , <b>RC5 128 bit (login only)</b> , <b>RC5 40 bit</b> , <b>RC5 56 bit</b> , <b>RC5 128 bit</b> .										
<b>Apply Windows key combinations (Ex. Alt + Tab key)</b>	Click the drop-down menu to select where to apply Windows key combinations. Three options are available: <b>On the local desktop</b> , <b>On the remote desktop</b> , <b>In full screen desktops only</b> .										

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

## Options Sub-tab

Window Settings											
Item	Description										
<b>Requested Color Quality</b>	<p>Click the drop-down menu to select the desired color quality for a Citrix ICA session. Three options are available: <b>No preference</b>, <b>Better Speed (16-bit)</b>, and <b>Better Appearance (32-bit)</b>.</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>No preference</b></td><td>No preference in a specific color quality.</td></tr> <tr> <td><b>Better Speed (16-bit)</b></td><td>The 16-bit color quality is used for better display speed.</td></tr> <tr> <td><b>Better Appearance (32-bit)</b></td><td>The 32-bit color quality is used for better desktop appearance.</td></tr> </table>	Option	Description	<b>No preference</b>	No preference in a specific color quality.	<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.	<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.		
Option	Description										
<b>No preference</b>	No preference in a specific color quality.										
<b>Better Speed (16-bit)</b>	The 16-bit color quality is used for better display speed.										
<b>Better Appearance (32-bit)</b>	The 32-bit color quality is used for better desktop appearance.										
<b>Window Size</b>	<p>Click the drop-down menu to select the desired window size of a Citrix ICA session. Eight options are available: <b>Default</b>, <b>Seamless</b>, <b>Full Screen</b>, <b>640 x 480</b>, <b>800 x 600</b>, <b>1024 x 768</b>, <b>1280 x 1024</b>, and <b>1600 x 1200</b>.</p> <p><b>NOTE:</b> When the XenDesktop toolbar is enabled on the server side, you may not be able to change the window size.</p> <p><b>NOTE:</b> For more information about how to disable the XenDesktop toolbar, visit Citrix websites at <a href="http://support.citrix.com">support.citrix.com</a> or <a href="http://www.citrix.com">www.citrix.com</a> for online help.</p> <p><b>NOTE:</b> In case that you don't want to disable the toolbar, you can use the toolbar or your mouse to resize the launched window if needed.</p>										
Device Mapping											
Item	Description										
<b>Mapping Local Drive</b>	Click the drop-down menu to enable/disable the mapping of the local drive(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached drive(s) will become available in launched Citrix ICA sessions through this connection.										
<b>Mapping Local Serial Ports</b>	Click the drop-down menu to enable/disable the mapping of the local serial device(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached serial device(s) will become available in launched Citrix ICA sessions. <b>NOTE:</b> <b>Mapping Local Serial Ports</b> is not available because US310e has no serial port.										
<b>Mapping local Printers</b>	Click the drop-down menu to enable/disable the mapping of the local printer(s) in a Citrix ICA session. If <b>Yes</b> is selected, the locally attached printer(s) will become available in launched Citrix ICA sessions through this connection.										
Connection Settings											
Item	Description										
<b>Network Protocol</b>	Click the drop-down menu to select the protocol(s) used for connection. Three options are available: <b>TCP/IP</b> , <b>TCP/IP + HTTP server location</b> , and <b>SSL/TLS + HTTPS server location</b> .										
<b>Audio Quality</b>	<p>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:</p> <table> <tr> <th>Option</th><th>Description</th></tr> <tr> <td><b>High - high definition audio</b></td><td>Allows endpoint devices to play a sound file at its native data transfer rate. This is recommended for connections where bandwidth is plentiful and sound quality is important.</td></tr> <tr> <td><b>Medium - optimized for speech</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 64Kbps, resulting in a moderate decrease in the quality of the sound. This option is suitable for speeches and recommended for most LAN-based connections.</td></tr> <tr> <td><b>Low - for low-speed connections</b></td><td>Compresses any sounds sent to endpoint devices to a maximum of 16Kbps, resulting in a significant decrease in the quality of the sound. This option is suitable for low-bandwidth connections, allowing reasonable audio performance during a low-speed connection.</td></tr> <tr> <td><b>Off</b></td><td>Disables audio playback in opened ICA sessions.</td></tr> </table>	Option	Description	<b>High - high definition audio</b>	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.	<b>Medium - optimized for speech</b>	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.	<b>Low - for low-speed connections</b>	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.	<b>Off</b>	Disables audio playback in opened ICA sessions.
Option	Description										
<b>High - high definition audio</b>	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.										
<b>Medium - optimized for speech</b>	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.										
<b>Low - for low-speed connections</b>	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.										
<b>Off</b>	Disables audio playback in opened ICA sessions.										
<b>Encryption</b>	Click the drop-down menu to select the desired encryption method. Five options are available: <b>Basic</b> , <b>RC5 128 bit (login only)</b> , <b>RC5 40 bit</b> , <b>RC5 56 bit</b> , <b>RC5 128 bit</b> .										
<b>Apply Windows key combinations (Ex. Alt + Tab keys)</b>	Click the drop-down menu to select where to apply Windows key combinations. Three options are available: <b>On the local desktop</b> , <b>On the remote desktop</b> , <b>In full screen desktops only</b> .										

## 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

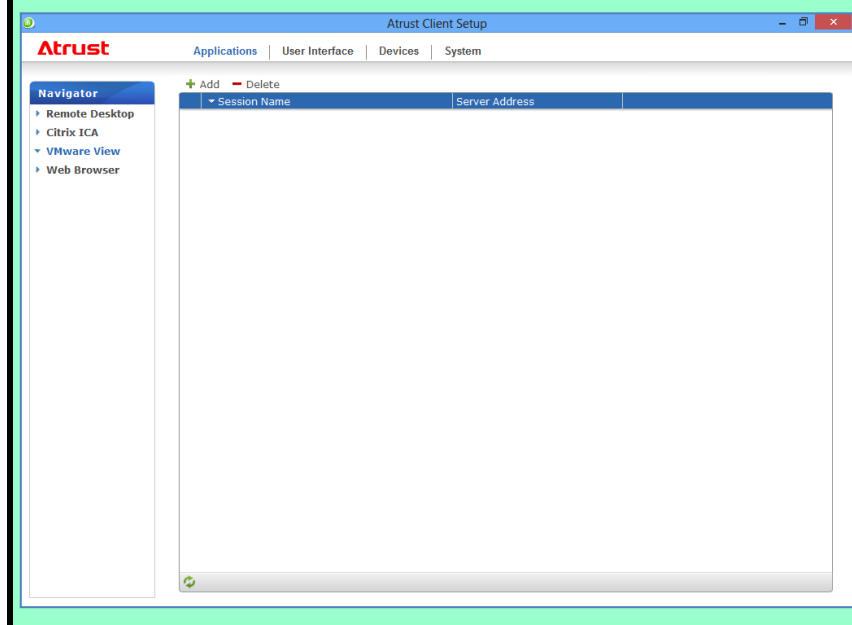
- For more information on VMware desktop virtualization solutions, visit VMware website at [www.vmware.com](http://www.vmware.com).
- You can also access VMware View or Horizon View services through the standard desktop shortcut **VMware Horizon View Client**. For detailed instructions on how to access 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 any entry, the View Connection list will be empty.



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

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

The screenshot shows the 'Atrust Client Setup' window with the 'General' tab selected. The 'Navigator' on the left lists 'Remote Desktop', 'Citrix ICA', 'VMware View' (selected), and 'Web Browser'. The main area is divided into three sections: 'Server Settings', 'Login Settings', and 'Common Settings'. 'Server Settings' includes 'Session Name' (a text field with a red asterisk), 'Connection Server', 'Port', a checked 'Use secure connection (SSL)' checkbox, and a 'Certificate checking mode' dropdown set to 'Warn before connecting to untrusted server'. 'Login Settings' includes a 'Log in as current user' checkbox, and fields for 'User Name', 'Password', 'Domain Name', 'Desktop Name', and 'Display Protocol' (set to 'Manual'). 'Common Settings' includes 'Autostart When Startup' (set to 'No') and 'On Application Exit' (set to 'Do Nothing'). 'Save' and 'Cancel' buttons are at the bottom.

**Note**

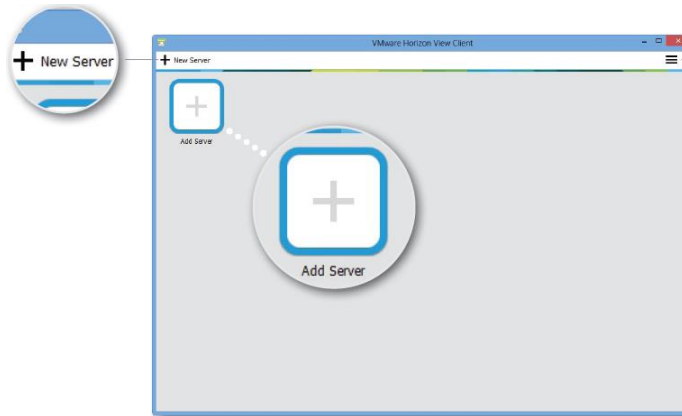
This is the only required field for the creation of a service access shortcut on the desktop. Other data can be provided during the period of service access. Depending on your needs, you might choose to type in more other data.

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

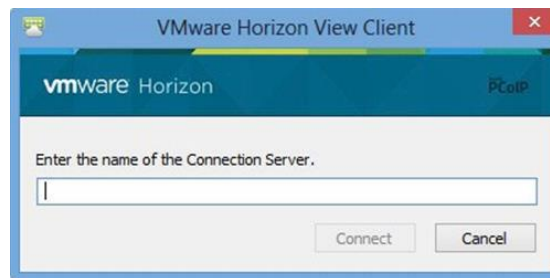
## 5.10 Accessing VMware View or Horizon View Services

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**.

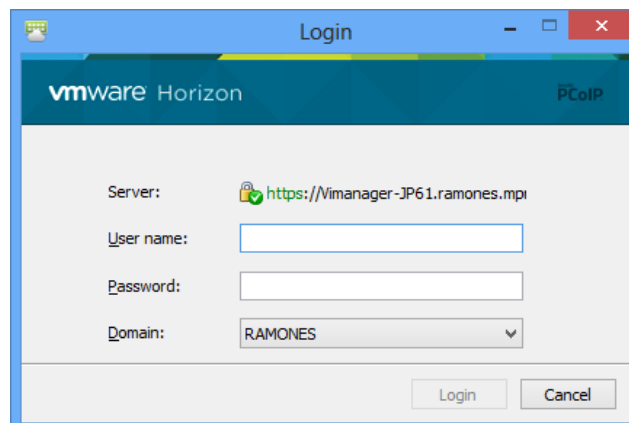


5. By default, a secure connection (HTTPS) is required to connect to the View Connection server. You therefore need to import a certificate.

### Note

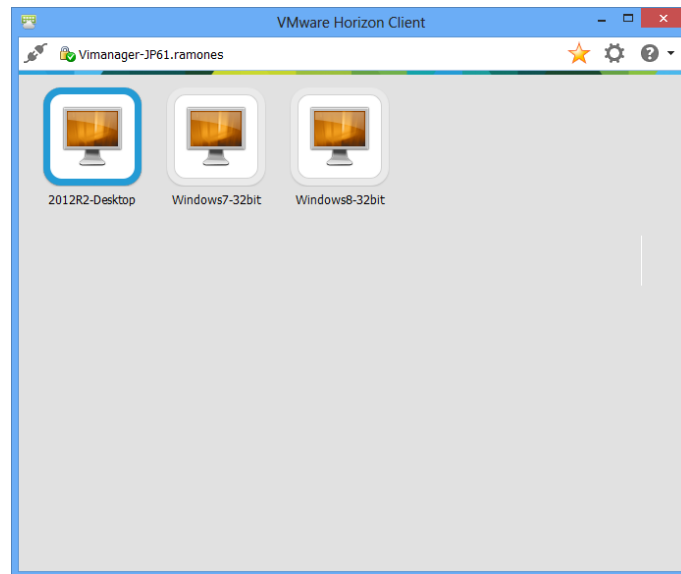
For how to import a certificate, see Chapter 5, "16. Saving the Certificate".

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								
<b>Session Name</b>	Type in the name for VMware View or Horizon View sessions.								
<b>Connection Server</b>	Type in the computer name or IP address of the View Connection Server. <b>NOTE:</b> For more information on View Connection Server, visit VMware website at <a href="http://www.vmware.com">www.vmware.com</a> .								
<b>Port</b>	Type in the port number used to communicate with the View Connection Server. To use the default value, simply leave it blank.								
<b>Use secure connection (SSL)</b>	Check/Uncheck to enable/disable secure connection.								
<b>Certificate checking mode</b>	Click to select whether to verify the identity of the remote server and whether to connect to an untrusted server. Three options are available: <b>Do not verify server identity certificates</b> , <b>Warn before connecting to untrusted servers</b> , and <b>Never connect to untrusted servers</b> . <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>Do not verify server identity certificates</b></td><td>Do not verify the identity of the remote server and connect to it anyway.</td></tr> <tr> <td><b>Warn before connecting to untrusted servers</b></td><td>Warns and allows users to choose whether to connect or not.</td></tr> <tr> <td><b>Never connect to untrusted servers</b></td><td>Disallows untrusted connections.</td></tr> </tbody> </table>	Option	Description	<b>Do not verify server identity certificates</b>	Do not verify the identity of the remote server and connect to it anyway.	<b>Warn before connecting to untrusted servers</b>	Warns and allows users to choose whether to connect or not.	<b>Never connect to untrusted servers</b>	Disallows untrusted connections.
Option	Description								
<b>Do not verify server identity certificates</b>	Do not verify the identity of the remote server and connect to it anyway.								
<b>Warn before connecting to untrusted servers</b>	Warns and allows users to choose whether to connect or not.								
<b>Never connect to untrusted servers</b>	Disallows untrusted connections.								
Login Settings									
Item	Description								
<b>Log in as current user</b>	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.								
<b>User Name</b>	Type in the user name for authentication.								
<b>Password</b>	Type in the password for authentication.								
<b>Domain Name</b>	Type in the domain name of the View Connection Server.								
<b>Desktop Name</b>	Type in the desktop name. Or, leave it blank for users to select one. <b>NOTE:</b> If <b>Manual</b> is selected for the Display Protocol field below, this field will be grayed out.								
<b>Display Protocol</b>	Click the drop-down menu to select the display protocol. Three options are available: <b>Manual</b> , <b>Microsoft RDP</b> , and <b>PCoIP</b> . <table border="1"> <thead> <tr> <th>Option</th><th>Description</th></tr> </thead> <tbody> <tr> <td><b>Manual</b></td><td>Manually select the desired display protocol.</td></tr> <tr> <td><b>Microsoft RDP</b></td><td>Use Microsoft RDP as the display protocol.</td></tr> <tr> <td><b>PCoIP</b></td><td>Use VMware PCoIP as the display protocol.</td></tr> </tbody> </table>	Option	Description	<b>Manual</b>	Manually select the desired display protocol.	<b>Microsoft RDP</b>	Use Microsoft RDP as the display protocol.	<b>PCoIP</b>	Use VMware PCoIP as the display protocol.
Option	Description								
<b>Manual</b>	Manually select the desired display protocol.								
<b>Microsoft RDP</b>	Use Microsoft RDP as the display protocol.								
<b>PCoIP</b>	Use VMware PCoIP as the display protocol.								

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

**Options Sub-tab**

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

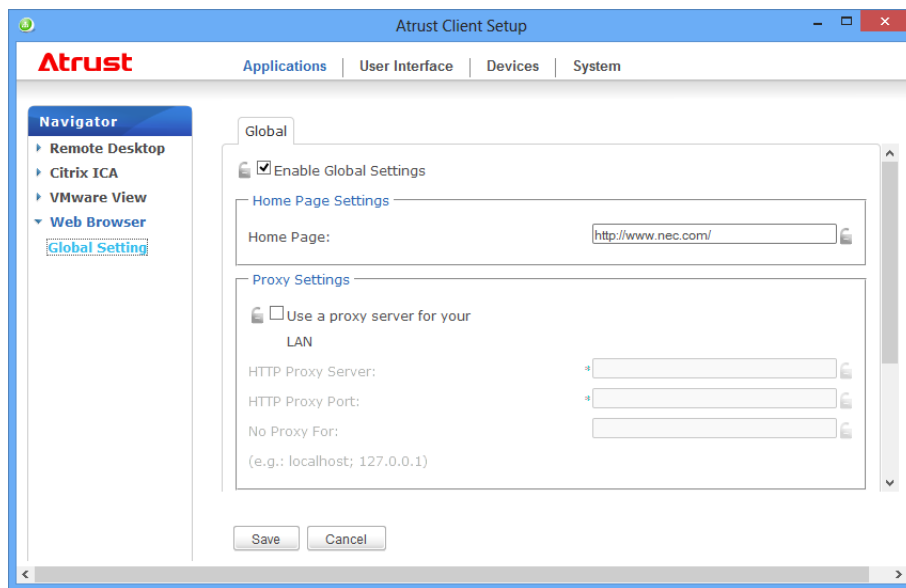
## 5.12 Configuring Web Browser Settings

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.

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

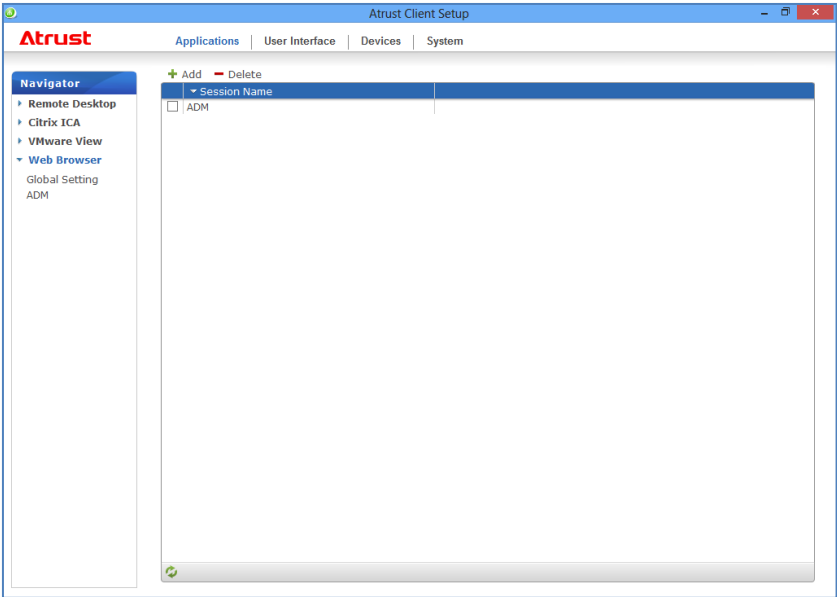
### 5.12.2 Configuring Specific Browser Session Settings

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.

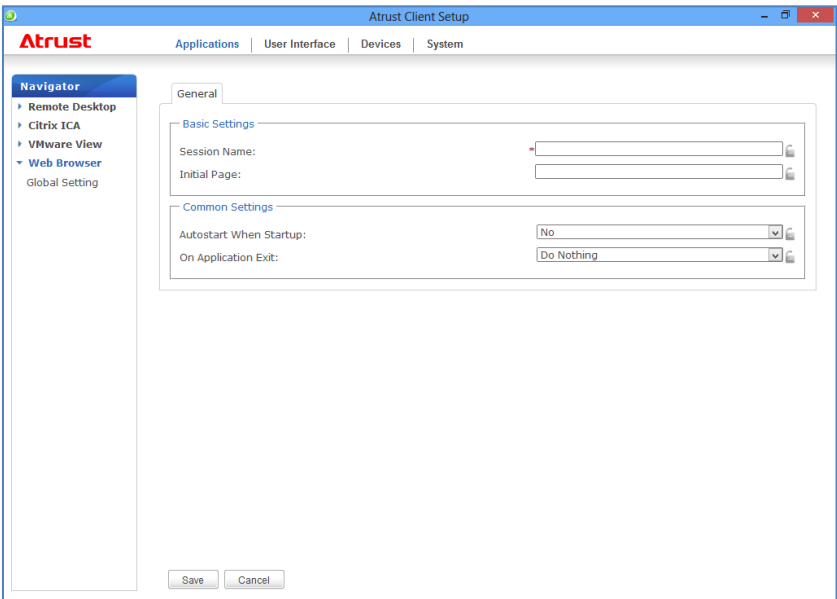
- 1. On Atrust Client Setup, click **Applications > Web Browser**.
- 2. The Browser Session list appears in the Configuration area.



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).



General Settings											
Item	Description										
Session Name	Specify the browser session name.										
Initial Page	Specify the URL of the page that opens when the browser session starts.										
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: <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>	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.
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.

---

## **Chapter 5 Administrative Utilities and Settings**

---

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

- 1. Launching UWF Automatically**  
Describes utilities to be launched automatically.
- 2. Utilities Affected by Shutdown and Restart**  
Describes utilities that are affected by shutdown or restart.
- 3. Using the Unified Write Filter (UWF)**  
Describes details of UWF (Unified Write Filter), system change under UWF environment, and UWF command line options.
- 4. Automatic Sign-In**  
Describes how to configure automatic sign-in.
- 5. Saving Files and Using Local Drives**  
Describes how to save files and how to use local drives.
- 6. 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. Setting up a Wireless Local Area Network (LAN)**  
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".

---

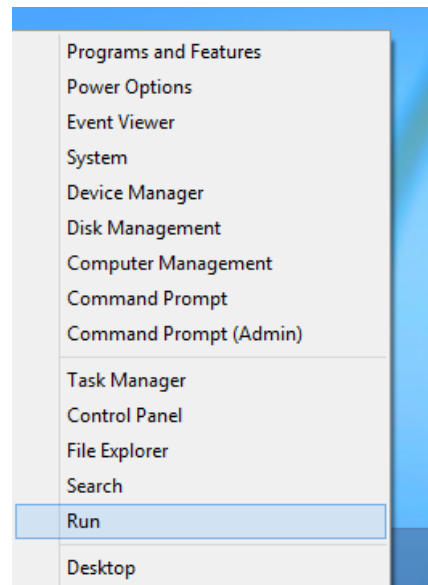
## 4. Automatic Sign-In

---

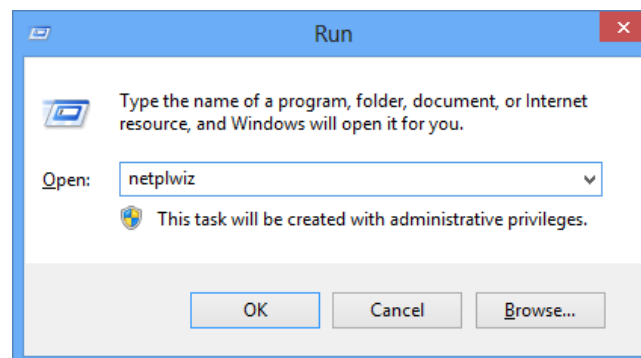
On US310e, the workgroup computers are configured to automatically sign-in with the default User account. If the default password is changed, auto sign-in password must also be changed in the following procedure:

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

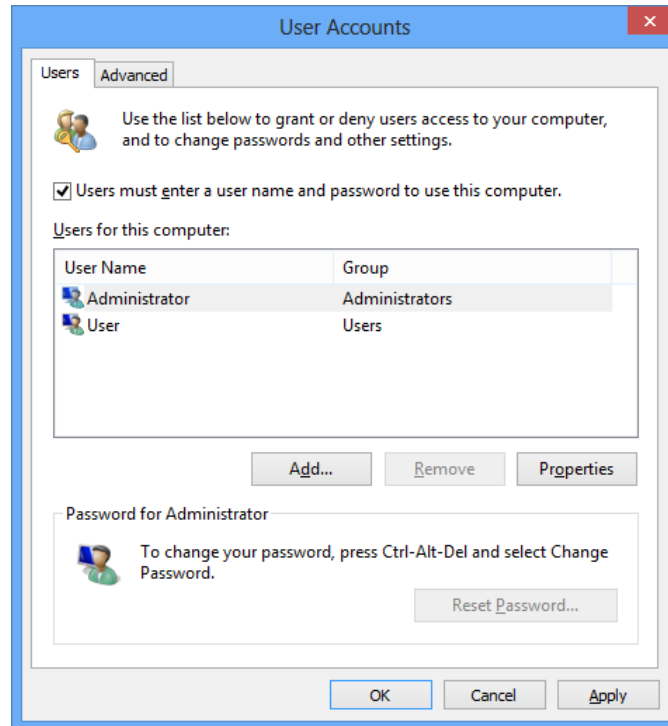
1. Sign in as an Administrator.
2. Click **Run** on the Start menu.



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

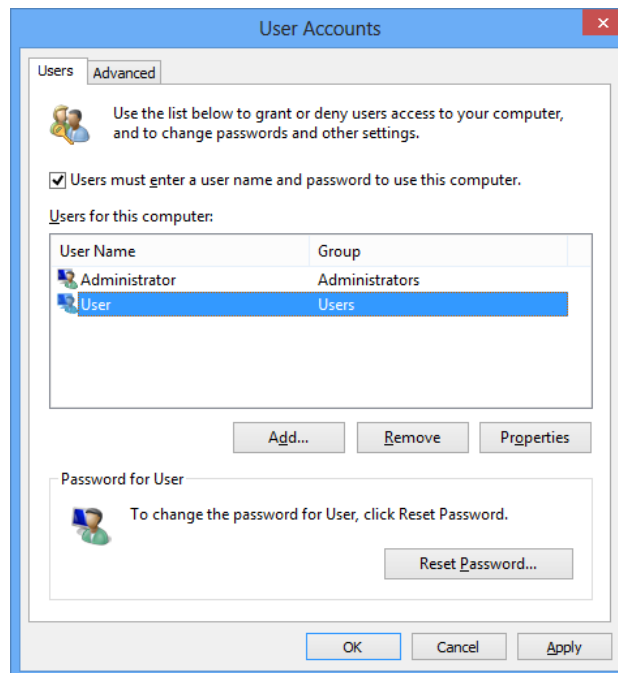


4. Click the **Users** tab in the **User Accounts** dialog box, and select the **Users must enter a user name and password to use this computer** check box.



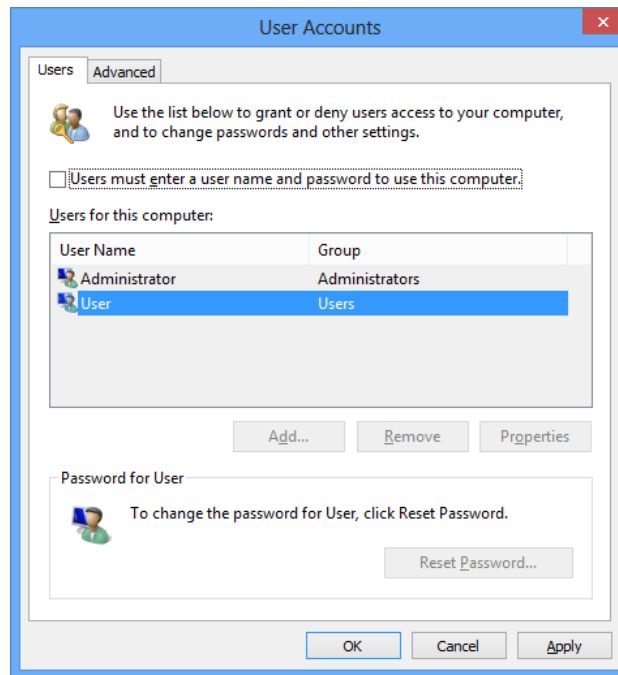
5. Select the name of the user for which you want to configure auto sign-in from the list of users.

\* As an example, select the User account.

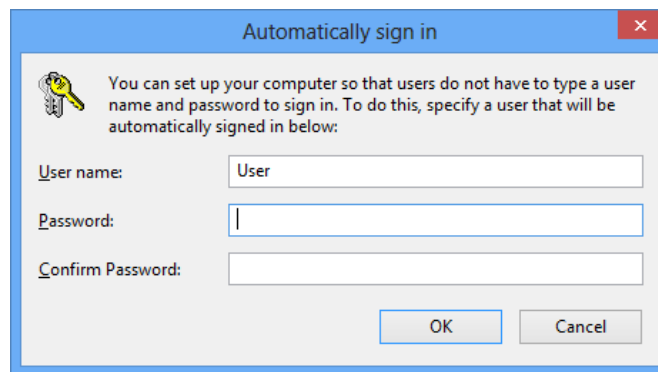




6. Clear the **Users must enter a user name and password to use this computer** checkbox, and click **OK**.



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. Sign 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.

# 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.
- CMO Terminal Agent cannot be downgraded by performing an overwrite install. To downgrade CMO Terminal Agent, uninstall the new version of CMO Terminal Agent and then install the old version of CMO Terminal Agent.

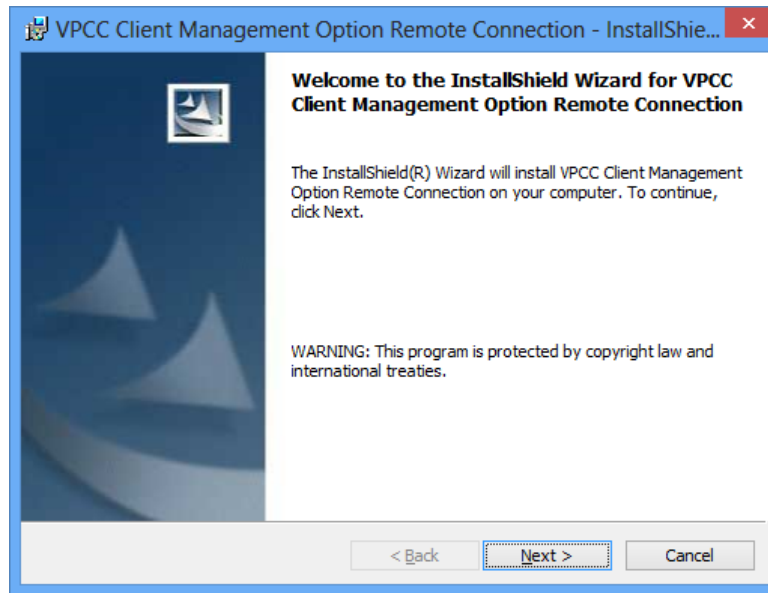
The table below shows the compatibility between the CMO Terminal Agent and server component versions (CMO Configuration Console, CMO Manager, CMO Manager Extension Pack, CMO Connector, and CMO Command).

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

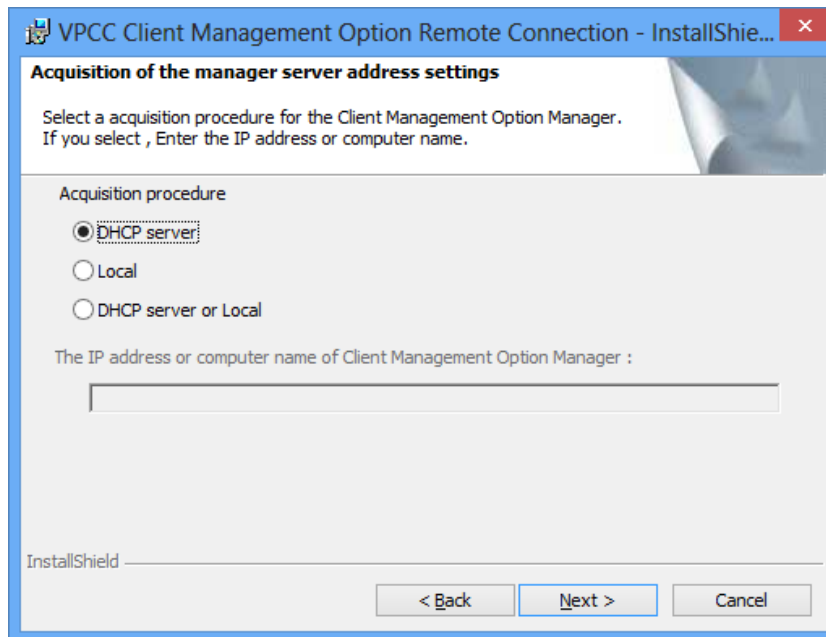
Install CMO Terminal Agent as follows:

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**.

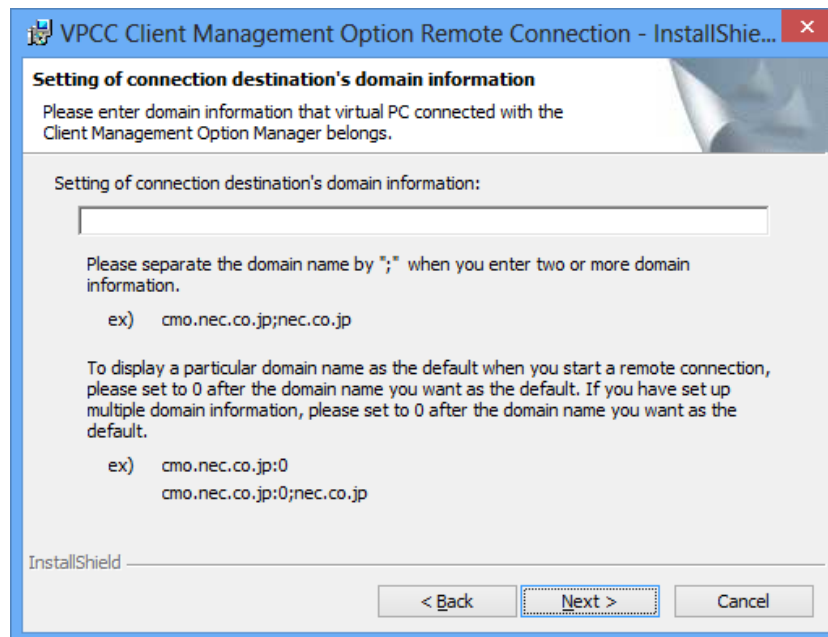


4. Select the method for obtaining Client Management Option Manager that is appropriate for your environment, and then click **Next**.

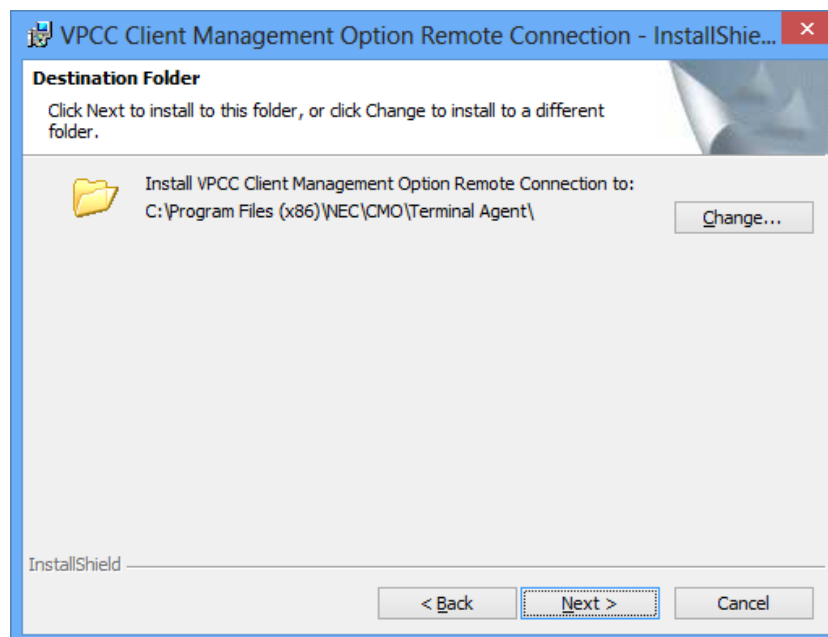


5. Type in the domain information, and then click **Next**.

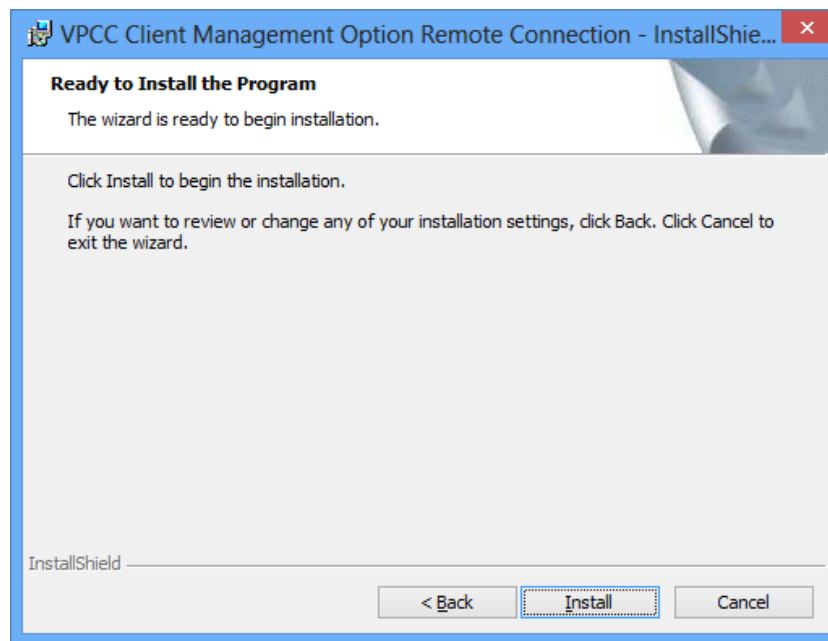
\* If you selected **DHCP Server** in step 4, this step is skipped.



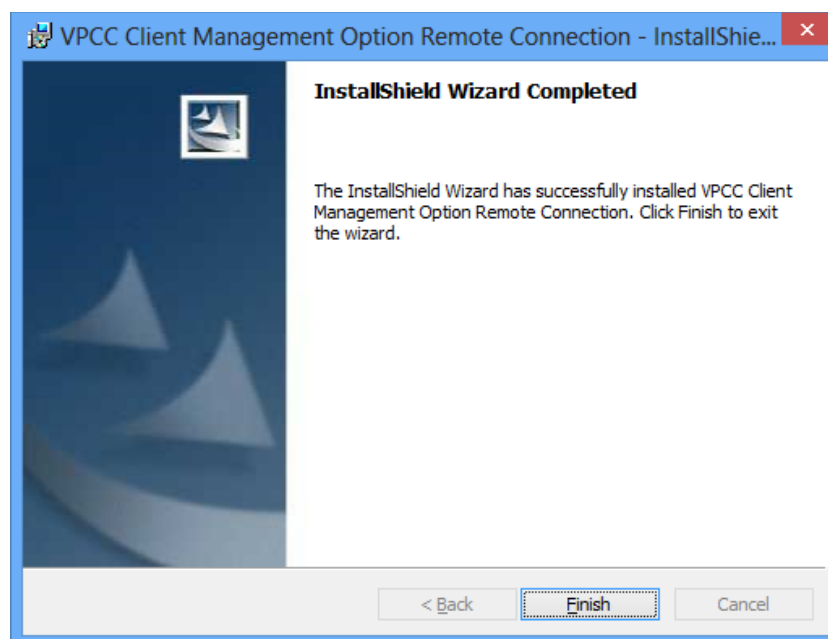
6. Specify the installation folder, and then click **Next**.



7. Click **Install**.



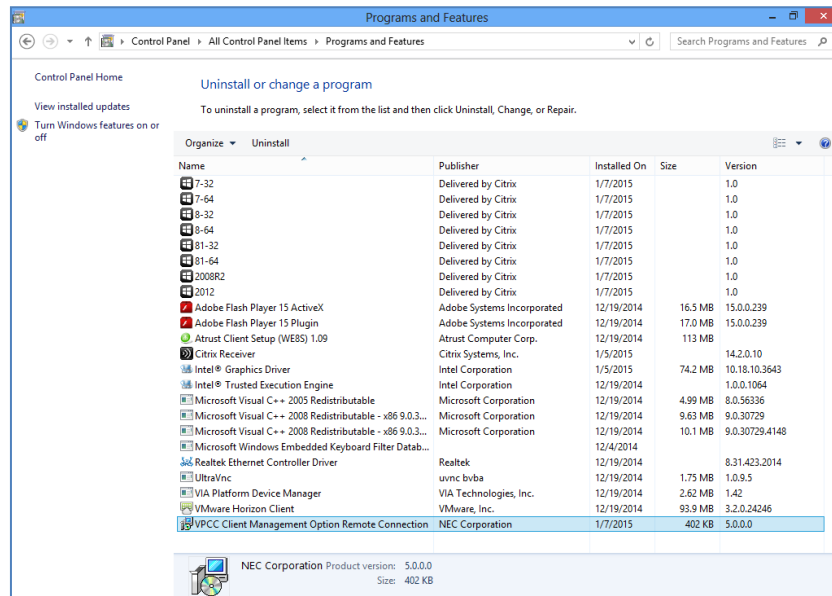
8. Click **Finish**.



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.

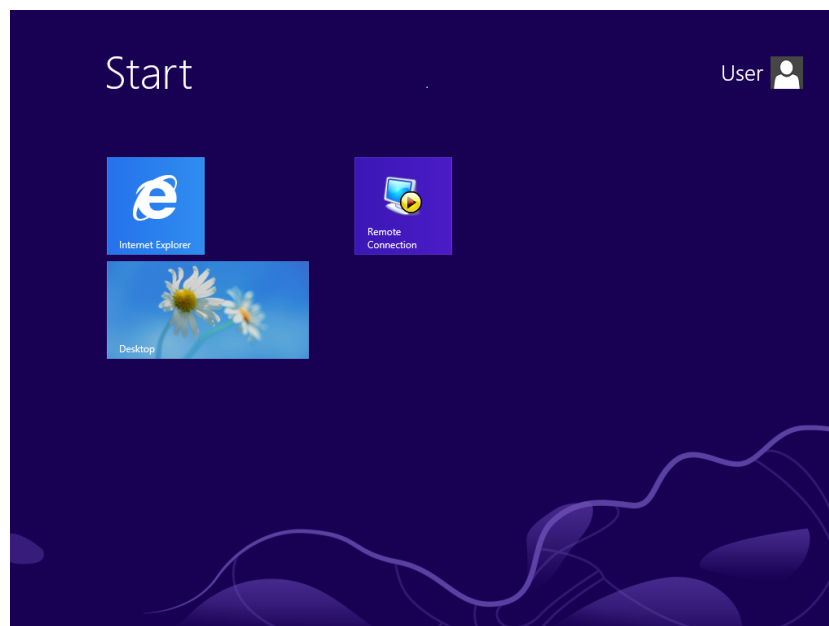
\* Also make sure the version of the installed CMO Terminal Agent is correct.



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. Setting up a Wireless Local Area Network (LAN)

---

The US310e wireless LAN model can be connected to a wireless LAN by connecting a USB wireless LAN adapter to the main unit.

To connect to a wireless LAN, wireless LAN connection settings must be configured in US310e.

You can connect to a wireless LAN by selecting a network (SSID) or by manually creating a network profile.

---

### 14.1 Selecting a Network (SSID) for Connection

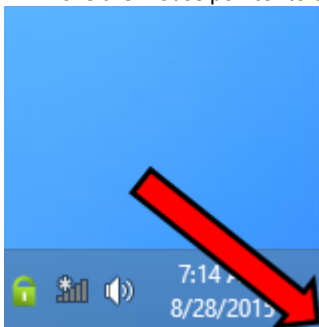
---

To select a network (SSID) for connection, do the following:

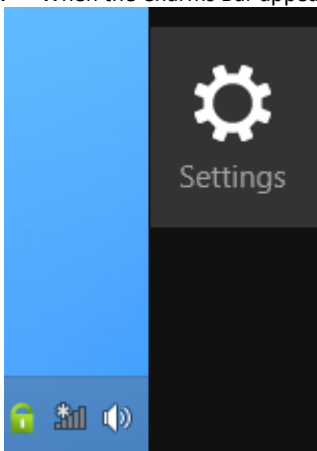
**Note**

You can use this procedure to connect to a wireless network within the service area. To create a profile for a wireless network outside of the service area or to connect to a network whose network name (SSID) is hidden by the stealth or other feature, manually create a network profile and connect to the network by referring to "14.2 Manually Creating a Network Profile for Connection" in this document.

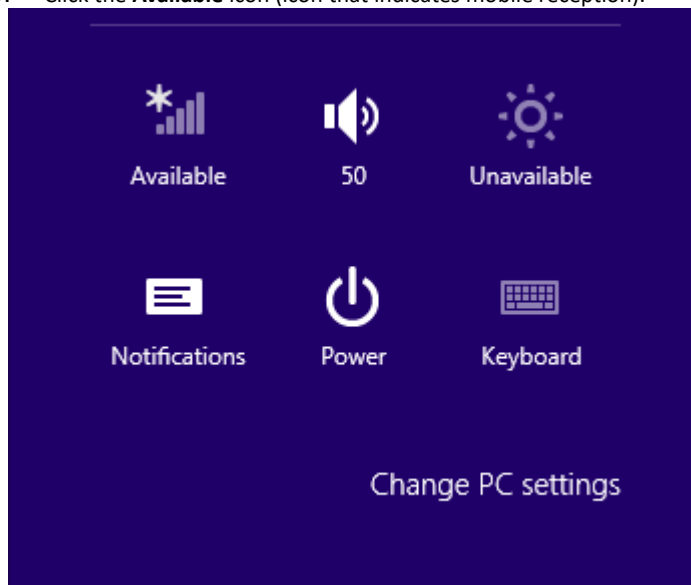
1. Move the mouse pointer to the bottom right corner of the desktop screen.



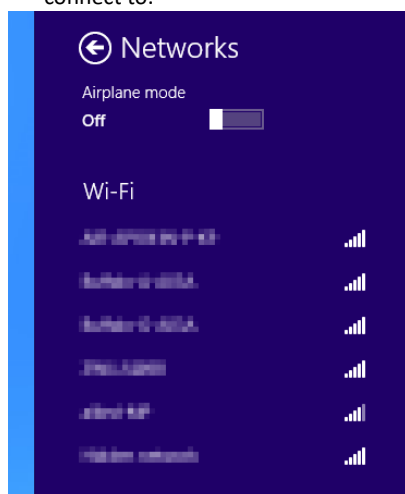
2. When the Charms Bar appears, click **Settings**.



3. Click the **Available** icon (icon that indicates mobile reception).



4. **Networks** and the available network names (SSIDs) are displayed. Click the name of the network you want to connect to.

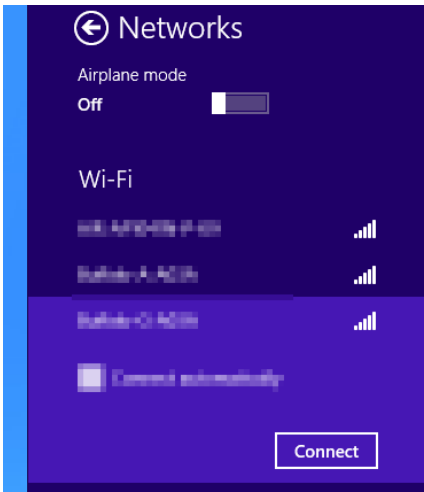




- 5. Click **Connect**.

Note

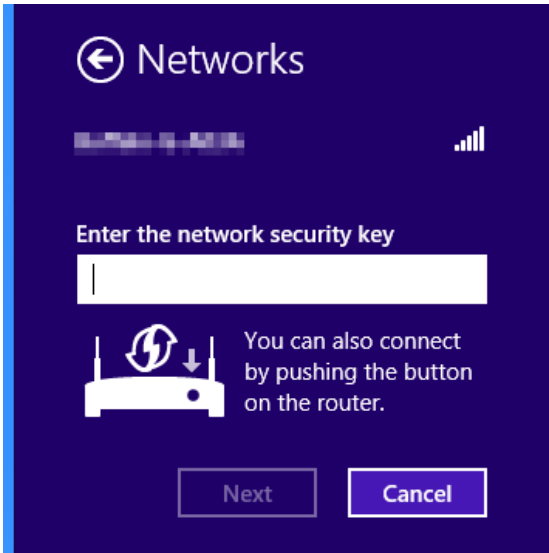
Check **Connect automatically** to always use this connection.



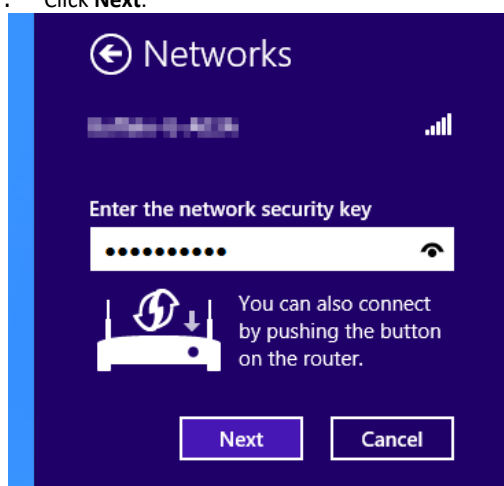
- 6. When **Enter the network security key** appears, enter the security key in the box.

Note

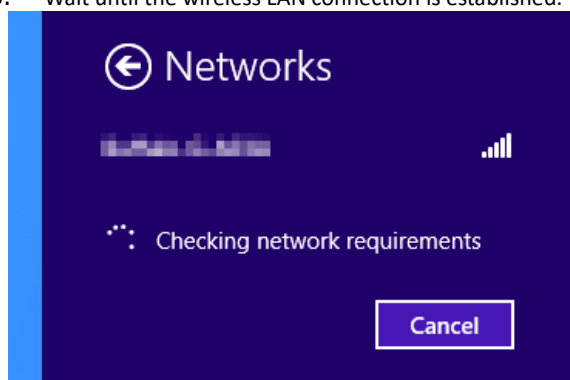
If **You can also connect by pushing the button on the router** is displayed, you can configure settings without having to enter the security key by pressing the button for connecting the wireless LAN device.  
  
Note that the connection button name differs depending on the wireless LAN device manufacturer (for example, "AOSS" or "WPS"). For the position of the button, setting procedures and other details, consult the manufacturer of your wireless LAN device.



7. Click **Next**.



8. Wait until the wireless LAN connection is established.

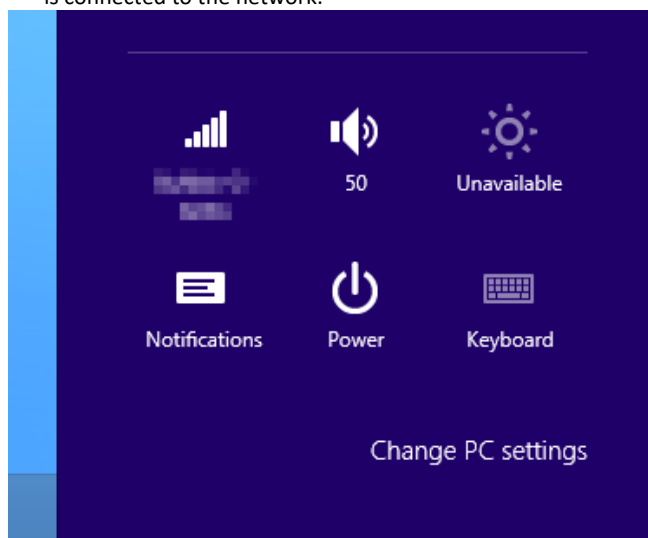


9. **Do you want to turn on sharing between PCs and connect to devices on this network?** may appear in some environments. Click the option appropriate for your network environment.

**Note**

- **No, don't turn on sharing and connect to devices**  
It is recommended not to enable sharing if you may connect to the network in public spaces when you are outside the office.
- **Yes, turn on sharing and connect to devices**  
You can enable sharing if you will only use a specific network at home or in the office or other private place.

10. Return to the **Settings** charm and confirm that the network name is displayed under the network icon and US310e is connected to the network.



---

## 14.2 Manually Creating a Network Profile for Connection

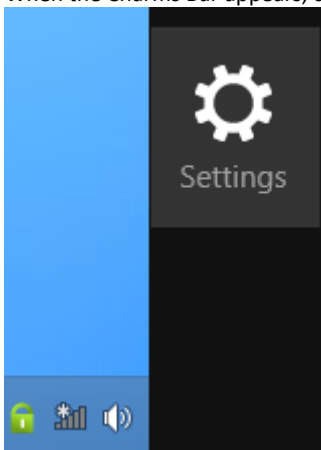
---

To manually create a network profile for connection, do the following:

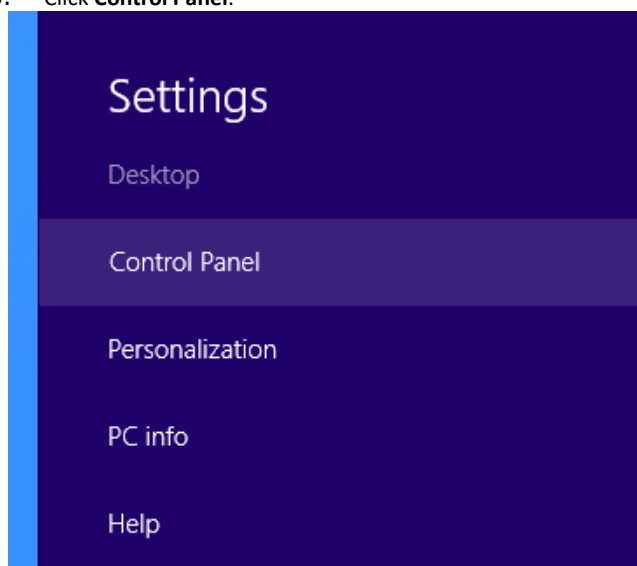
1. Move the mouse pointer to the bottom right corner of the desktop screen.



2. When the Charms Bar appears, click **Settings**.



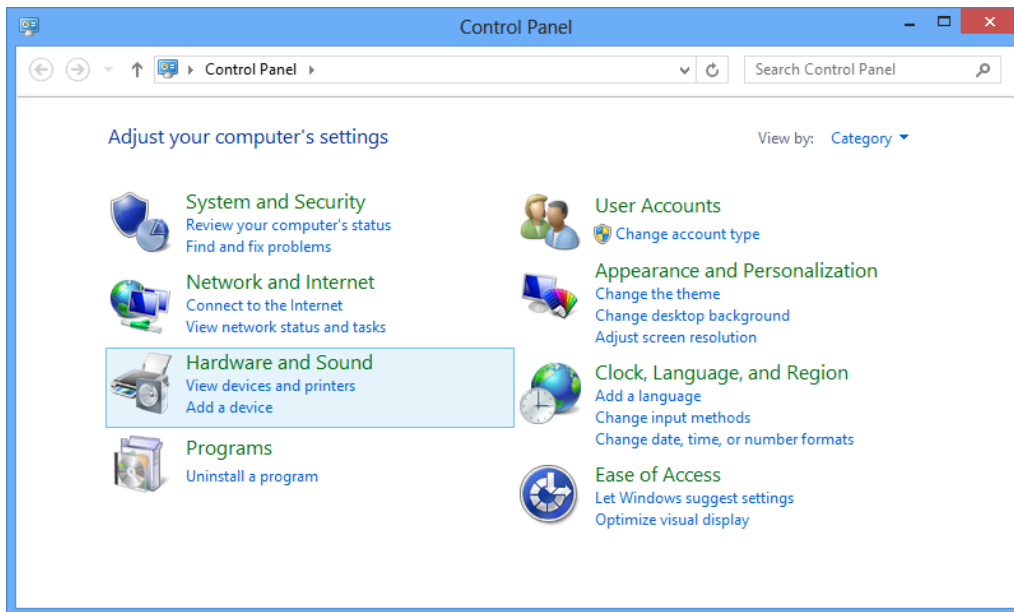
3. Click **Control Panel**.



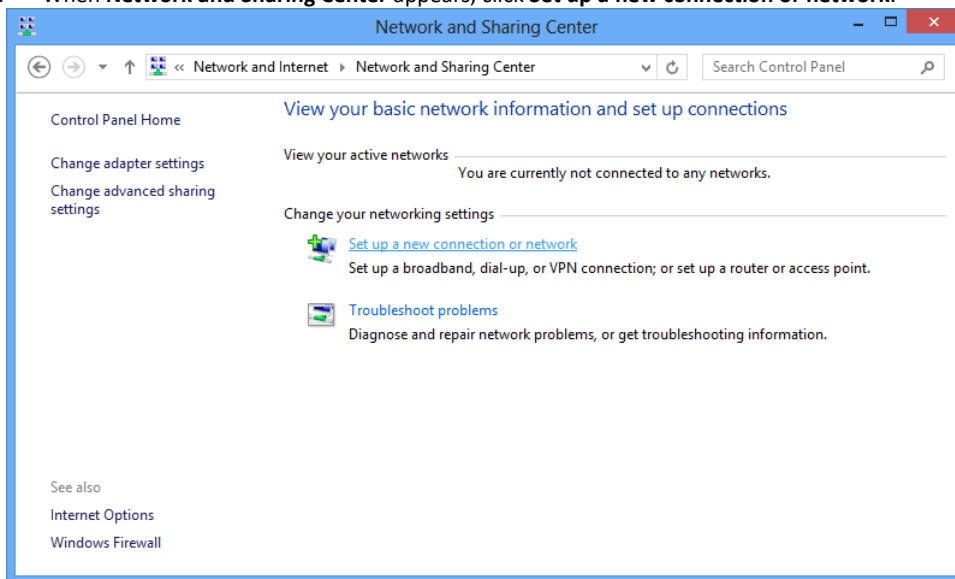
4. Click **View network status and tasks**.

**Note**

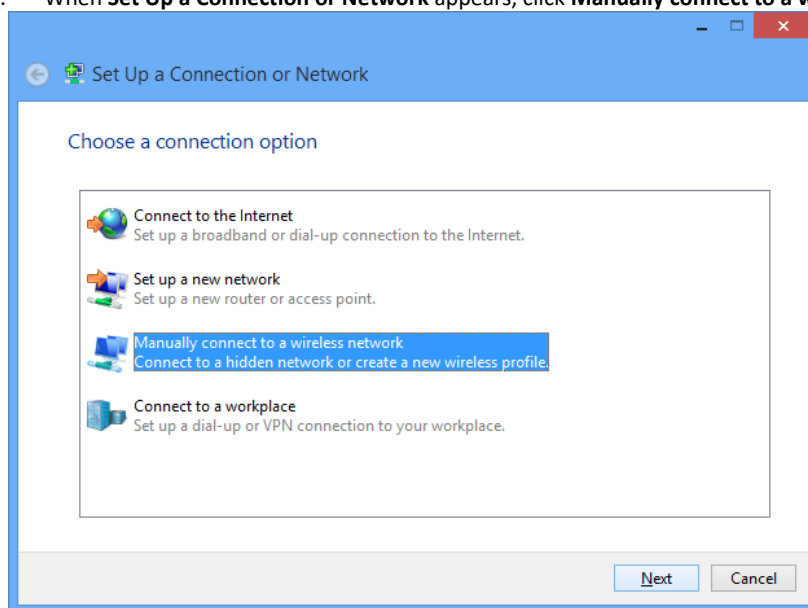
If **View by** is **Icon**, click **Network and Sharing Center**.



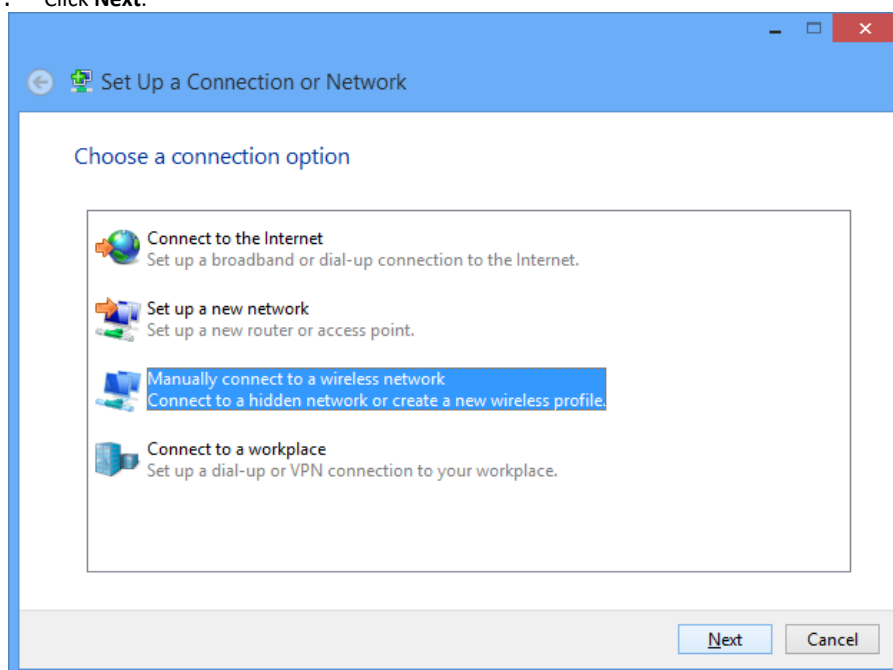
5. When **Network and Sharing Center** appears, click **Set up a new connection or network**.



6. When **Set Up a Connection or Network** appears, click **Manually connect to a wireless network**.



7. Click **Next**.



8. When **Manually connect to a wireless network** appears, enter information about the wireless network you want to add.

**Note**

- To always use this connection, check **Start this connection automatically**.
- When you check **Connect even if the network is not broadcasting**, the system tries to connect to a wireless LAN access point even if there is no reception from wireless LAN access points.
- The security type and the encryption type differ depending on your network settings. For the items you must enter, refer to the manual for your wireless LAN device and other relevant documentation.

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: WPA2-Personal

Encryption type: AES

Security Key:  ☐ Hide characters

☒ Start this connection automatically

☒ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

9. When you have completed entry, click **Next**.

Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name:

Security type: WPA2-Personal

Encryption type: AES

Security Key:  ☐ Hide characters

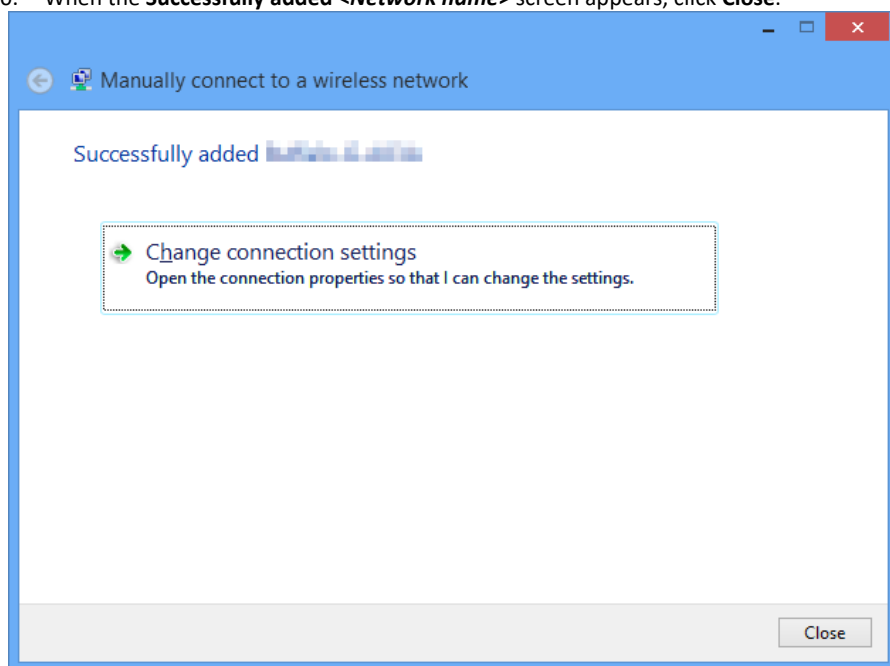
☒ Start this connection automatically

☒ Connect even if the network is not broadcasting

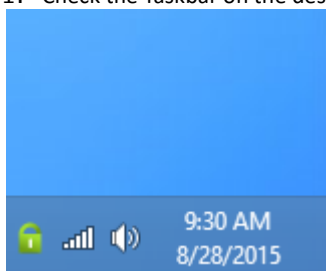
Warning: If you select this option, your computer's privacy might be at risk.

Next Cancel

10. When the **Successfully added <Network name>** screen appears, click **Close**.



11. Check the Taskbar on the desktop to confirm that US310e is connected to the network.





---

## 14.3 Managing a Network Profile

---

This section describes how to check, delete, or otherwise operate network profiles (SSIDs).

**Note**

The UI cannot be used to operate a profile for a wireless LAN that is outside the service area and that cannot be currently detected (such as a wireless LAN that you have connected to in the past), a wireless LAN profile that you have inadvertently created, or a wireless LAN profile whose information has been changed because you have changed the encryption or other settings on the main wireless device. In these cases, use the command prompt.

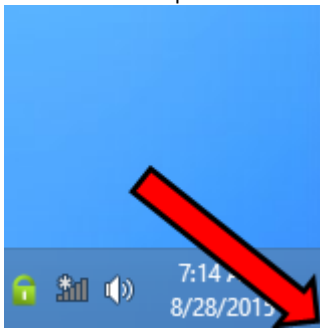
---

### 14.3.1 Checking a Network Profile (SSID)

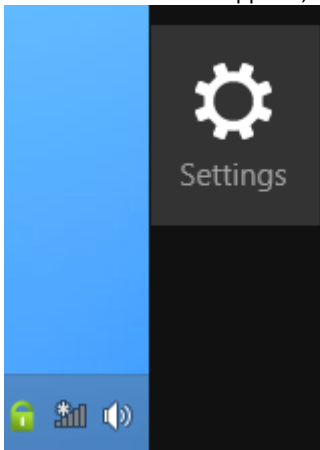
---

To check a network profile (SSID) or network security level, do the following:

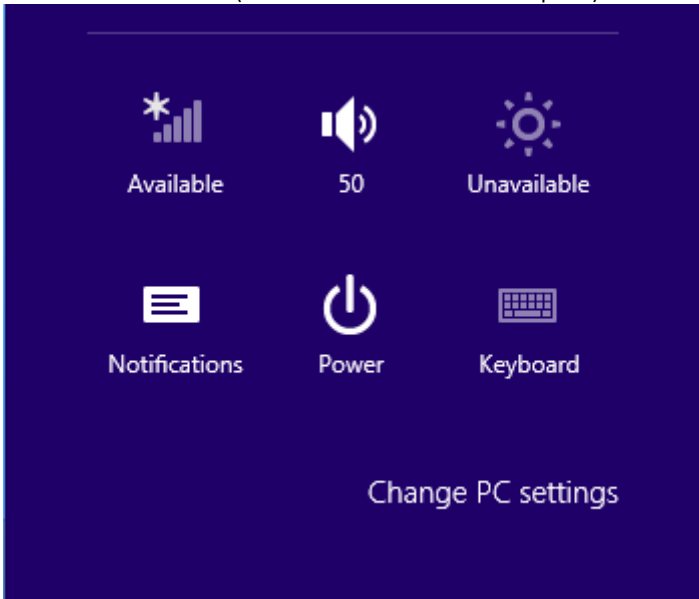
1. Move the mouse pointer to the bottom right corner of the desktop screen.



2. When the Charms Bar appears, click **Settings**.



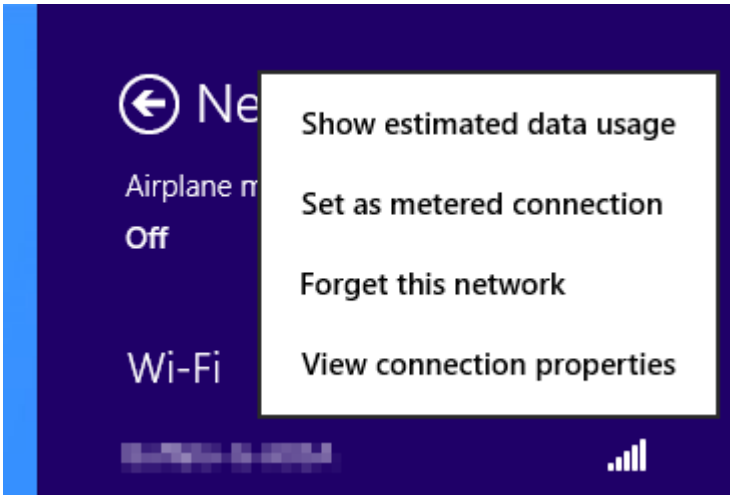
3. Click the **Available** icon (icon that indicates mobile reception).



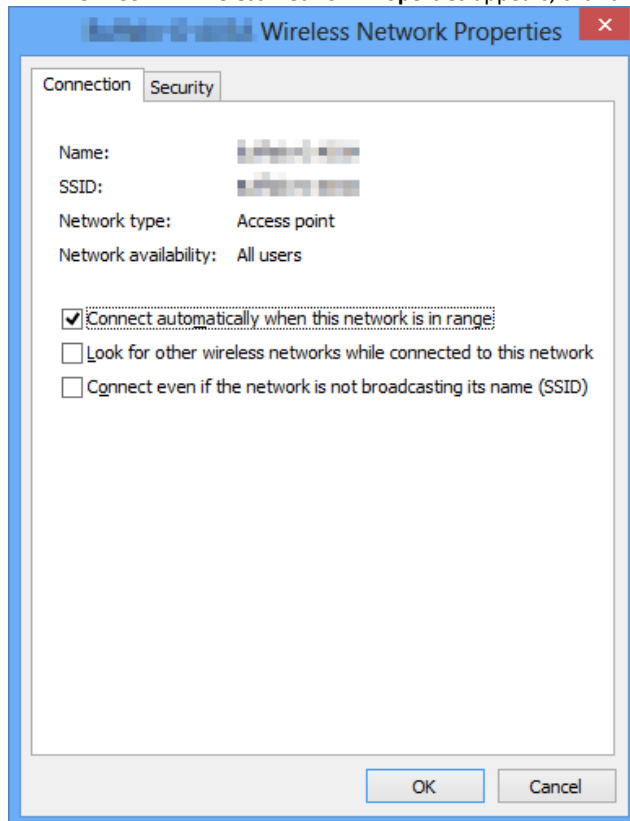
4. When **Networks** appears, right-click the name (SSID) of the network whose settings you want to check and click **View connection properties** from the menu that appears.

Note

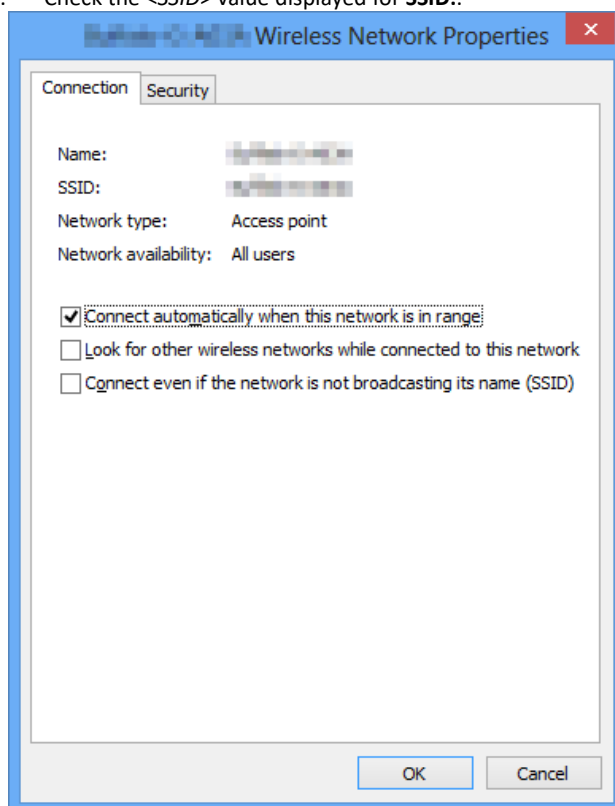
- If the menu does not appear even when you right-click the network name (SSID), it means that the profile for the SSID is not saved in US310e.
- If the list does not show the name (SSID) of the network whose settings you want to check, check the manual for your wireless LAN device and other relevant documentation.



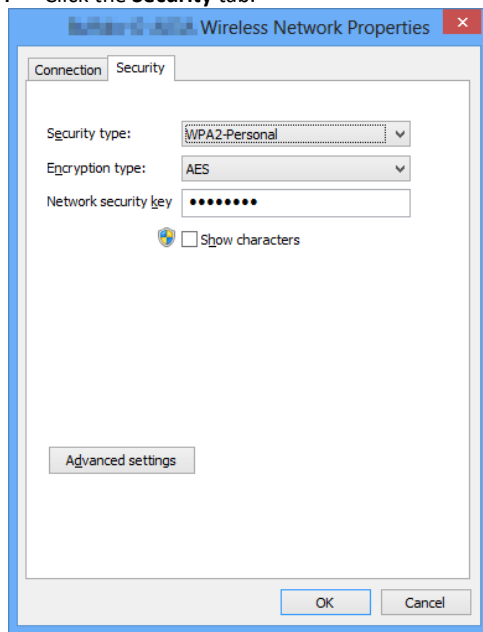
5. When **<SSID> Wireless Network Properties** appears, click the **Connection** tab.



6. Check the **<SSID>** value displayed for **SSID**:



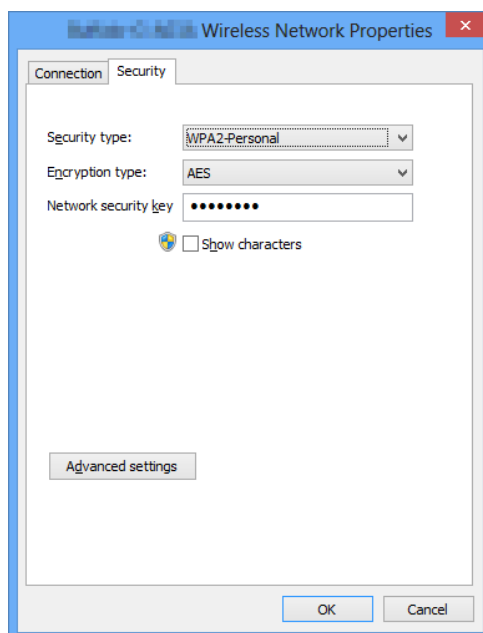
7. Click the **Security** tab.



8. Check the values displayed for **Security type**, **Encryption type**, and **Network security key**.

**Note**

- When you select the **Show characters** check box, the security key is displayed. Note that the security key may be converted depending on the security type and, therefore, be different from the value at the router or the access point.
- This setting screen can be used to change the security type, encryption type, or network security key. When changing these, make sure that new settings are suitable for your wireless LAN device.



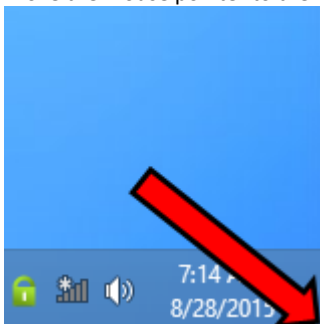
9. Click the × button to close **<SSID> Wireless Network Properties**.

### 14.3.2 Deleting a Network Profile (SSID)

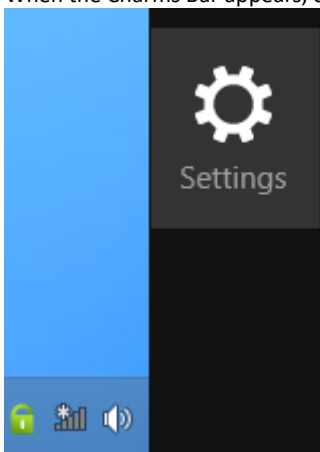
---

To delete a network profile (SSID), do the following:

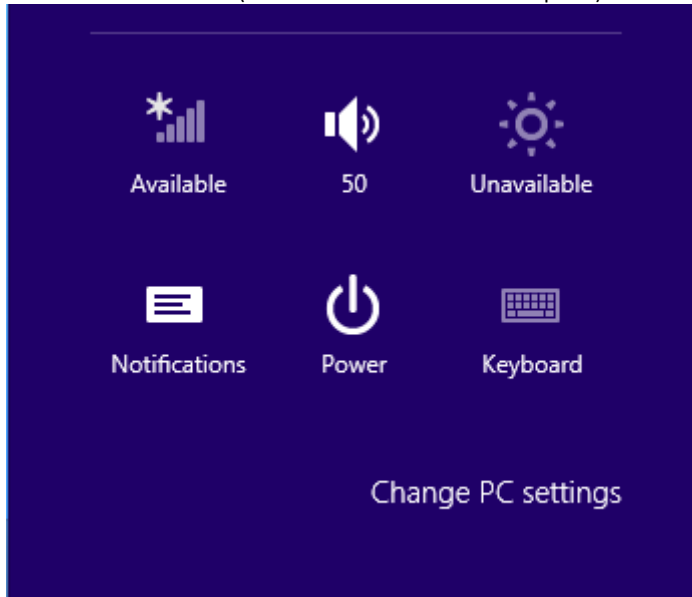
1. Move the mouse pointer to the bottom right corner of the desktop screen.



2. When the Charms Bar appears, click **Settings**.



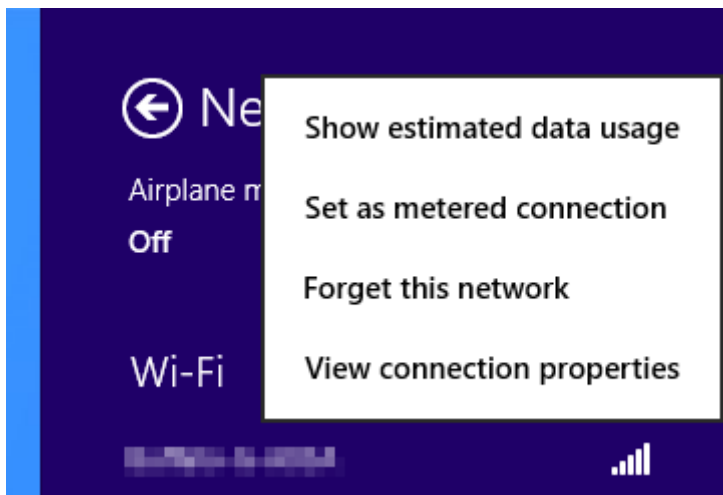
3. Click the **Available** icon (icon that indicates mobile reception).



4. When **Networks** appears, right-click the name (SSID) of the network you want to delete and click **Forget this network** from the menu that appears.

**Note**

- If the menu does not appear even when you right-click the network name (SSID), it means that the profile for the SSID is not saved in US310e.
- If the list does not show the name (SSID) of the network that you want to delete, check the manual for your wireless LAN device and other relevant documentation.



5. The network profile is deleted.

### 14.3.3 Managing a Network Profile (SSID) from the Command Prompt

---

The UI cannot be used to operate some network profiles (SSID) such as the profile of a network that is outside the service area. Execute commands at the command prompt to operate such network profiles.

The following are sample commands:

1. To display all the wireless LAN profiles:  
`netsh wlan show profiles`
2. To display the security key for a profile that is outside the service area:  
`netsh wlan show profile name="profile-name" key=clear`
3. To delete a profile that is outside the service area:  
`netsh wlan delete profile name="profile-name"`
4. To not automatically connect to a network that is outside the service area:  
`netsh wlan set profileparameter name="profile-name" connectionmode=manual`

\* Enter a profile name from the list displayed by using sample command 1. in "*profile-name*" in samples 2. to 4.

---

## 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.

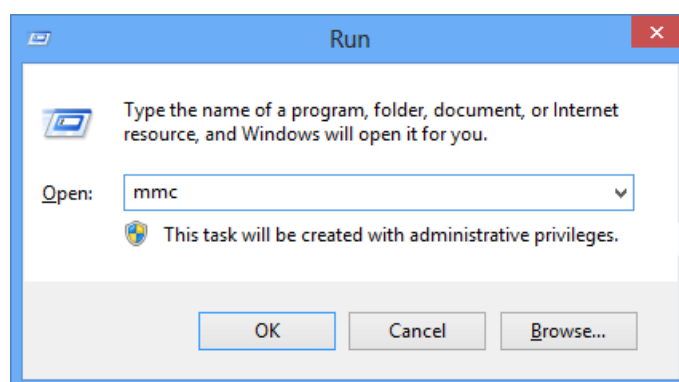
In both situations, after the initial authentication with the new RADIUS server succeeds, the client caches the new TLS session keys. Clients can cache TLS session keys for multiple RADIUS servers.

## 16. Saving the Certificate

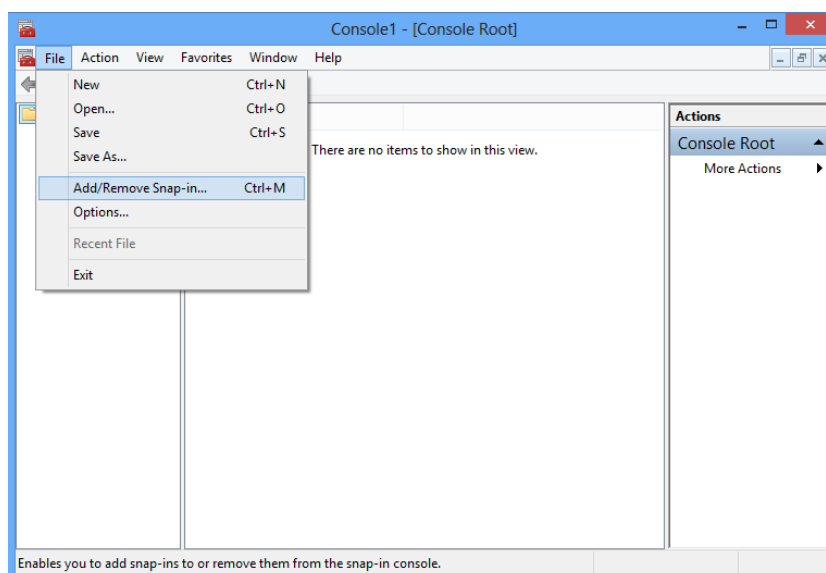
In Windows Embedded Standard 8 (WE8S), the Unified Writer Filter (UWF) protects the clients from undesired flash memory writes. The protected and cached flash memory contents are retained while the thin client is active, but they are lost when the thin client is restarted or shut down. In the same manner,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

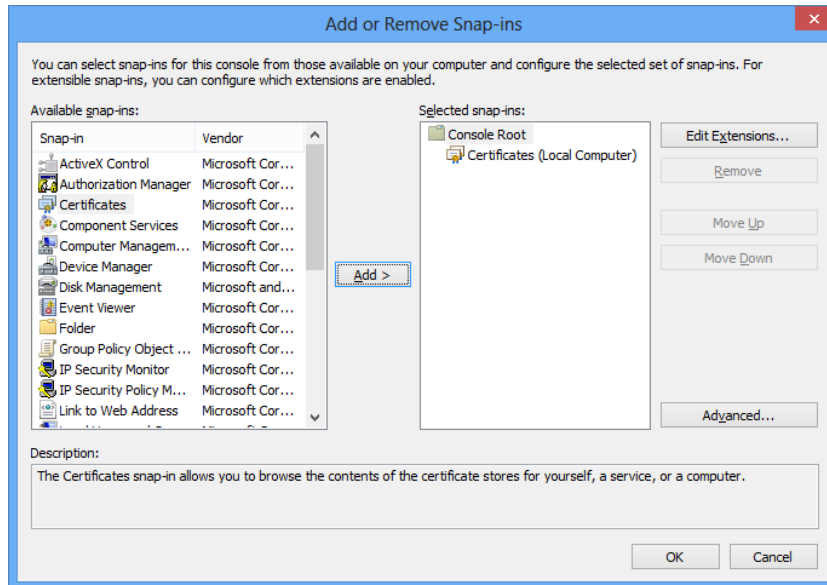
1. Log on to US310e as an administrator.
2. On the desktop, move the mouse pointer to the bottom-left corner, and then right-click on the appeared **Start** to open the popup menu.
3. Click to select **Run** on that popup menu.
4. Click **Run**, type "mmc" in the **Open** box, and then click **OK**.



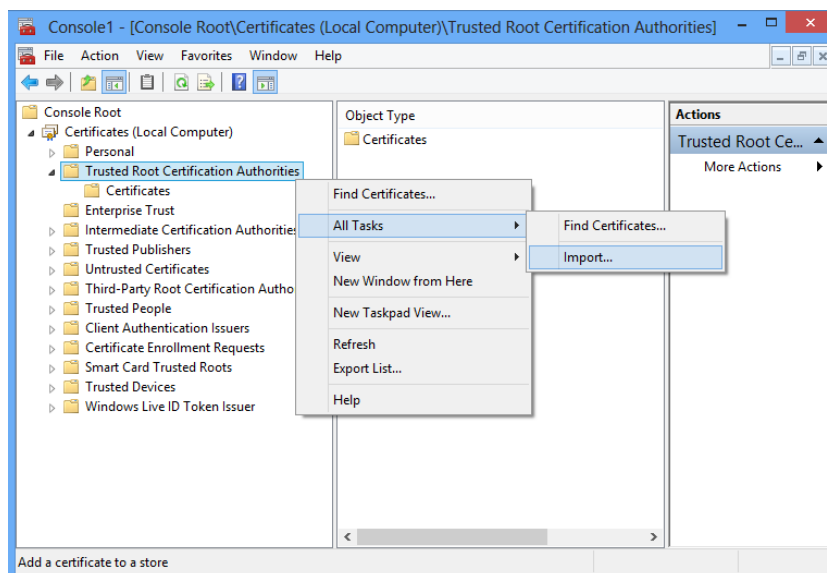
5. On the Console window, click the **File** menu to select **Add/Remove Snap-in**.



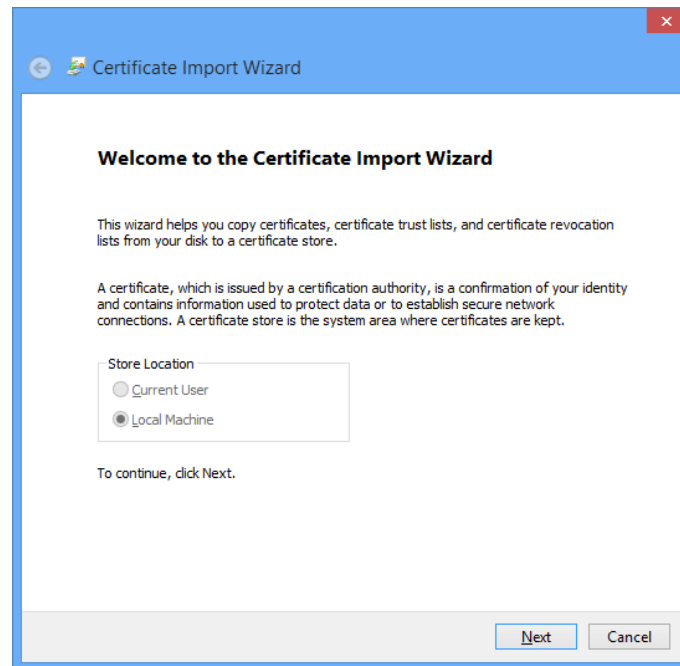
6. On the **Add or Remove Snap-ins** window, click **Certificates > Add > Computer account > Local computer > Finish > OK** to add the Certificates snap-in.



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.

---

## **Chapter 6 System Administration**

This chapter contains local and remote system administration information to help you perform the routine tasks needed to maintain your thin client environment.

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

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.

---

## **I. Using Atrust Device Manager (ADM) Software for Remote Administration**

---

Atrust Device Manager™ (ADM) servers provide network management services to thin clients, allowing complete user-desktop control through features such as shortcut creation, firmware updates, snapshot capture for mass deployment, remote shadow, reboot, shutdown, and Wake-on-LAN). By using ADM, you can manage all of your network devices from one simple-to-use console.

You can download Atrust Device Manager from the following website:

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

**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 malicious servers. If a thin client is not registered as a management target of the ADM server, it might be detected by a malicious server, and its settings might be changed. Therefore, be sure to register a thin client running in the production environment as a management target of the ADM server.

**Important** Care is required when migrating a thin client in which ACS was configured in the kitting environment to the production environment. In this case, you need to remove this thin client information from the kitting environment ADM server. If this operation is not performed, the production environment ADM server cannot register this thin client.

Note also that in Reset Mode, not only the ACS managed status, but also all ACS settings are initialized. For details about the Reset Mode, see Chapter 6, “2.2. Restoring Settings by Using Atrust Client Setup.”

Note with care that the production environment ADM server executes “Pull Settings” after detecting the thin client. As a result, the thin client ACS settings are synchronized to the ADM server and overwrite the settings on the ADM server side.

**Note**

- The registration information in Thin Client is not removed when the thin client is removed by ADM in the condition that thin client is disconnected from network. In this case you need to execute **Reset Mode** at Thin Client.
- Even if **Reset Mode** is executed at the Thin Client, registration information on ADM side isn't updated. Administrators need to remove the Thin Client at ADM side.

---

## 2. Restoring 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™

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

- Atrust Device Manager™

Recommended for larger environments. (See *Chapter 6*, "1. Using Atrust Device Manager (ADM) Software for Remote Administration".)

### **Important**

Thin client has been activated at the factory. But if, by using Atrust Device Manager (ADM) or Atrust 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*, "2.9 Activating US310eConfiguring UWF (Unified Write Filter)" 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.

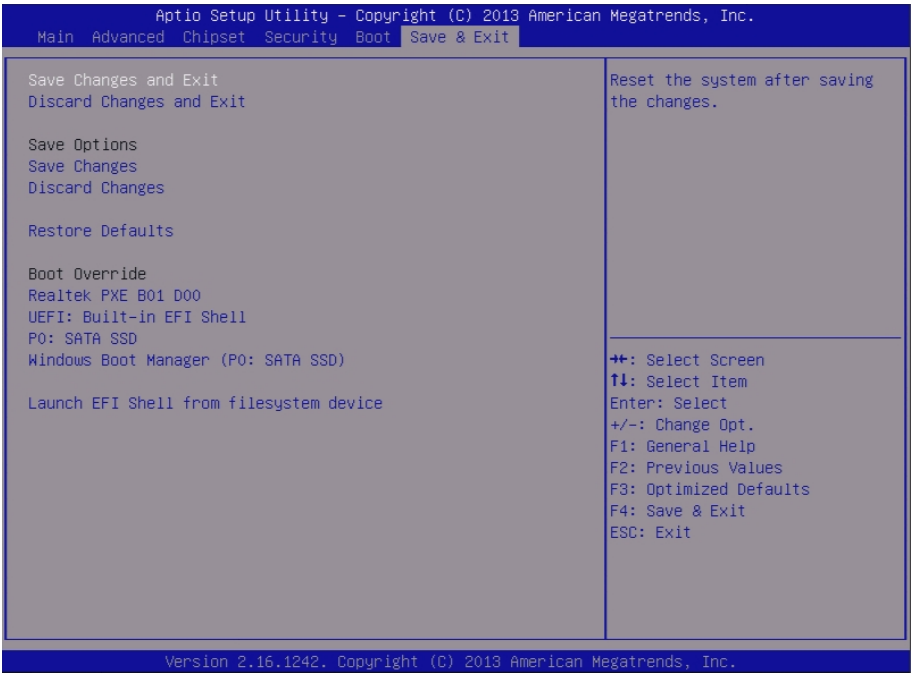
**Important** The factory-set BIOS settings may differ from the restored settings.

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.



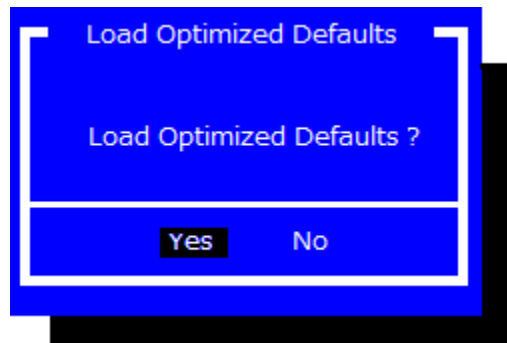
- 3. Move to the **Save & Exit** menu of BIOS Setup.



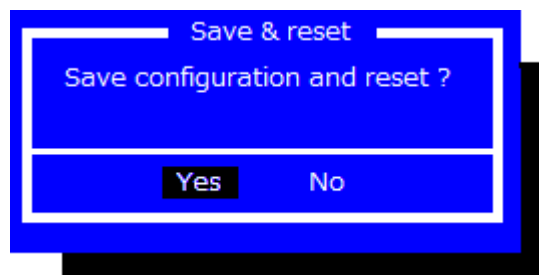
- 4. Select **Restore Defaults**, and press **Enter**.



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.

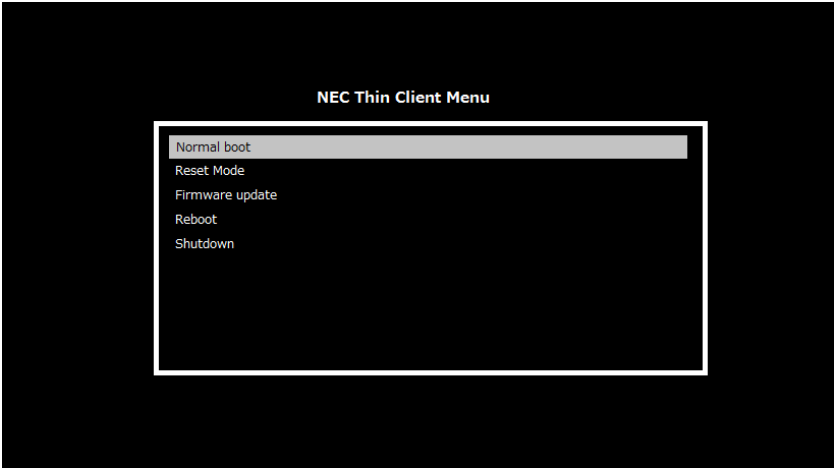
You can perform **Reset Mode** locally through NEC Thin Client Menu.

**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**

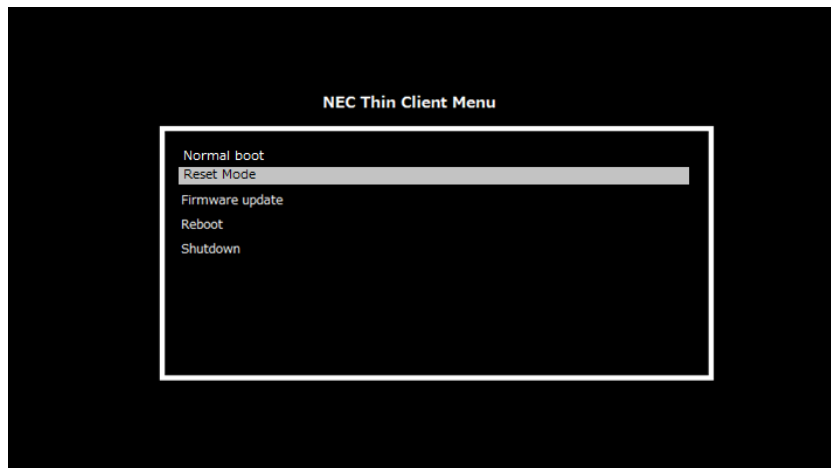
Five options are available on NEC Thin Client Menu: **Normal boot**, **Reset Mode**, **Firmware Update**, **Reboot**, and **Shutdown**. See the table below for the description of each option:

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

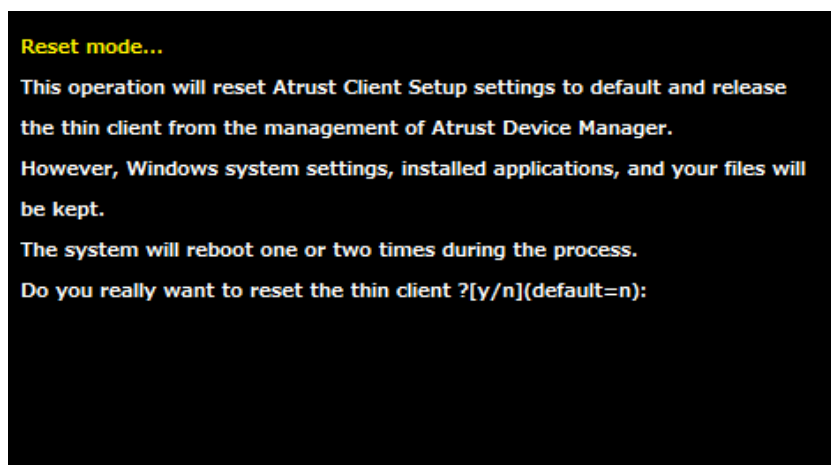
**Note**

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.

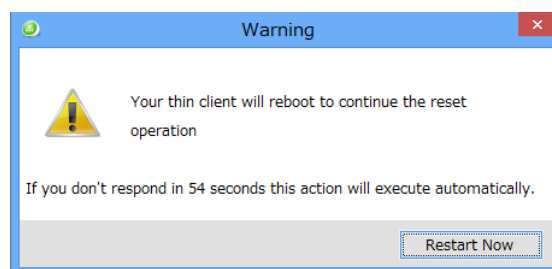
3. Use arrow keys to select **Reset Mode**, and then press **Enter** to continue.



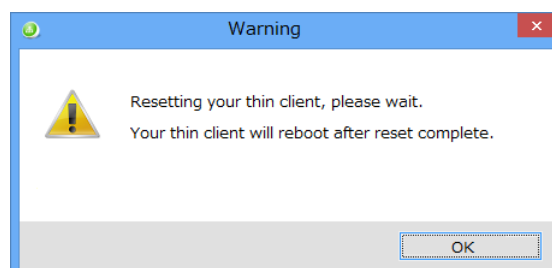
4. A message appears prompting you for confirmation. Type **y** to confirm, then press **Enter** to continue.



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**

USB flash drive of 32 GB (only) is required to deliver the firmware image by using the Atrust Recovery USB Disk Creator.

---

## **3. Configuring and Using Peripherals**

---

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**

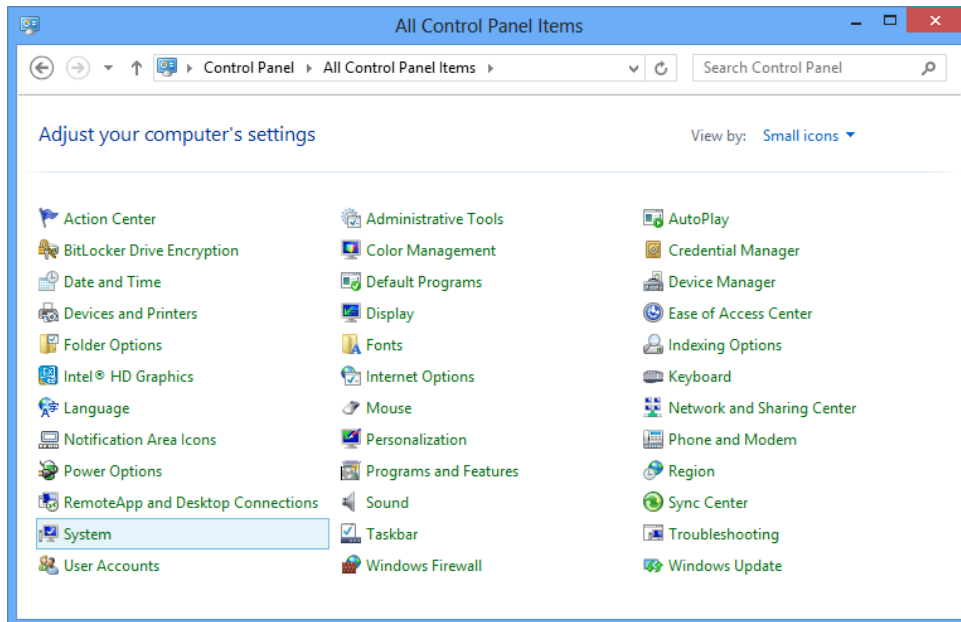
- **US310e WE8S 1. 20-INTL or later supports automatic activation. When US310e is connected to a network connected to the Internet, activation is automatically executed in the background when US310e starts up. This means that you do not have to manually authenticate the license.**
- **In US310e WE8S 1. 20-INTL or later, activation information is registered in the UWF “through” list. The activation status is therefore retained even after US310e restarts, allowing activation with UWF enabled.**

You can activate US310e via the Internet or by phone.

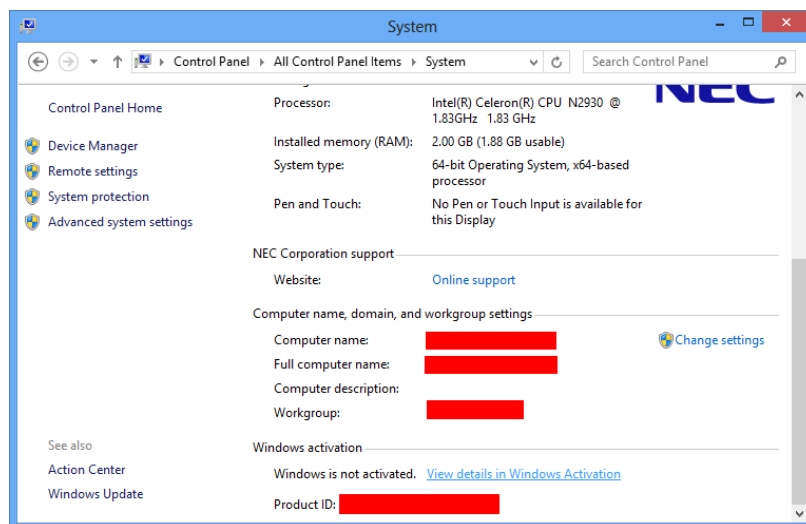
## 4.1 Via the Internet

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

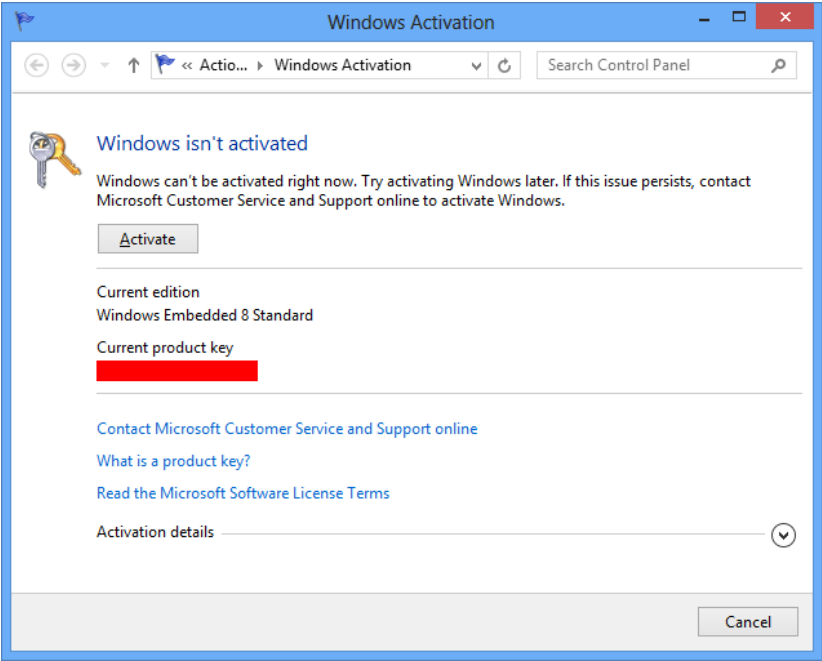
1. Restart your US310e.
2. Select **Start** → **Apps** → **Control Panel** → **All Control Panel Items**.
3. Select **System** on **All Control Panel Items**.



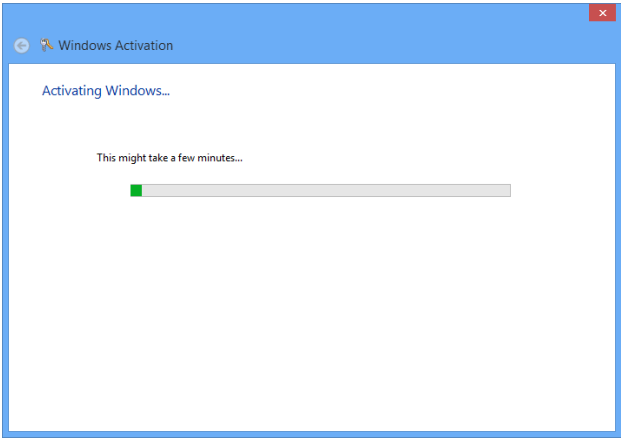
4. Click **Windows activation** in **View basic information about your computer**.



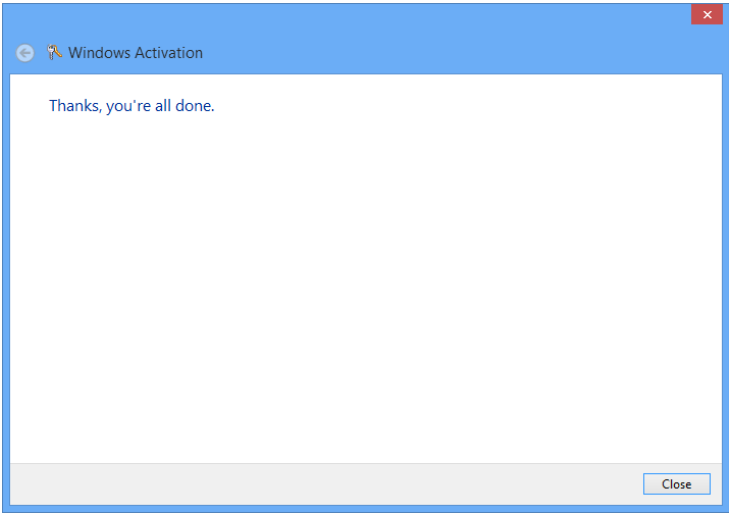
5. Click **Activate**.



6. Windows activation dialog starts. Wait for the process to complete.

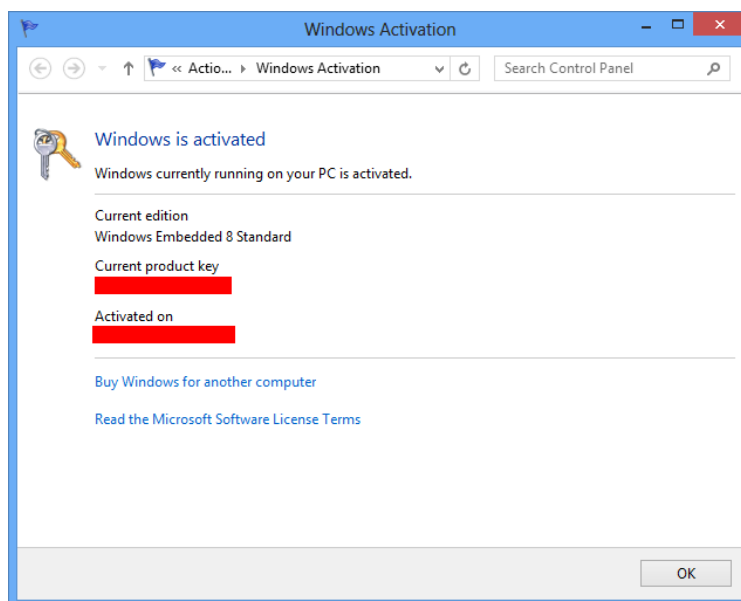


7. Upon completion of Windows activation, click **Close**.





8. Confirm that **Windows is activated** is shown, and click **OK**.



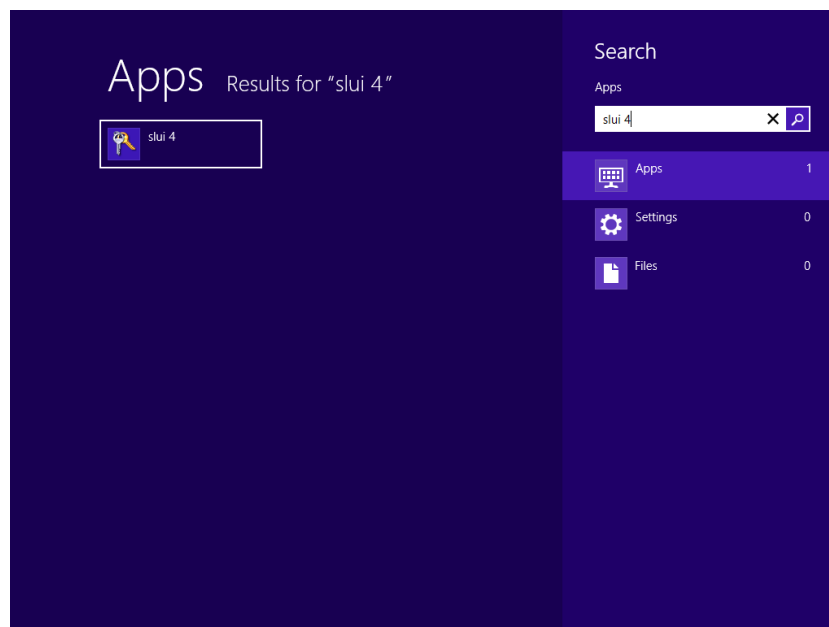
---

## 4.2 By phone

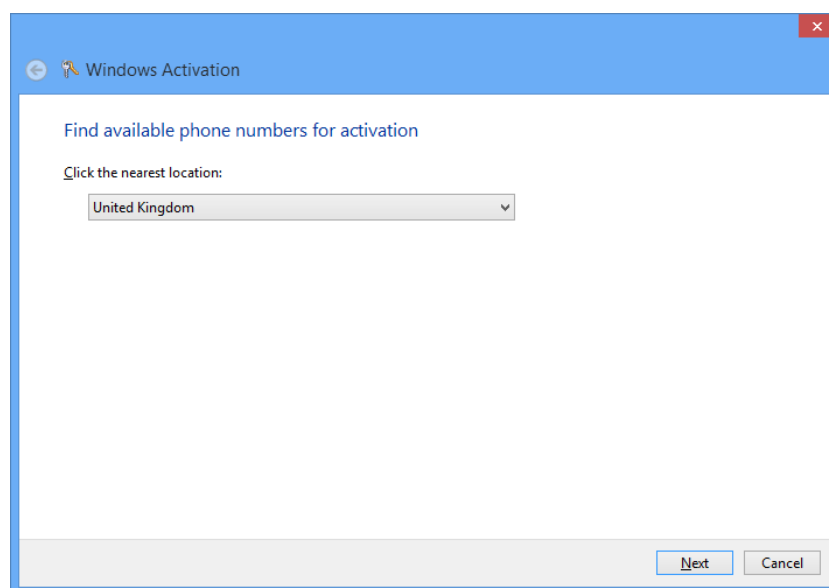
---

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

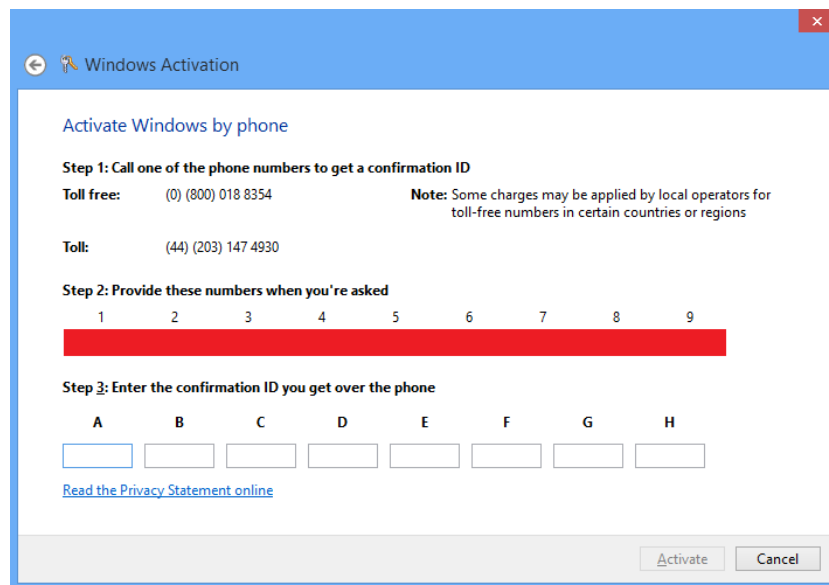
1. Restart your US310e.
2. On the **Start** screen, open the **Search** charm. Type in **slui 4**, and select "slui 4" in the search results.



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**.



The screenshot shows the 'Windows Activation' window with the title bar 'Windows Activation'. The main content area is titled 'Activate Windows by phone'. It contains three steps:

- Step 1: Call one of the phone numbers to get a confirmation ID**
  - Toll free:** (0) (800) 018 8354
  - Note:** Some charges may be applied by local operators for toll-free numbers in certain countries or regions
  - Toll:** (44) (203) 147 4930
- Step 2: Provide these numbers when you're asked**
  - A red bar with numbers 1 through 9 is displayed.
- Step 3: Enter the confirmation ID you get over the phone**
  - Letters A through H are displayed above a row of eight input boxes.

At the bottom, there is a link [Read the Privacy Statement online](#) and two buttons: 'Activate' and 'Cancel'.

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.

## 4.3 Activating US310e via the Volume Activation Management Tool (VAMT)

You can also activate US310e using VAMT proxy activation. The VAMT host computer distributes a Multiple Activation Key (MAK) to one or more US310e terminals and collects the installation ID (IID) from each US310e terminal. The VAMT host computer sends the IIDs to Microsoft on behalf of the US310e terminals and obtains the corresponding Confirmation IDs (CIDs). Then, the VAMT host computer installs the CIDs on the US310e terminals to complete the activation. To use this activation method, only the VAMT host computer needs to be enabled to access the Internet. For details about the VAMT, see the Microsoft documentation.

To perform VAMT proxy activation, it is necessary to register a firewall exception and set the registry on US310e terminals in advance to allow communication with the VAMT among subnets. Disable UWF to keep the setting also after the restart of US310e, and then perform the following steps:

1. Sign in to US310e as an Administrator.
2. If your device is in a workgroup, you may need to disable Remote UAC. Open a command prompt with administrator user rights and type the following to disable Remote UAC:

```
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

3. Type the following to enable the Remote Administration exception:

```
netsh advfirewall set service RemoteAdmin enable
```

4. Type the following to enable WMI traffic at a command prompt by using a WMI rule:

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

5. Type the following to establish a firewall exception for DCOM port 135:

```
netsh advfirewall firewall add rule dir=in name="DCOM" program=%systemroot%\system32\svchost.exe
service=rpcss action=allow protocol=TCP localport=135
```

6. Type the following to establish a firewall exception for the WMI service:

```
netsh advfirewall firewall add rule dir=in name="WMI" program=%systemroot%\system32\svchost.exe
service=winmgmt action=allow protocol=TCP localport=any
```

7. Type the following to establish a firewall exception for the sink that receives callbacks from a remote device:

```
netsh advfirewall firewall add rule dir=in name="UnsecApp"
program=%systemroot%\system32\wbem\unsecapp.exe action=allow
```

8. Type the following to establish a firewall exception for outgoing connections to a remote device that the local computer is communicating with asynchronously:

```
netsh advfirewall firewall add rule dir=out name="WMI_OUT" program=%systemroot%\system32\svchost.exe
service=winmgmt action=allow protocol=TCP localport=any
```

---

---

## **Chapter 7   Establishing a Server Environment**

This chapter contains information about the network architecture and enterprise server environment needed to provide network and session services for your thin clients.

It includes:

**1. Understanding How to Configure Your Network Services**

Describes the network services available for your 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 R2 or Windows Server 2012 R2 with Terminal Services (remote desktop service) and one of the following installed:

- Citrix XenApp
- Citrix XenDesktop
- 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 versions only)
- Windows 8.1 (Supported versions only)
- Windows 10 (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.

---

---

## **Chapter 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 1.30-INTL
Build version of Japanese OS	WE8S 1.30-INTL

- \* This product release supports Atrust Device Manager (ADM) 2.08.045 or later. If you are using an older version of ADM, upgrade ADM before upgrading the firmware.
- \* This product release supports a BIOS version of US310e v1.62 or later. If you are using an older version of BIOS, upgrade BIOS before upgrading the firmware.

### Expansion and modification history

#### WE8S 1.30-INTL

1. Security has been enhanced.
2. Time synchronization at the startup of a terminal has been enhanced.
3. The maximum log file size for ACS has been expanded to 100 MB.
4. Japanese ACS notation has been corrected.
5. **Snapshot type** has been deleted from ACS snapshot setting.
6. The residual capacity in the upload destination is now checked when the network is selected as the upload destination for taking a snapshot with ACS.
7. Characters and string length available for a password are now displayed in the Set Password dialog displayed for setting an ACS Shadow password and a password for accessing ACS.
8. Taking a snapshot when the password of the default administrator account (Administrator) is changed is now supported.

9. Taking a snapshot when a double quotation (") is used for the password of the default administrator account (Administrator) is now supported.
10. The hot key for starting ACS in the Appliance mode has been changed from Shift+Ctrl+Delete to Shift+Ctrl+A.
11. The problem that a warning message is displayed when a virtual machine is connected with a shortcut of an RDP session created using ADM/ACS has been corrected.
12. The problem that a double quotation (") is unavailable in the password field of ACS VMware Horizon has been corrected.
13. The problem that an unintentional setting may be saved with ACS has been corrected.
14. The problem that the ACS remote shadow feature may not be able to reflect a password containing a special character string normally has been corrected.
15. The problem that multiple settings reflected from ADM may not be reflected to US310e normally has been corrected.
16. The problem that there is erroneous information displayed in the ADM log when a package is distributed has been corrected.
17. The problem that once a connected entry is deleted with a virtual desktop connected in the Appliance mode, the screen may not be displayed at the next startup has been corrected.
18. The problem that when the Citrix Receiver 4.4 update package is installed, the design of the Citrix icon on ACS is not changed from that for Citrix Receiver 4.2 has been corrected.
19. The problem that when the Citrix Receiver 4.4 update package is installed, a blank desktop icon is displayed for a Citrix ICA session created with ACS has been corrected.
20. The problem that icon in the notification area on the desktop screen becomes unjust has been corrected.
21. VMware Horizon Client has been upgraded to version 3.5.2.3039.
22. .NET Framework has been upgraded to version 4.6.1.

---

# 1.3 BIOS

---

Item	Description
Platform	US310e
BIOS version	US310e v1.62

**Expansion and modification history**

**US310e v1.62**

1. The stability of the sleep operation and restoration from sleep mode has been improved.
2. The stability of the startup operation of the OS has been improved.
3. The problem that the OS may not start up in rare cases when a certain keyboard is connected has been corrected.

## 1.4 Applications

Application	Version
Adobe Flash Player 17 NPAPI	17.0.0.188
Atrust Client Setup (WE8S)	1.18
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
Intel (R) Sideband Fabric Device Driver	1.70.305.16316
Internet Explorer	10.0.9200.16384
Microsoft .NET Framework 4.6.1	4.6.01055
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	3.5.2.30397
Windows Media Player	12.0.9200.16578

---

## **1.5 Media Codecs**

---

Your US310e contains the following codecs:

### Audio

- WMA
- 2ch Dolby Digital (AC-3)
- AAC
- MP3

### Video

- WMV
- MPEG-4 Visual (MPEG-4 Part 2)
- AVC.H.264 (MPEG-4 Part 10)



---

## 2. Notes and Restrictions

---

This section describes notes and restrictions on using 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 Sideload
- 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).
- 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.
- Currently, USB 3.0 host controllers are not yet supported. The USB mode of BIOS is EHCI (USB 2.0) by default. Use this default EHCI as the USB mode of the BIOS. Do not switch to XHCI (USB 3.0).
- The file encryption credential management function cannot be used.
- The Windows help function cannot be used.

## 2.2 Notes and Restrictions

- Failure of the software built into this product and related software published on the support page can no longer be corrected after the relevant software developer discontinues support. In this case, only limited support such as actions based on known cases is provided and you must basically operate the system by working around the failure (the failure remains “as-is”). To avoid such a situation, promptly conduct verification in all the operation scenarios to confirm that the product operates normally while building the system and after starting operation.
- The thin client terminal equipped with Windows OS is putting into effect the basic security measure for restricting part of operation to the User account in the factory shipment state, but it isn't guaranteed that there are no problems for security. According to the practical environment and the security for the customer, it's necessary to customize function restriction for User account and the blockade of the network port which isn't used, and so on. After confirming the no problem thing sufficiently beforehand, please use it.
- Like other IT systems, the thin client system might not operate correctly or it might not work sufficiently due to factors such as network configuration, policy settings, and the specifications of the connected peripheral devices. Some features require installation of third party software. NEC does not guarantee the use of this thin client in any environment under any conditions. Before using the thin client, thoroughly evaluate the operation in the actual operating environment and confirm that there is no problem.
- Hotfixes of thin client are published by support page. It is recommended to configure ADM server for deploying the Hotfixes to a thin client over the network and register the thin client as a management target of the ADM server. You need install the Hotfixes to each thin client manually if ADM is not used.
- OS to be equipped with this product is renewed for functional enhancement and quality improvement. Because of the timing of OS renewal at the production plant, there is a possibility that old and new OS is mixed in the case of additional purchase or two or more purchase. When needing unification of the OS version by the whole system, please use system image delivery by ADM and USB flash memory.
- If you copy a file whose size exceeds the pre-set maximum memory size (640 MB by default) of UWF to C drive of US310e while the UWF is enabled, US310e becomes extremely unstable.
- Be sure to the following points when creating ICA connection shortcut in ACS.
  - 1 If XenApp/XenDesktop is specified as session type, the session is connected to DC(Delivery Controller) server directly. The session is not connected to StoreFront server.
  - 2 When DC and StoreFront are installed on same server, the session connected from ICA shortcut, created by ACS, fails if http protocol is used as base URL of StoreFront. A session of “SSL/TLS + HTTPS Server Location” is supported before XenApp 6.5, and not supported in XenDesktop/XenApp 7 or later. Use http protocol for URL when DC and StoreFront are installed on same server.
  - 3 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 ACS, "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.
  - 4 ACS is not support XenDesktop/XenApp 7.6 or later. So use Citrix Receiver to connect XenDesktop/XenApp 7.6 or later.

5 Atrust Client Setup supports Citrix Receiver and VMWare Horizon View Client preinstalled in US310e. If you upgrade them, the connection entry created in Atrust Client Setup no longer properly operates.

- Connect to VMware Horizon View + VM Win8.1 and play YouTube, the video playback performance is not smooth on 1920x1080, 1680x1050.
- 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 permanently 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.
  - 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.
  - 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.

- 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.
  - 6 Sign in US310e with an Administrator account.
  - 7 Click **Run** from the Start menu.
  - 8 Enter **gpedit.msc**, and click **OK**.
  - 9 Select **Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies**.
  - 10 Double-click **Turn Off AutoPlay**, select **Enable** in the dialog box opened, select **All Drives** as an option, and then click **OK**.
  - 11 Double-click **Prevent AutoPlay From Remembering User Choice**, select **Enable** in the dialog box opened, and then click **OK**.
  - 12 Double-click **Enable or Disable AutoPlay for Non-volume Devices**, select **Enable** in the dialog box opened, and then click **OK**.
  - 13 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**.
  - 14 Click **Run** from the Start menu.
  - 15 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.
- In US310e local environment, the shortcut keys combined with Windows logo key are disabled.

- Only Japanese and English (U.S.) are supported as keyboard languages.  
If using another language, be sure to verify in advance that it will not cause any problems when the system is integrated.
- When performing port-level redirection for a mass storage device in a Citrix ICA or VMware Horizon 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.
- **On resume, display logon screen** in the screensaver settings does not operate even if you select this option. To validate this setting, change the registry settings by using the following procedure. In addition, disable UWF before setting the registry and enable it again after completing the setting.
  1. Sign in to US310e with an Administrator account.
  2. Click **Control Panel** from the Start menu.
  3. Start **Folder Options**.
  4. Select the **View** tab and clear the **Hide extensions for known file types** and **Hide protected operation system files (Recommended)** check boxes.
  5. Click **OK** to exit **Folder Options**.
  6. Click **Run** from the Start menu.
  7. Enter "regedit.msc" and click **OK** to start Registry Editor.
  8. Select **HKEY\_USERS**.
  9. Select **File - Load Hive** to open "C:\Users\<user-name>\NTUSER.DAT."
  10. Specify a key name in **Key Name** and click **OK**. (Here, it is assumed that "temp" is specified in **Key Name**.)
  11. Set the following to [HKEY\_USERS\tmp\Software\Microsoft\Windows\CurrentVersion\Policies\System]:  
"DisableLockWorkstation"=dword:00000000
  12. Select **File - Unload Hive**.
  13. Select **File - Exit** to exit Registry Editor.
  14. Click **Control Panel** from the Start menu.
  15. Start **Folder Options**.
  16. Select the **View** tab and select the **Hide extensions for known file types** and **Hide protected operation system files (Recommended)** check boxes.
- US310e is set to not use the virtual memory (page file) (0 MB). To use the virtual memory (page file), you must set the page file on a volume not protected by UWF. The virtual memory (page file) cannot be used in US310e because US310e consists of a single volume protected by UWF.
- The **ACS > Web browser > Global > Home page** setting is not retained when firmware is distributed.
- The screen display may be distorted in rare cases if you perform certain operations on Atrust Client Setup.
- Although Recycle Bin is displayed when you sign in with a domain user account, the recycle function is not provided. When you delete a folder or file, it is completely deleted.
- Although **Help and Support** is displayed on the application screen when you sign in with a domain user account, this function is not provided and cannot be started.
- You may fail to sign in with a domain user account. In this case, "There are currently no logon servers available to service the logon request." appears and Event ID 5719 is recorded in the log.

With the Windows fast logon function, US310e starts up without waiting for initialization of the network. So if the network connection is not yet established when you sign in with a domain user account, this phenomenon will occur because the domain server cannot be found.

If you have already initially signed in with a domain user account (created a domain user profile), you can sign in using the domain cache the next time even if the network connection is not established. (Group policies are asynchronously applied by the fast logon optimization function.) However, changes to US310e are discarded by UWF after restart. Therefore, unless you initially sign in with a domain user account with UWF disabled, the created domain user profile is discarded at every restart and this phenomenon occurs.

There are many possible scenarios where it takes time to establish a network connection. For example, the DHCP relay agent may need a long time to acquire the IP address or the 802.1X authentication process may take a long time. If it is difficult to solve the problem due to a variety of factors, you may be able to avoid this phenomenon by enabling **Computer configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon** under the group policies. If this setting is enabled, Windows displays the sign-in screen after the network connection is established. (Startup takes more time.) Although Event ID5719 may not be avoided and recorded in the log, you can ignore it as long as you can normally sign in to the domain.

- If you enable **Computer configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of removable devices** under the group policies, a blue screen error occurs after you restart US310e, so do not enable this policy.
- Windows KB files cannot be used to upgrade the built-in IE Flash Player.
- Atrust Client Setup supports Citrix Receiver and VMWare Horizon View Client preinstalled in US310e. If you upgrade them, the connection entry created in Atrust Client Setup no longer properly operates.
- If the snapshot image contains setting information configured in **Profile Group** in ADM, you may not be able to properly acquire or distribute setting information from ADM in US310e after the snapshot image is distributed if you delete setting information for the profile group.
- When you specify a IP address as Computer Name and a UPN(User Principal Name) as User Name the connection of NLA (Network Level Authentication) fails. This is a restriction specific to Windows 8、Windows Embedded 8 Standard.

[Example]

Computer Name : 192.168.0.1

User Name : [testuser@nec.com](mailto:testuser@nec.com)

The cause of this is the acquired Domain Name is added to User Name by Remote Desktop Client's communication with Active Directory.

\* The RDP connection succeeds, if specifying a IP address as Computer Name and a UPN (User Principal Name) as User Name, in NLA security dialog displayed after RDP connection failed.

[How to avoid]

1. Specify DNS (FQDN, NetBIOS) as Computer Name.  
The User Name is set properly because Kerberos authentication is used by specifying DNS as Computer Name.
2. Specify <NetBIOS domain name>\<User name> as User Name.  
The User name is set properly by specifying <NetBIOS domain name>\<User name> as User name.

Kerberos authentication is not used if not DNS but IP address is specified. Be sure to specify DNS as Computer name if using Kerberos authentication. This is a recommendation on the security.

- When a thin client is registered in an ADM Server, the managed status is enabled, and other ADM Servers become unable to detect the thin client. This specification is intended to prevent access from malicious servers. If a thin client is not registered as a management target of the ADM server, it might be detected by a malicious server, and its settings might be changed. Be sure to register a thin client as a management target of the ADM server for security.
- When ADM is built on the virtual machine of VMware ESXi and an update of firmware or a snapshot is installed in US310e from ADM, delay of a network occurs, and it sometimes fail in download of an image file. There is a possibility that it's improved by invalidating a flow control of a virtual NIC of VMware ESXi in setting. Please refer to the following knowledge base about the way to invalidate a flow control of a virtual NIC of VMware ESXi in setting.

Configuring Flow Control on VMware ESXi and VMware ESX

<http://kb.vmware.com/kb/1013413>

---

## **Chapter 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.leaning

---

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

 <b>WARNING</b>	
	<p>Observe the following instructions to use US310e safely. Failure to follow these instructions may result in loss of life or serious personal injury.</p> <ul style="list-style-type: none"><li>• Do not disassemble, repair, or alter US310e.</li></ul>

---

### 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:  $-10^{\circ}\text{C}$  to  $55^{\circ}\text{C}$ , 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.

**NEC Express5800 Series  
US310e**

# 10

---

---

## Chapter 10 Appendix

### **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: 3.5 mini-jack Input: 3.5 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  
FW WE8S 1.30-INTL**

**Third Edition, JUNE 2018**

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

©NEC Corporation 2018

The contents of this manual may not be copied or altered without the prior written permission of NEC Corporation.