

Atrust Device Manager 2.09.001 User's Guide

Contents

Chapter 1	Overview	4
1.1	Introduction.....	5
1.2	New Features.....	6
1.3	Features.....	7
1.4	System Requirements	8
1.4.1	Supported Endpoint Devices	8
1.4.2	Supported Platforms	9
1.4.3	Hardware Requirements	9
1.4.4	Used ports.....	9
1.4.5	Configuring the network environment.....	10
Chapter 2	Installing and Upgrading ADM	12
2.1	Installing ADM	13
2.2	Initial Setup	18
2.3	Upgrading ADM	20
2.4	Stopping Atrust-Multicast Service	20
2.5	Uninstalling ADM.....	24
Chapter 3	Using ADM.....	25
3.1	ADM	26
3.1.1	Interface Overview.....	26
3.1.2	Available Tasks at a Glance.....	27
3.2	Establishing a Basic Administration Environment.....	28
3.2.1	System Tab Overview	28
3.2.2	Available Tasks at a Glance.....	29
3.2.3	Managing Accounts for Administration	30
3.2.4	Managing Thin Client Firmware Files.....	32
3.2.5	Managing WES Package Files	35
3.2.6	Managing Client Snapshots.....	38
3.2.7	Managing Certificates	40
3.2.8	Configuring Remote Deployment Settings	42
3.2.9	Selecting the Service IP of ADM.....	45
3.2.10	Configuring Auto-Logout for ADM	46
3.2.11	Configuring Auto Registration.....	47
3.2.12	Configuring Password Protection for Managed Devices	56
3.2.13	Configuring the Database Source of ADM.....	60
3.2.14	Selecting the Interface Language of ADM.....	62
3.2.15	Backing Up the Management Database.....	63
3.2.16	Managing Database Archive Files	64
3.2.17	Restoring a Database Archive File	66
3.2.18	Scheduling Automatically Performed Tasks	67
3.3	Adding Clients into a Managed Group.....	71
3.3.1	Scan Tab Overview	71
3.3.2	Available Tasks at a Glance.....	71
3.3.3	Client Detection and Management.....	72
3.3.4	Discovering Clients in the Whole Range of a Local Network.....	73
3.3.5	Discovering Clients in a Specified Range of IP Addresses.....	74
3.3.6	Creating and Managing an IP Range List	76
3.3.7	Discovering Clients using a Predefined IP Range List	77
3.3.8	Discovering Clients Including Password-Protected Devices	79
3.4	Managing All Your Clients	80
3.4.1	Thin Clients Tab Overview.....	80
3.4.2	Available Tasks at a Glance.....	81
3.4.3	Creating Client Groups	82
3.4.4	Managing Client Groups.....	84

3.4.5	Moving Clients to Another Group	85
3.4.6	Deleting Clients from a Group.....	86
3.4.7	Client Status Icons.....	87
3.4.8	Client Settings	88
3.4.9	Creating Setting Profile Groups.....	90
3.4.10	Managing Setting Profile Groups	92
3.4.11	Creating Client Setting Profiles.....	93
3.4.12	Managing Client Setting Profiles	97
3.4.13	Using Individualized Client Settings	103
3.4.14	Using Hybrid Client Settings.....	105
3.4.15	Pushing Settings to Clients through Your Local Network	108
3.4.16	Pulling Client Settings through Your Local Network	114
3.4.17	Pushing Certificates.....	119
3.4.18	Sending Messages to Clients.....	122
3.4.19	Editing or Viewing the Basic Information about a Client.....	124
3.4.20	Rebooting Clients through Your Local Network	125
3.4.21	Shutting Down Clients through Your Local Network	128
3.4.22	Starting Up Clients through Your Local Network.....	132
3.4.23	Updating Client Firmware	136
3.4.24	Installing and Uninstalling Software Packages	140
3.4.25	Taking Client Snapshots	142
3.4.26	Installing Client Snapshots	144
3.4.27	Using the Shadow Feature	146
3.4.28	Exporting Client Data	148
3.4.29	Digging Out Profiles, Clients, or Event Logs with Quick Search	149
3.4.30	Digging Out Clients with Filters	151
3.4.31	Managing Your Filters	153
3.5	Viewing and Managing Event Logs	155
3.5.1	Logs Tab Overview	155
3.5.2	Available Tasks at a Glance.....	155
3.5.3	Viewing Event Logs	156
3.5.4	Exporting Event Logs.....	157
3.5.5	Emptying Event Logs	158
3.6	Viewing Software Information.....	160
3.6.1	About Tab Overview.....	160
3.6.2	Available Tasks at a Glance.....	160
3.6.3	Viewing Information on ADM	160
3.6.4	Viewing ADM Contact Information	161
3.6.5	Viewing ADM Software License Agreement.....	161
Chapter 4	Configuring Client Settings	162
4.1	Desktop Virtualization and Client Configuration	163
4.2	Client Settings at a Glance	164
4.2.1	US320f	164
4.2.2	US310e.....	165
4.2.3	US120f	166
4.3	Editing or Adjusting a Group Configuration	168
4.4	Editing or Adjusting an Individual Configuration	171
4.5	Using Custom Wallpapers on Clients with ADM	174
4.6	Configuring Client Settings with ACS	180
Chapter 5	Advanced Uses of ADM	181
5.1	Using ADM as an Auto Setup File Server	182
Chapter 6	Notes and Restrictions.....	187
6.1	Synchronizing ADM with ACS Settings.....	188
6.2	Adding to and Releasing from Management	189
6.3	Notes on Taking and Installing Snapshots.....	190
6.3.1	Types of Snapshots	190
6.3.2	Behavior of Default User Account at Snapshot Installation	190
6.3.3	About Joining a Domain	191

6.4	Notes on Updating Firmware and Installing Snapshots	192
6.4.1	Maintenance of ACS Settings	192
6.4.2	Canceling Activation (License Authentication) (US320f and US310e).....	192
6.5	Notes on Accessing the ADM Management Console	193
6.6	Notes on Using VNC (Remote Shadow)	194
6.7	Notes on Backup and Restoring ADM Server.....	195
6.7.1	Database and Firmware and Package Backup	195
6.7.2	Restoration of ADM Server	195
6.8	Restrictions.....	196
6.8.1	Restrictions on ADM	196
6.8.2	Restrictions on US320f	196
6.8.3	Restrictions on US310e	197
6.8.4	Restrictions on US120f	197

Chapter 1 Overview

This chapter provides an overview of the Atrust Device Manager (called ADM below) and the system requirements.

1.1 Introduction

A brief introduction to ADM

1.2 New Features

New features and enhanced functions in this product release

1.3 Features

The key features of ADM

1.4 System Requirements

The system requirements for the installation and operation of ADM

1.1 Introduction

Desktop virtualization provides a new perspective to reconsider the design and implementation of an IT infrastructure. In a desktop virtualization infrastructure, a client is no longer a cumbersome desktop, but simply an endpoint device for users to access delivery services from the server(s).

With the introduction of the desktop virtualization technologies, you can considerably benefit from:

- On-demand application / desktop access
- Centralized management of work environments
- Drastically reduced endpoint software/hardware issues
- Simplified system maintenance
- Improved system security
- More scalability with low-cost endpoint devices

But still you need powerful software for managing a large number of endpoint devices in a desktop virtualization infrastructure. The ADM console is designed to fill this need. It enables you to remotely deploy, manage, update clients, and assist users from a single computer. You can manage and update clients simply and quickly in groups with a flexible and secure mechanism. Additionally, you can remotely assist users in resolving problems or configuring local settings.

1.2 New Features

This product release provides the following new and enhanced functions:

US320f supported

US320f is supported as a manageable device in ADM.

1.3 Features

The key features of ADM are:

- Pushing custom settings to a large number of clients
- Updating firmware and installing software packages for clients
- Taking client snapshots for mass deployment, system backup, and recovery
- Rebooting, powering off, and waking clients through the local network
- Scheduling automatically performed tasks
- Helping users to troubleshoot problems remotely
- Identifying clients and managing IT assets with automatically-captured client information
- Helping the management of zero clients

Note

A **zero client** is an endpoint device without any operating system pre-installed. ADM does not support the management of zero clients because US320f/US310e/US120f is not the zero clients.

1.4 System Requirements

The system requirements for the installation and operation of ADM as follows:

1.4.1 Supported Endpoint Devices

ADM supports the following Atrust client family:

Model:

- US320f
- US310e
- US120f

Firmware:

US320f

- 1.04-INTL

US310e

- 1.10-INTL
- 1.20-INTL
- 1.30-INTL

Important

If ADM and the old version of US310e firmware are used together, some of the functions of ADM cannot be supported. It is recommended to upgrade the US310e firmware to 1.30-INTL or apply 1.20-INTL Update Package ver 1.3 for ADM to 1.20-INTL.

US120f

- 8.43-FAKC
- 8.51-CAKD

Note

- The supported client list above is not exhausted; newly developed models may be included in the future.
- For more information on detailed specifications of different models, visit our website at <http://www.nec.com>.

1.4.2 Supported Platforms

- Windows 7
- Windows 8 / 8.1
- Windows 10
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2
- Windows Server 2016

Important

The server on which you install ADM should be dedicated to ADM services and should not be performing additional functions. For example, the server should not be functioning as a Domain Controller, Backup Controller, Mail Server, Production Web Server, DHCP Server, MSMQ Server, or Application Server.

1.4.3 Hardware Requirements

- Pentium 4, 1.0 GHz processor or the equivalent
- 512 MB of free system memory
- 2 GB of free disk space for installation / 100 GB or more for firmware and snapshot management
- 100 Mb Ethernet network adapter / network interface card

1.4.4 Used ports

Background Service and Used Ports for ADM					
No.	Service Name	Source	Source port Number	Destination	Destination Port Number
1	Atrust – Apache 2.2 (Local use only)	ADM	Any	ADM	TCP/10443
2	Atrust – Apache 2.2	Thin Client	Any	ADM	TCP/10080
3		ADM	TCP/10080	Thin Client	Any
4	Atrust - Multicast	Thin Client	Any	ADM	Both/10081
5		ADM	Both/10081	Thin Client	Any
6	Atrust - PostgreSQL (Local use only)	ADM	Any	ADM	TCP/5432
7	Atrust Device Manager	ADM	UDP/Any	Thin Client	UDP/10005
8		Thin Client	UDP/10005	ADM	UDP/Any
9		ADM	TCP/Any	Thin Client	TCP/10005
10		Thin Client	TCP/Any	ADM	TCP/10005
11		Thin Client	TCP/10005	ADM	TCP/Any
12		ADM	Both/Any	ADM	Both/10006
13		Thin Client	Any	ADM	TCP/10007
14		ADM	TCP/10007	Thin Client	Any
15	VNC	ADM	Any	Thin Client	TCP/5900
16		Thin Client	TCP/5900	ADM	Any

Note

- You can find the Service Name on Windows Services management console.
- “Any” in above table means ADM or thin client uses ephemeral port assigned by OS.
- At "Both" in above, a protocol of both of TCP and UDP is used.

Important

- It isn't necessary to add firewall exceptions manually. ADM automatically configures everything you need for ADM use with respect to HTTP server, database, and the Windows Firewall when this software is installed.
- ADM does not support changing the default port numbers.

1.4.5 Configuring the network environment

Installing a DHCP server

When using only US320f and US120f, the DHCP server isn't indispensable. It's because fixed IP address information is available for establishment of network link at UEFI bootup. The fixed IP information configured at the respective thin clients becomes effective. DHCP server is essential in environment including US310e.

Wake on LAN

Wake on LAN messages cannot be sent to a thin client that does not belong to the same segment as ADM. It's because a magic packet on layer 2 which is broadcasted for Wake on LAN cannot be sent to any PC located in a different segment.

Note

Wake on LAN is used in a wired LAN environment. It cannot be used for a wireless LAN client.

Important

US120f does not support resume from suspend via Wake on LAN.

VPN

ADM cannot be used in a remote access VPN environment in which VPN software is used on a thin client to implement Network Address Translation (NAT).

Note

ADM can be used in cases when a site-to-site VPN is configured between routers that have VPN software installed but do not perform Network Address Translation (NAT).

Important

Note that no ADM features are supported in a remote access VPN environment.

Wireless LAN

Updating firmware, taking snapshots, and installing thin clients cannot be performed in a wireless LAN environment.

Note

Features other than those described above can be used in a wireless LAN environment.

IEEE 802.1x authentication

Updating and installing firmware, and taking snapshots cannot be performed if user authentication is executed by using IEEE 802.1x (that is, EAP-PEAP or EAP-TLS) in a wired or wireless LAN environment. Thin clients need to establish a network link at UEFI bootup to obtain the firmware update and snapshot image files from the server; however, thin clients do not support IEEE 802.1x authentication.

Chapter 2 Installing and Upgrading ADM

This chapter gives detailed instructions on how to install and upgrade your ADM.

2.1 Installing ADM

The installation of ADM

2.2 Initial Setup

The initial setup of ADM

2.3 Upgrading ADM

The upgrade of ADM

2.4 Stopping Atrust-Multicast Service

The stop of Atrust-Multicast Service to manage US320f by ADM

2.5 Uninstalling ADM

The uninstallation of ADM

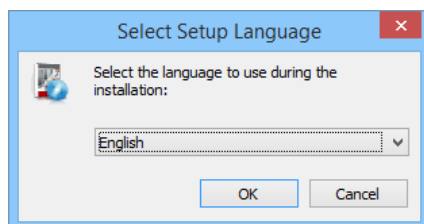
2.1 Installing ADM

To install ADM on your computer, please follow the steps below:

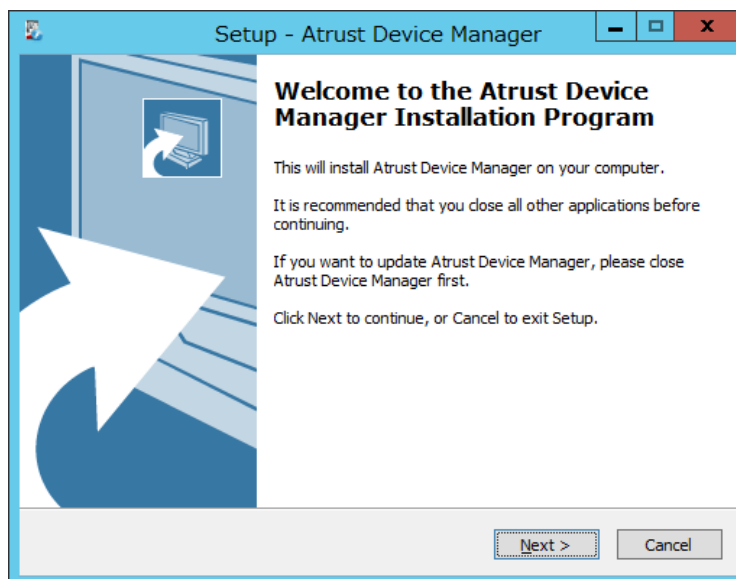
Note

- Before proceeding, ensure that. Your operating system is supported (see "1.4 System Requirements")
- Before proceeding, ensure that. Your computer meets system requirements (see "1.4 System Requirements")
- To install a newer version of ADM, it's recommended to install it directly without uninstalling the current ADM. For more information on how to upgrade your ADM, please refer to section "2.3 Upgrading ADM".
- Setting up a static IP address on your computer.

1. Get a copy of the installation program of ADM for your computer.
2. Log in to your computer with an administrator account, and then locate and double-click that program.
3. Select the language used during the installation.



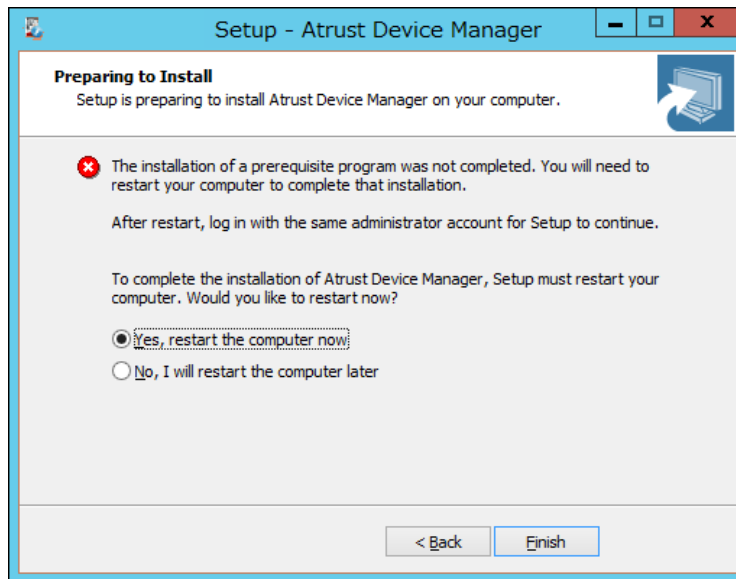
4. The Setup Wizard appears. Click **Next** to continue.



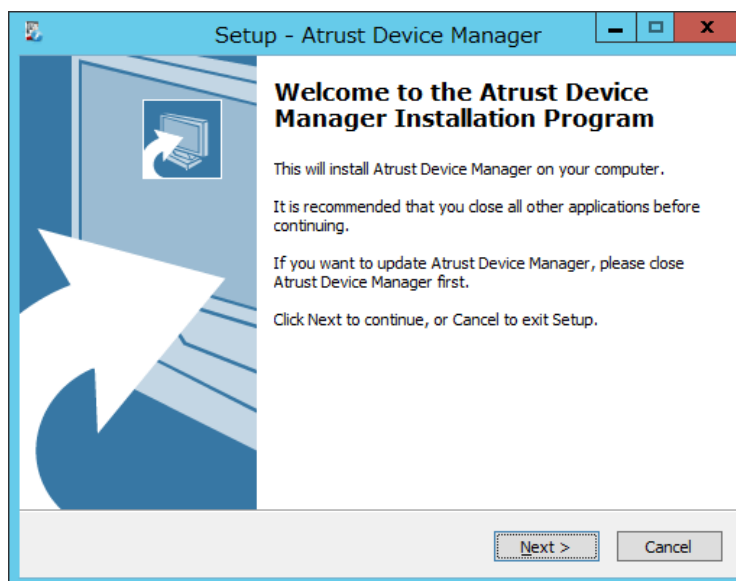
Note

It may take a few seconds for the wizard to enter the next page/step while preparing for the installation of ADM.

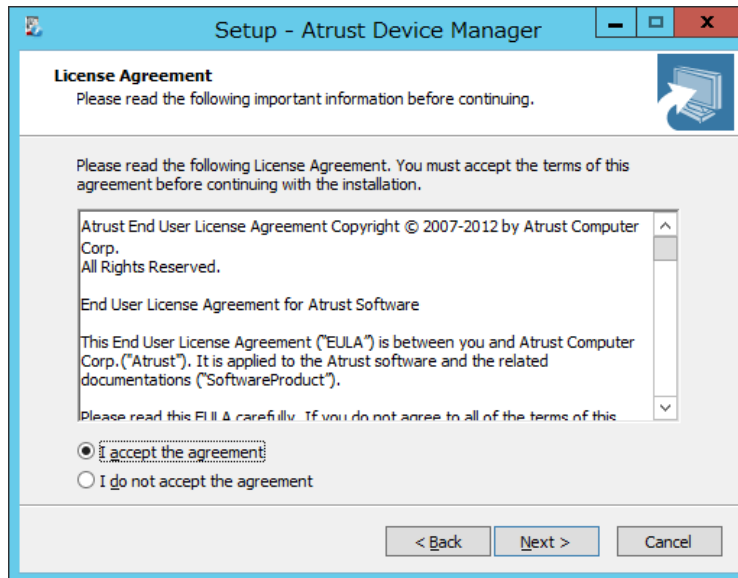
5. A message appears prompting you to restart for the installation of a prerequisite program. Select **Yes, restart the computer now**, and then click **Finish**.



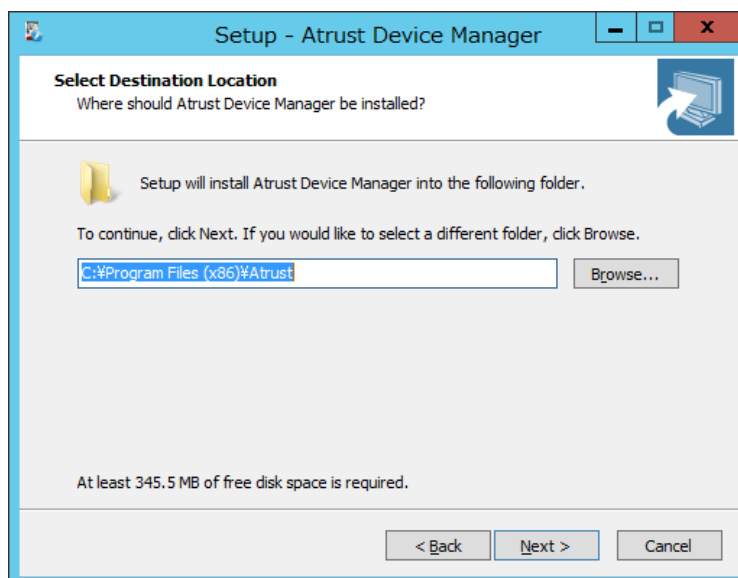
6. After restart, the Setup Wizard appears again. Click **Next** to continue.



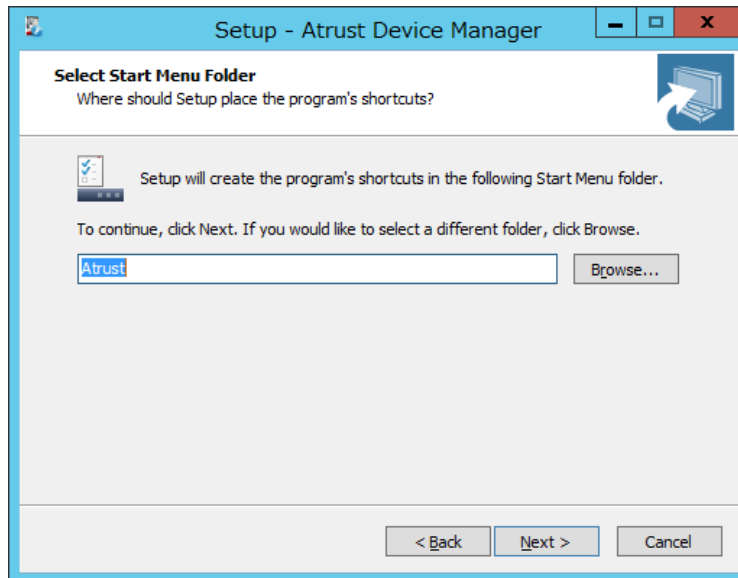
7. The License Agreement page appears. Read this agreement, select **I accept the agreement**, and then click **Next** to continue.



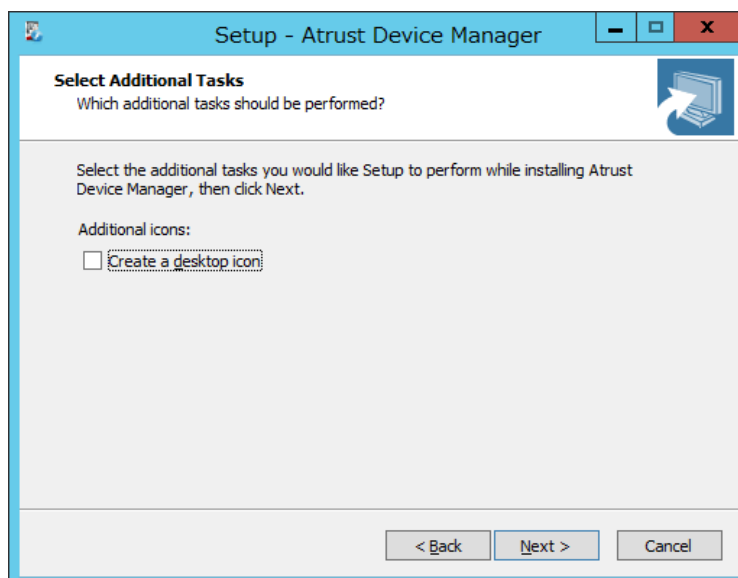
8. Use the default installation directory or click **Browse** to locate the desired one, and then click **Next** to continue.



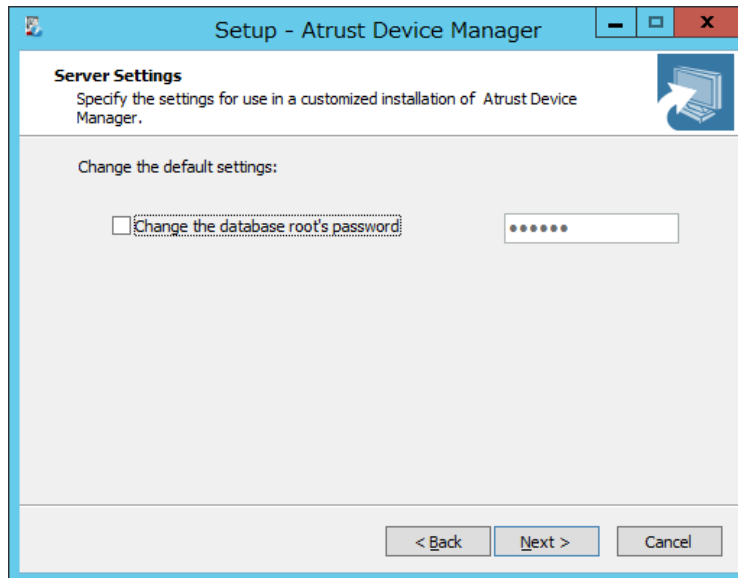
9. Use the default Start menu folder or type to create a new folder for the shortcuts of programs. Or, click **Browse** to choose an existing folder. Click **Next** to continue.



10. Select or clear **Create a desktop icon**, and then click **Next** to continue.

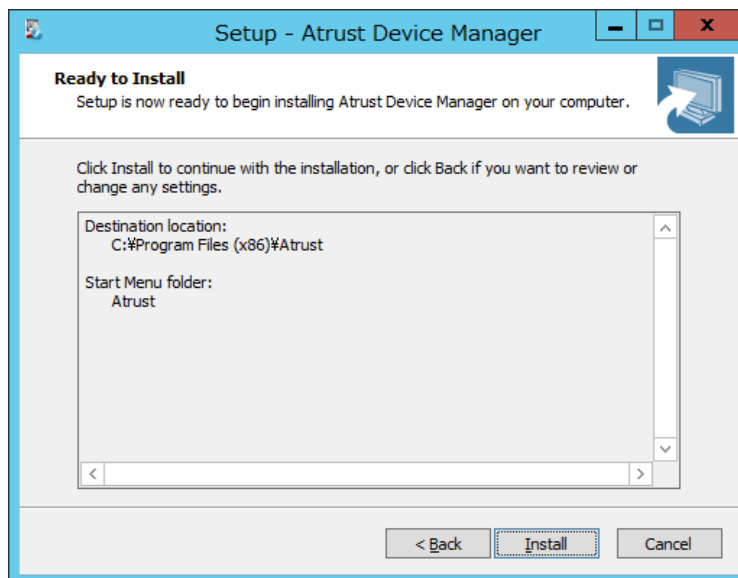


11. Change the default database password for the superuser or use the default. After completion, click **Next** to continue.

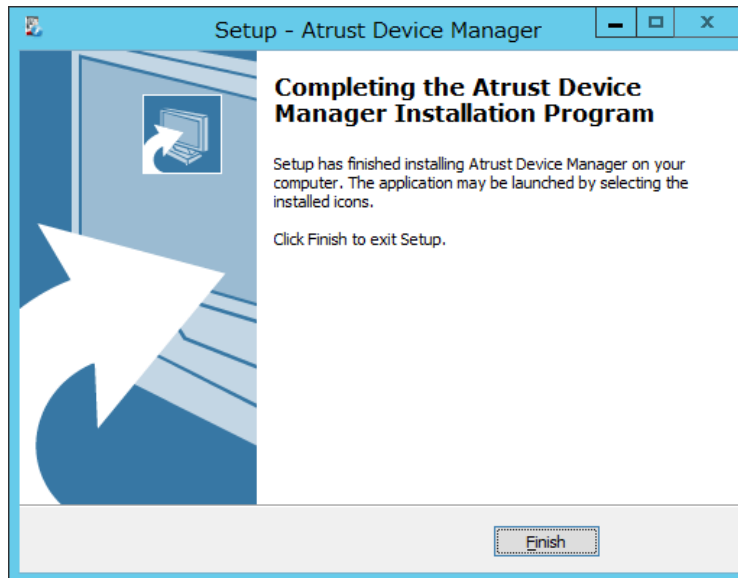
**Note**

- A superuser is a user who has full access to the database of ADM.
- The default password is "secret".

12. Click **Install** to start installing ADM on your computer.



13. After completion, click **Finish** to exit.



2.2 Initial Setup

On first boot of ADM, you need to complete the initial setup. Follow the instructions below to complete the required configuration:

1. Launch ADM on your computer.
2. A window appears prompting you to choose the service IP address and create an administrator account. Click the drop-down menu to select the desired IP address from the list of available IP addresses, type the desired account name and password, and then click **Save** to continue.

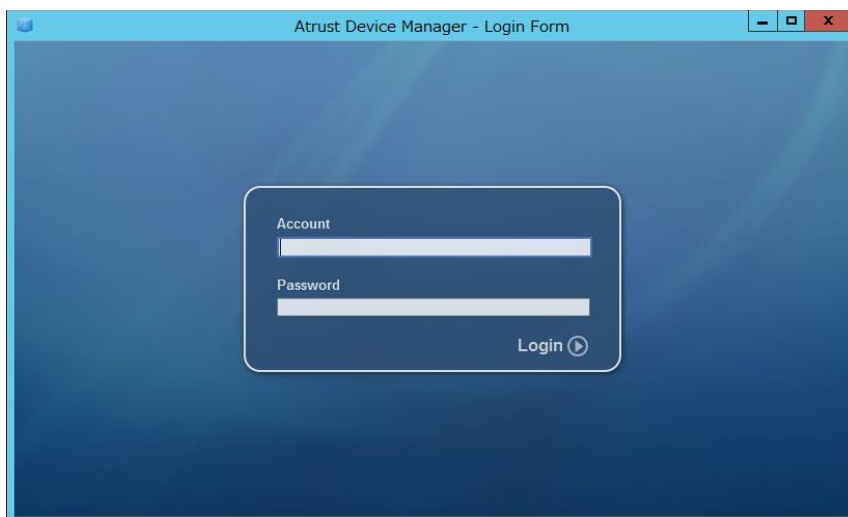
A screenshot of the "Atrust Device Manager Setup Wizard" window. The title bar is grey with the text "Atrust Device Manager Setup Wizard" in blue. The window is divided into two sections. The first section, "Choose service IP address", contains a label "IP Address:" and a drop-down menu showing "192.168.7.1". The second section, "Create default administrator account", contains three labels: "Account:", "New Password:", and "Confirm Password:", each followed by a text input field. A "Save" button is located at the bottom right of the window.

Note

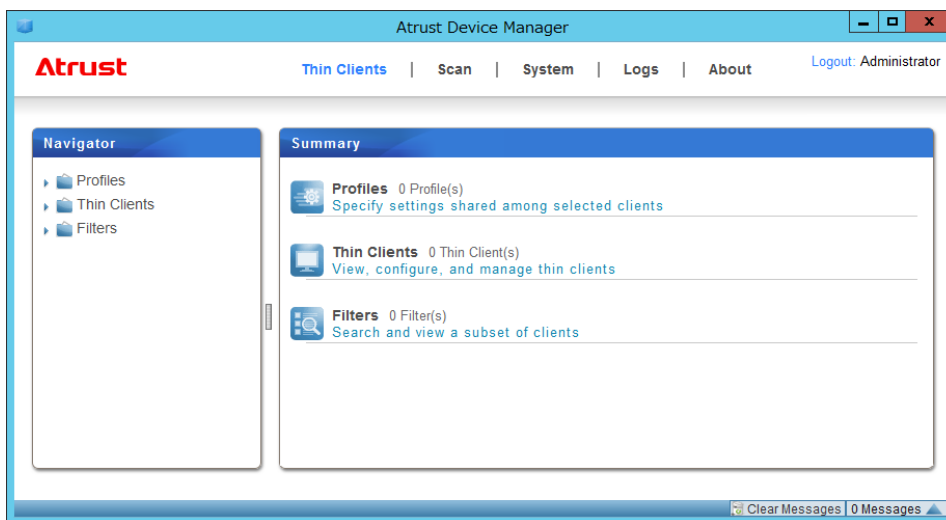
- The unconnected LAN port may appear in the list of available IP addresses with the address value **0.0.0.0**.

- It is strongly recommended to use a fixed IP address as the service IP of ADM. The change of the service IP may make all the managed clients become unmanageable.

3. The Login screen appears prompting you to sign in to ADM with your credentials (account name and password).



4. The management interface of ADM appears.



Note In next chapter, we will describe the functionality and use of ADM in details.

2.3 Upgrading ADM

To upgrade your ADM to a newer version, you can just install the new program without uninstalling the old one. For information on how to install ADM, please refer to section "2.1 Installing ADM"

Note

It is highly recommended to upgrade your ADM without uninstalling the old version. If you uninstall the current ADM on a computer, all your settings and client CA (Certificate Authority) files will be removed. With a newly installed ADM, this computer will fail to manage clients which are originally under its management, and those clients will become unmanageable.

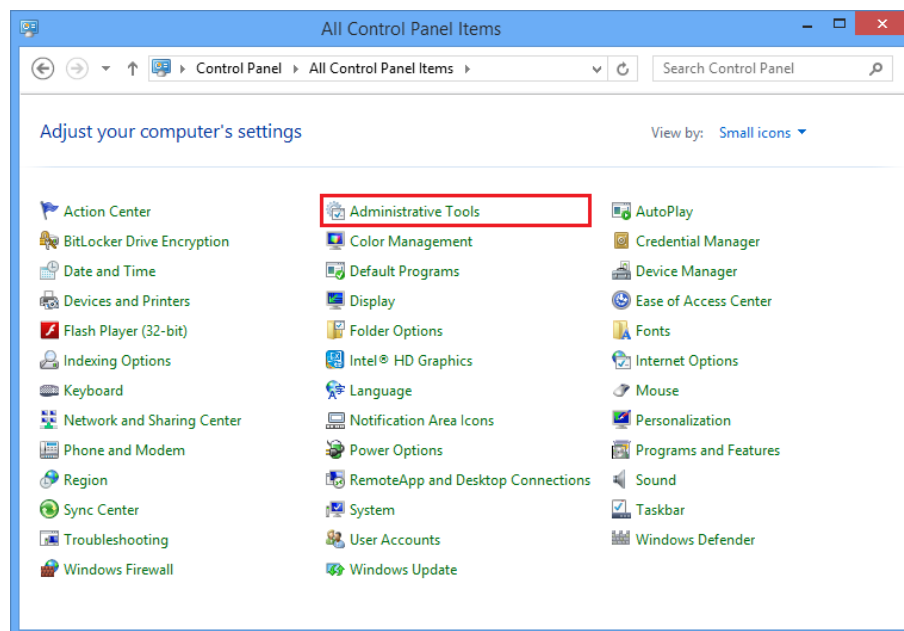
Important

Before upgrading your ADM, ensure that you've logged out and closed the ADM console.

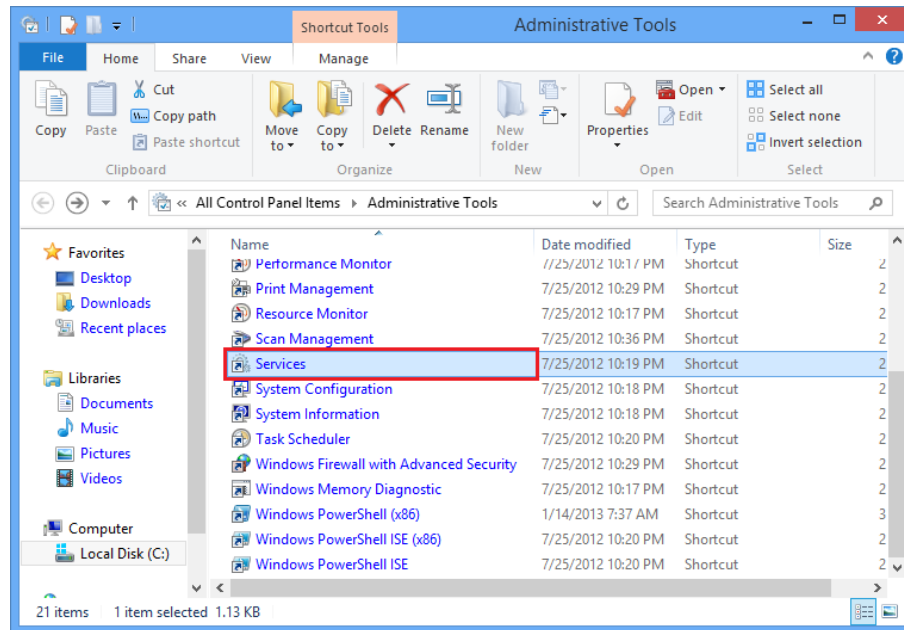
2.4 Stopping Atrust-Multicast Service

When you manage US320f by ADM, it is necessary to stop Atrust-Multicast Service. Follow the steps below to stop Atrust-Multicast Service. You need not stop the service if you don't manage US320f by ADM.

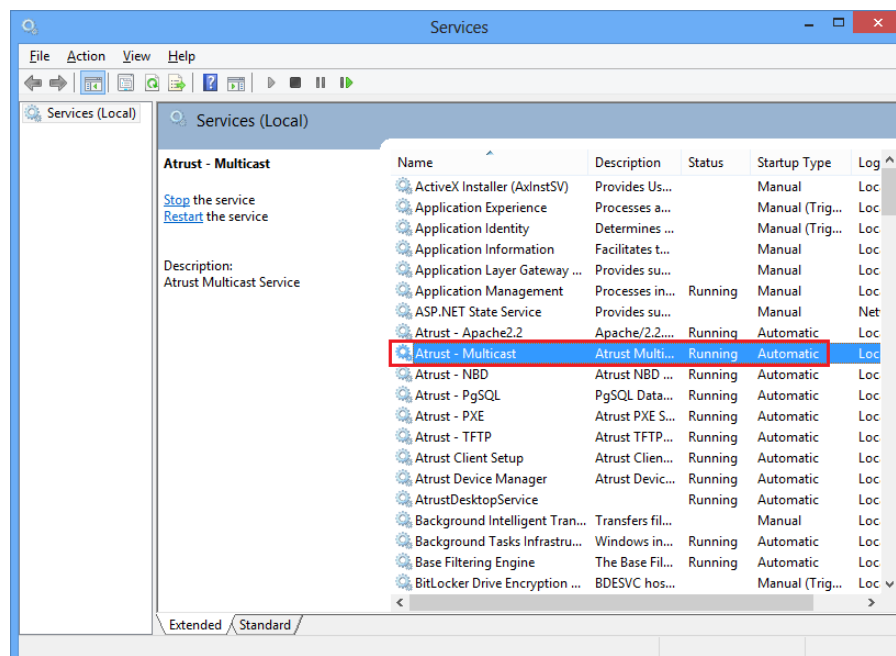
1. Choose **Control Panel > Administrative Tools**.



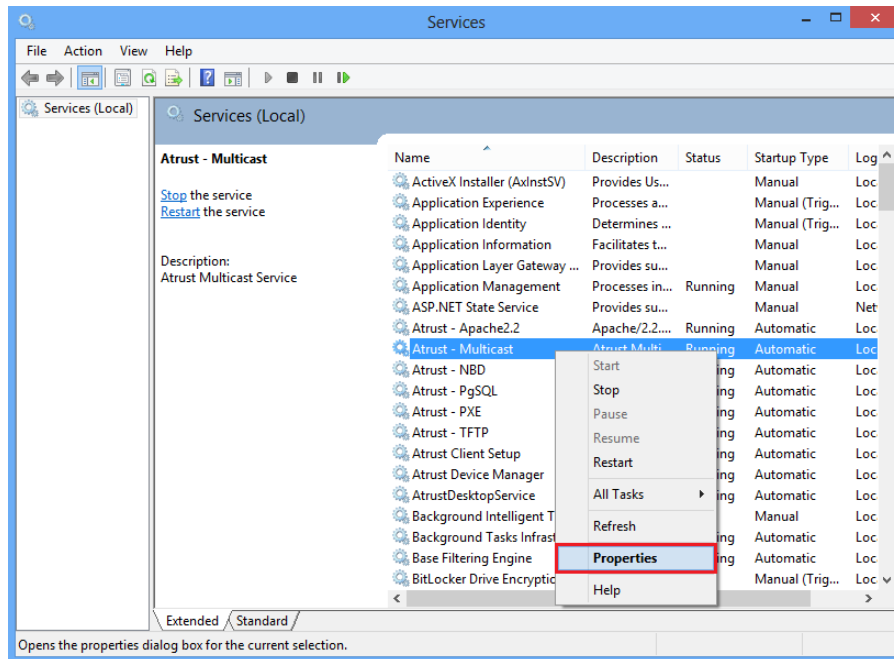
2. Double-click **Services** in the Administrative Tools.



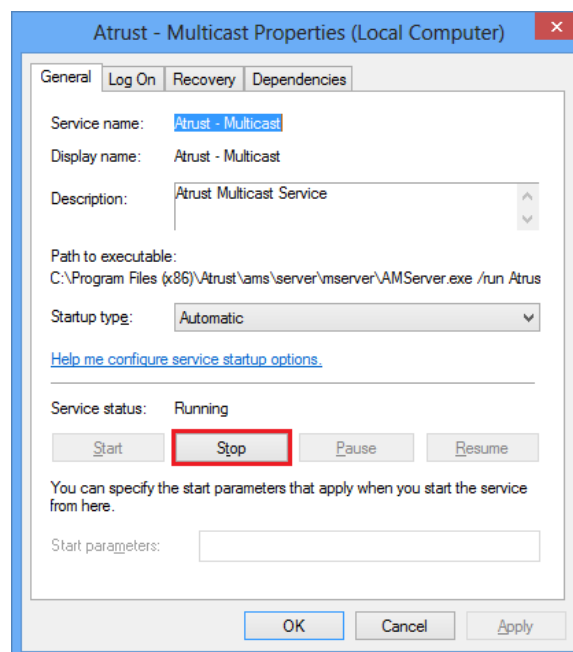
3. Select **Atrust - multicast** from Windows services list.



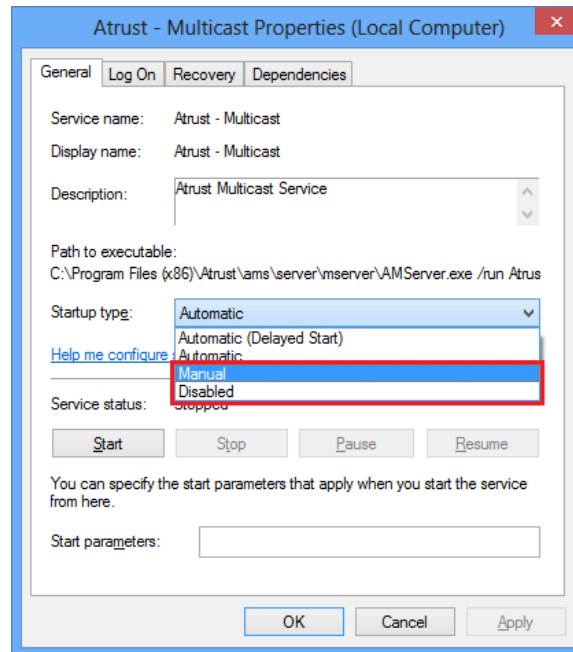
4. Click **Properties** on the right-click menu.



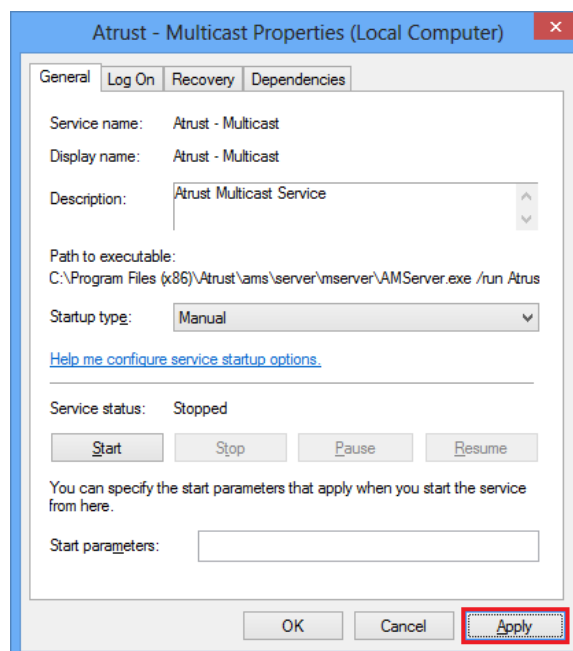
5. Click **Stop** button in **General** tab.



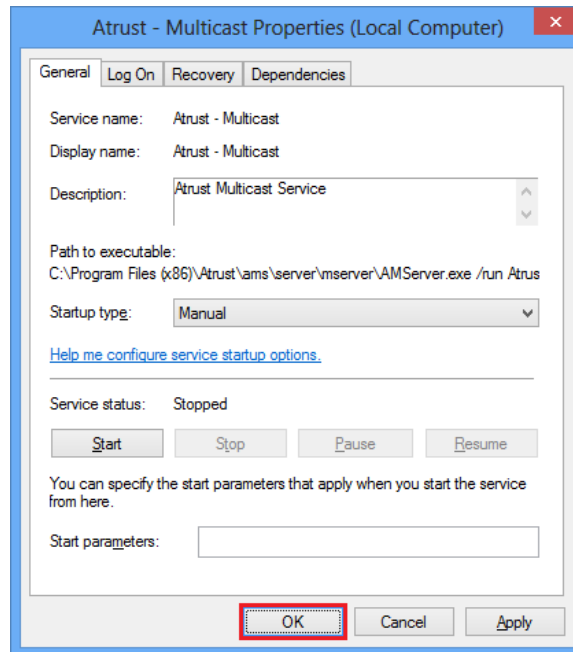
6. choose **Manual** or **Disabled** from the Startup type drop-down menu.



7. Click **Apply** button.



8. Click **OK** button.



9. Close Services window.
10. A stop of Atrust-Multicast Service is completion.

2.5 Uninstalling ADM

To uninstall ADM on your computer, please do the following:

Note

- To upgrade your ADM, it's recommended not to uninstall the current ADM. For more information, please refer to section "2.3 Upgrading ADM".
- It is strongly recommended to use a fixed IP address as the service IP of ADM. The change of the service IP may make all the managed clients become unmanageable.

Important

Before uninstalling your ADM, ensure that you've logged out and closed the ADM console.

1. Uninstall your ADM through the Control Panel.
2. Follow the on-screen instructions to complete the uninstallation.

Chapter 3 Using ADM

This chapter provides instructions on how to manage clients with ADM.

3.1 ADM

Interface Overview

Available Tasks at a Glance

3.2 Establishing a Basic Administration Environment

System Tab Overview

Available Tasks at a Glance

3.3 Adding Clients into a Managed Group

Scan Tab Overview

Available Tasks at a Glance

3.4 Managing All Your Clients

Thin Clients Tab Overview

Available Tasks at a Glance

3.5 Viewing and Managing Event Logs

Logs Tab Overview

Available Tasks at a Glance

3.6 Viewing Software Information

About Tab Overview

Available Tasks at a Glance

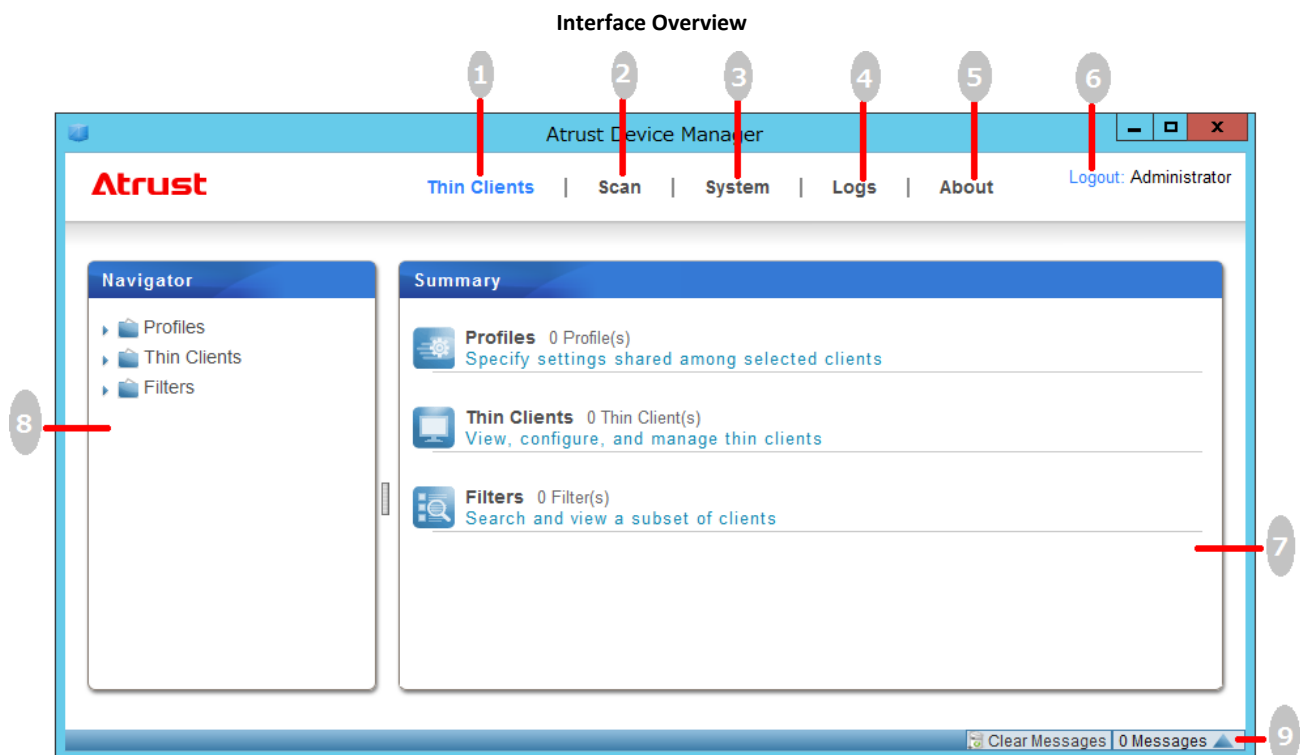
3.1 ADM

ADM enables you to remotely deploy, manage, update clients, and assist users from a single computer. You can manage clients simply and quickly in groups with a flexible and secure mechanism. Additionally, you can remotely assist users in resolving problems or configuring local settings.

3.1.1 Interface Overview

To access ADM, please do the following:

1. Launch ADM on your computer.
2. Type your credentials, and then press **Enter** or click **Login**. The ADM window appears.



Interface Elements		
No.	Name	Description
1	Thin Clients tab	Click to access client management.
2	Scan tab	Click to look for unmanaged thin clients over your local network.
3	System tab	Click to establish and configure the basic administration environment.
4	Logs tab	Click to view event logs.
5	About tab	Click to view information about ADM.
6	Logout button	Click to log out from ADM.
7	Management / Information Area	Select to perform desired tasks, configure desired settings, or view related information available under a selected tab.
8	Navigation Area	Click to select a specific item, option, or task under a tab.
9	Message Area	Click to view messages about management activities.

3.1.2 Available Tasks at a Glance

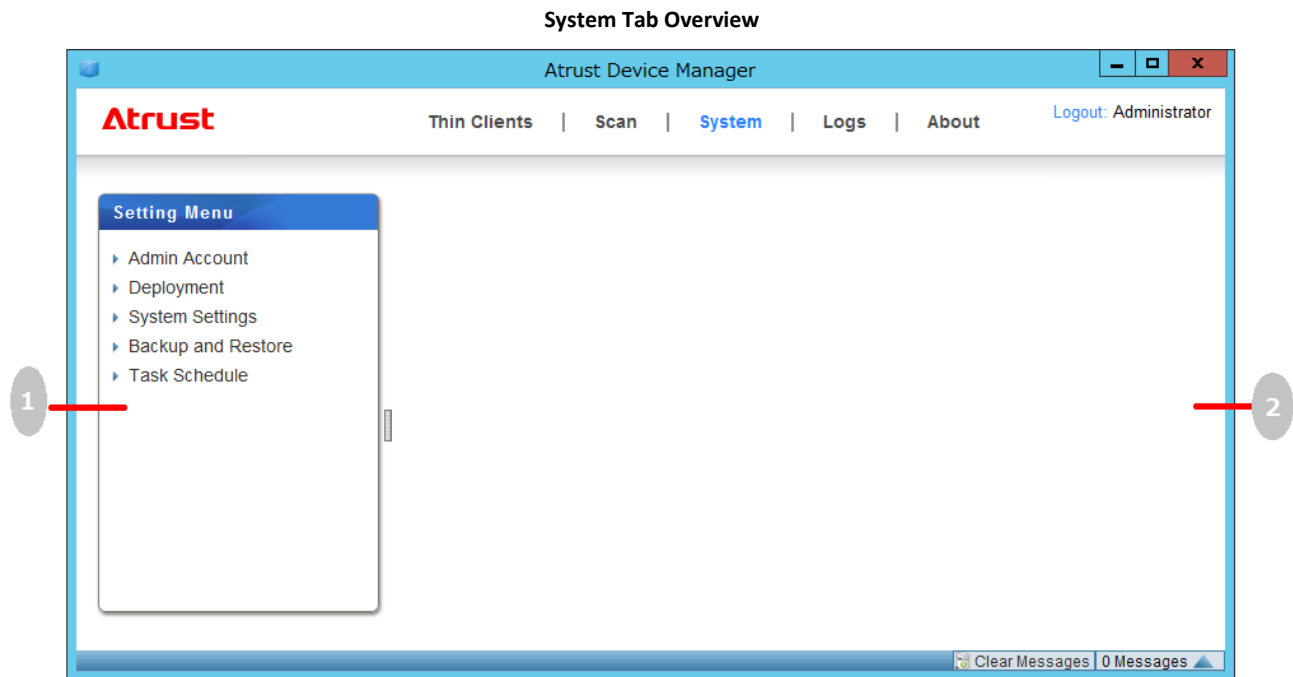
The following table shows functionality provided in each tab. For more details, please refer to the corresponding section as shown below:

Tab	Function List	Section
System	<ul style="list-style-type: none"> • Creating accounts for administration • Managing thin client firmware files • Managing zero client image files • Managing WES package files • Managing client snapshots • Managing certificates of remote computers • Configuring remote deployment settings • Specifying deployed servers • Specifying ADM settings • Backing up the management database • Managing database archive files • Restoring the management database • Task scheduling 	3.2 Establishing a Basic Administration Environment
Scan	<ul style="list-style-type: none"> • Looking for clients in the whole range of a local network • Looking for clients in a specified range of IP addresses • Looking for clients with predefined IP range lists • Detecting clients including "password-protected" clients 	3.3 Adding Clients into a Managed Group
Thin Clients	<ul style="list-style-type: none"> • Getting zero clients ready for use • Creating group configuration for clients • Using individualized configuration for clients • Using hybrid configuration for clients • Pushing settings to clients • Pulling settings from clients • Pushing certificates to clients • Sending messages to clients • Rebooting clients remotely • Shutting down clients remotely • Wake-On-LAN of clients • Updating client firmware • Installing and Uninstalling Software Packages • Taking snapshots • Installing snapshots • Using the Shadow Feature • Controlling clients remotely • Exporting client data • Detecting profiles/clients/logs using quick search • Managing filters 	3.4 Managing All Your Clients
Logs	<ul style="list-style-type: none"> • Viewing event logs • Exporting event logs • Deleting event logs 	3.5 Viewing and Managing Event Logs
About	<ul style="list-style-type: none"> • Viewing information on ADM • Viewing Atrust contact information • Viewing Software License Agreement 	3.6 Viewing Software Information

3.2 Establishing a Basic Administration Environment

3.2.1 System Tab Overview

System tab enables you to establish a basic administration environment. To access the functionality of **System** tab, click the tab on ADM.



Interface Elements		
No.	Name	Description
1	Navigation Area	Click to access the desired setting item.
2	Management Area	Select to perform desired tasks, configure desired settings, or view related information available under a selected item.

3.2.2 Available Tasks at a Glance

No.	Available Task	Section
1	Creating accounts for administration	3.2.3
2	Deleting an account	
3	Editing an account	
4	Importing thin client firmware files	3.2.4
5	Deleting thin client firmware files	
6	Scanning thin client firmware files	
7	Importing WES package files	3.2.5
8	Deleting WES package files	
9	Scanning WES package files	
10	Exporting client snapshots	3.2.6
11	Importing client snapshots	
12	Deleting client snapshots	
13	Scanning client snapshots	3.2.7
14	Importing certificates	
15	Deleting certificates	
16	Configuring remote deployment settings	3.2.8
17	Selecting the service IP address of ADM	3.2.9
18	Configuring auto-logout for ADM	3.2.10
19	Configuring Auto Registration	3.2.11
20	Configuring Password Protection for Managed Devices	3.2.12
21	Configuring the database source of ADM	3.2.13
22	Selecting the interface language of ADM	3.2.14
23	Backing up the management database	3.2.15
24	Downloading a database archive file	3.2.16
25	Uploading a database archive file	
26	Deleting a database archive file	
27	Restoring a database archive file	3.2.17
28	Scheduling automatically performed tasks	3.2.18

3.2.3 Managing Accounts for Administration

Creating an Account

To create an account for administration, please do the following:

1. On **System** tab, click **Admin Account**.
2. The Account list appears in Management area.

+ Add - Delete Edit

Username	Information	Last login	Authority
Administrator		2017-03-15 09:51:10	Admin

Note

When you log in to ADM for the first time, you are prompted to create an administrator account for client management. This account will be specified in the Account list.

3. Click **Add** to open the Add window.
4. Type the desired user/account name and password.

Add

Username: *

New Password: *

Confirm Password: *

Information:

Authority: Admin

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

* The maximum length of password is 40.

Add Cancel

Note

You can click Authority drop-down menu to choose its type: Admin or User. The former has complete access to ADM; the latter is only for viewing Thin Clients and Logs tabs.

5. Click **Add** to apply.
6. The newly added account appears in the Account list.

+ Add - Delete Edit

Username	Information	Last login	Authority
Administrator		2017-03-15 09:51:10	Admin
TestUser	TEST USER		Admin

Deleting an Account

To delete an account, please do the following:

1. On **System** tab, click **Admin Account**.
2. The Account list appears in Management area.
3. Click to select the desired account.

Note

To delete more than one account, Ctrl-click to select multiple accounts.

4. Click **Delete** on the top of the Account list.
5. The Delete window appears prompting for confirmation.
6. Click **Yes** to confirm.
7. The selected account is removed from the Account list.

Adjusting an Account

To adjust an existing account, please do the following:

1. On **System** tab, Click **Admin Account**.
2. The Account list appears in Management area.
3. Click to select the desired account.
4. Click **Edit** to open the Edit window.
5. Adjust the password or the description in the Information field.

Note

If you only want to add or edit the description in the Information field, you need to type the current password for the selected account.

6. Click **Modify** to apply.

3.2.4 Managing Thin Client Firmware Files

You can update firmware for your clients remotely with ADM. Before proceeding, you need to import firmware files of appropriate versions for ADM.

Note For instructions on how to update firmware for clients remotely, please see section "3.4.23 Updating Client Firmware".

Importing Thin Client Firmware Files

To import a firmware file for thin clients, please do the following:

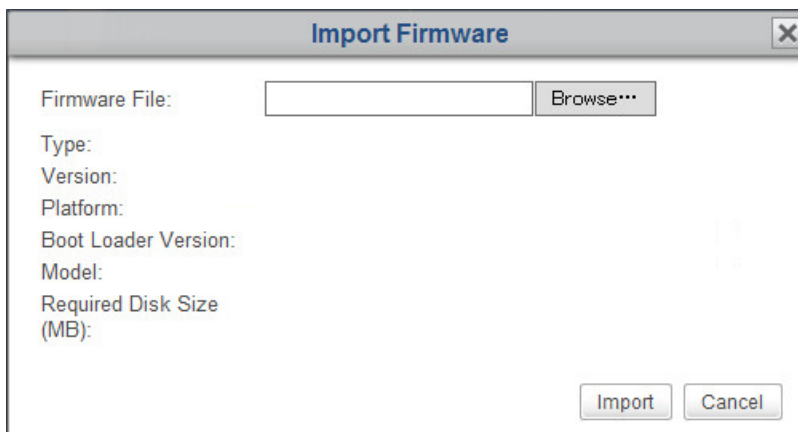
1. On **System** tab, click **Deployment > Firmware**.
2. The Firmware list appears.

 Scan Firmware
  Delete Firmware
  Import Firmware

Name	Platform	Version	Model
ARM LINUX 8.43-FAKC	ARM Linux	8.43	US120f

Note If you have never imported firmware files into ADM, the Firmware list will be empty as shown above.

3. Click **Import Firmware** on the top of the Firmware list.
4. The Import Firmware window appears.



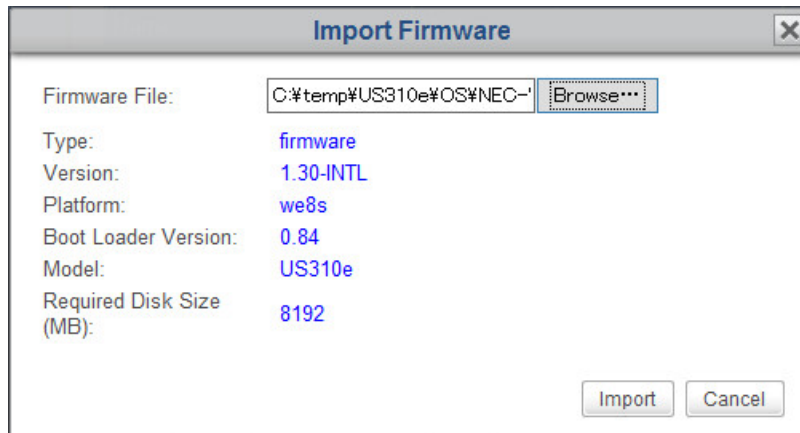
The 'Import Firmware' dialog box contains the following fields and controls:

- Firmware File:** A text input field with a 'Browse...' button to its right.
- Type:** A text input field.
- Version:** A text input field.
- Platform:** A text input field.
- Boot Loader Version:** A text input field.
- Model:** A text input field.
- Required Disk Size (MB):** A text input field.
- Buttons:** 'Import' and 'Cancel' buttons at the bottom right.

5. Click **Browse** to locate the desired firmware file, and then click **Open** to confirm.

Note ADM will automatically perform file check to ensure that the file is a valid firmware file for thin clients and there is no duplicate in the Firmware list.

6. Click **Import** to start importing the selected firmware file.



7. On completion, the imported firmware file appears as an entry in the Firmware list.

Scan Firmware
 Delete Firmware
 Import Firmware

Name	Platform	Version	Model
ARM LINUX 8.43-FAKC	ARM Linux	8.43	US120f
WE8S 1.30-INTL	Windows Embedded 8 Standard	1.30	US310e

Deleting Thin Client Firmware Files

To delete a thin client firmware file, please do the following:

1. On **System** tab, click **Deployment > Firmware**.
2. The Firmware list appears in Management area.
3. Click to select the desired firmware file, and then click **Delete Firmware** on the top of the Firmware list.

Note To delete more than one firmware file, Ctrl-click to select multiple files.

4. The Delete Firmware window appears prompting you for confirmation.
5. Click **Delete** to confirm.
6. On completion, the selected firmware file is removed from the Firmware list.

Scanning Thin Client Firmware Files

The **Scan Firmware** feature helps you to discover the local or remote firmware files. There are two scenarios that you need the help of this feature. The first scenario is that you choose to update clients with remote firmware files rather than local imported ones. In this scenario, the local list of available firmware in ADM may be not in sync with the remote list of firmware files on another computer where you choose to get firmware files. The **Scan Firmware** feature can synchronize your local list with the remote one.

Note

For instructions on how to configure your ADM to use remote firmware files on another computer for client management, please refer to section "3.2.8 Configuring Remote Deployment Settings"

The other scenario is when you copy the file set of an imported firmware file from the installation directory of another ADM into the same installation directory of your ADM, this firmware file may not appear as an entry in the Firmware list.

Note

The default installation directory of ADM is C:\Program Files (x86)\Atrust. The file set of an imported firmware file is placed in C:\Program Files (x86)\Atrust\firmware, under an uppermost dedicated folder.

In both scenarios, to synchronize the entries in the Firmware list with your local or remote firmware files, please do the following:

1. On **System** tab, Click **Deployment > Firmware**.
2. The Firmware list appears in Management area.
3. Click **Scan Firmware** on the top of the Firmware list.
4. On completion, the Firmware list is now in sync with your local or remote firmware files.

3.2.5 Managing WES Package Files

With Windows Embedded Standard (called WES below) package files, you can install applications or language packs remotely for your WES-based thin clients. Before proceeding, you need to import package files of appropriate versions into ADM.

Note

- The WES version of your client may not support multiple user interface packs. In this case, installing a language pack for a client will replace its display (user interface) language with the new one.
- For instructions on how to update your WES clients with package files remotely, please refer to "3.4.24 Installing and Uninstalling Software Packages"

Importing WES Package Files

To import a WES package file, please do the following:

1. On **System** tab, click **Deployment > WES Package**.
2. The Package list appears.

🔍 Scan Package 🗑️ Delete Package 📁 Import Package				
Name	Category	Version	Req. Firmware	Platform
VMware Horizon Client 3.5.2	Application	1.1	1.20-INTL	Windows Embedded 8 Standard

Note

If you never imported WES package files into ADM, the Package list will be empty as shown above.

3. Click **Import Package** on the top of the list.
4. The Import Package window appears.

5. Click **Browse** to locate the desired package file, and then click **Open** to confirm.

Note

ADM will automatically perform file check to ensure it's a valid package file for WES-based clients and there is no duplicate in the Package list.

- Click **Import** to start importing the desired package file.



- On completion, the imported package file appears as an entry in the Package list.

Scan Package
 Delete Package
 Import Package

Name	Category	Version	Req. Firmware	Platform
VMware Horizon Client 3.5.2	Application	1.1	1.20-INTL	Windows Embedded 8 Standard
Citrix Receiver 4.4 with SSON	Application	1.2	1.20-INTL	Windows Embedded 8 Standard

Deleting WES Packages

To delete a WES package file, please do the following:

- On **System** tab, click **Deployment > WES Package**.
- The Package list appears.
- Click to select the desired package file, and then click **Delete Package**.
- The Delete Package window appears prompting you for confirmation.
- Click **Delete** to confirm.
- The selected package file is removed from the Package list.

Scanning WES Packages

The **Scan Package** feature helps you to discover the local or remote WES package files. There are two scenarios that you need the help of this feature. The first scenario is that you choose to update clients with remote package files rather than local imported ones. In this scenario, the local list of available packages in ADM may be not in sync with the remote list of packages on another computer where you choose to get package files. The **Scan Package** feature can synchronize your local list with the remote one.

Note

For instructions on how to configure your ADM to use remote package files on another computer for client management, please refer to section "3.2.8 Configuring Remote Deployment Settings"

The other scenario is when you copy the file set of an imported package file from the installation directory of another ADM into the same installation directory of your ADM, this package file may not appear as an entry in the Package list.

Note

The default installation directory of ADM is C:\Program Files (x86)\Atrust. The file set of an imported package file is placed in C:\Program Files (x86)\Atrust\packages, under an uppermost dedicated folder.

To synchronize entries in the Package list with the local or remote package files, please do the following:

1. On **System** tab, click **Deployment > WES Package**.
2. The Package list appears in Management area.
3. Click **Scan Package** on the top of the list.
4. On completion, the package file is added as an entry in the Package list.

3.2.6 Managing Client Snapshots

A snapshot is the system copy of a client at a specific point of time, which you can use for mass deployment, system backup, and recovery.

Important US120f does not support snapshots.

Note For instructions on how to take a system snapshot for clients, please refer to section "3.4.25 Taking Client Snapshots".

Exporting Client Snapshots

To export a client snapshot, please do the following:

1. On **System** tab, click **Deployment > Snapshot**.
2. The Snapshot list appears in Management area.

Note The Snapshot list might be empty, if you never took or imported client snapshots.

3. Click to select the desired client snapshot, and then click **Export Snapshot** on the top of the list.
4. The Export Snapshot window appears prompting for confirmation.
5. Click **Export** to confirm.
6. A window appears prompting you to choose either opening or saving the exported file.
7. Click to select **Save File**, and then click **OK** to confirm.
8. In the opened window, choose the location to save the exported file, and then click **Save** to confirm.

Importing Client Snapshots

To import a client snapshot, please do the following:

Note Ensure that you have got the desired client snapshot (.zip format) which is taken and exported from ADM on this or another computer.

1. On **System** tab, click **Deployment > Snapshot**.
2. The Snapshot list appears.
3. Click **Import Snapshot** on the top of the Snapshot list.
4. The Import Snapshot window appears.
5. Click **Browse** to locate the desired client snapshot, and then click **Open** to confirm.

Note ADM will automatically perform file check to ensure that the file is a valid snapshot and there is no duplicate in the Snapshot list.

6. Click **Import** to start importing the desired snapshot.
7. On completion, the snapshot appears as an entry in the Snapshot list.

Deleting Client Snapshots

To delete a client snapshot, please do the following:

1. On **System** tab, click **Deployment > Snapshot**.
2. The Snapshot list appears.
3. Click to select the desired snapshot, and then click **Delete Snapshot** on the top of the list.
4. The Delete Snapshot window appears prompting for confirmation.

Note To delete more than one snapshot, Ctrl-click to select multiple snapshots.

5. Click **Delete** to confirm.
6. The selected snapshot is removed from the Snapshot list.

Scanning Client Snapshots

The **Scan Snapshot** feature helps you to discover the local or remote client snapshots. There are two scenarios that you need the help of this feature. The first scenario is that you choose to restore clients with remote snapshots rather than local imported ones. In this scenario, the local list of available snapshots in ADM may be not in sync with the remote list of snapshots on another computer where you choose to get snapshots.

The **Scan Snapshot** feature can synchronize your local list with the remote one

Note For instructions on how to configure your ADM to use remote snapshots on another computer for client management, please refer to section "3.2.8 Configuring Remote Deployment Settings".

The other scenario is when you copy a snapshot file set from the installation directory of another ADM into the same installation directory of your ADM, this snapshot may not appear as an entry in the Snapshot list.

Note The default installation directory of ADM is C:\Program Files (x86)\Atrust. All snapshots taken or imported through ADM are placed in C:\Program Files (x86)\Atrust\snapshot, under an uppermost dedicated folder.

To synchronize entries in the Snapshot list with your local or remote snapshots, please do the following:

1. On **System** tab, click **Deployment > Snapshot**.
2. The Snapshot list appears in Management area.
3. Click **Scan Snapshot** on the top of the list.
4. On completion, the snapshot is added as an entry in the Snapshot list.

3.2.7 Managing Certificates

Important

The function to push certificates is supported only by US120f. This function is not supported by US320f and US310e. For information on how to push certificates, please refer to "3.4.17 Pushing Certificates".

Importing certificates

To import a certificate to be pushed on clients to ADM, please do the following:

1. On **System** tab, click **Deployment > Certificate**.
2. The Certificate list appears in Management area.

Delete Certificate
Import Certificate

Issued to	Issued by	Expired on	Valid
		2025-11-30	Valid

Note

If you have never imported certificates, the Certificate list will be empty.

3. Click **Import Certificate** on the top of the list.
4. The Import Certificate window appears.

Import Certificate

File Name:

Browse...

Issued to:

Issued by:

Valid from:

Note:

Please select PEM or DER format certificate (limit of 16 certificates).

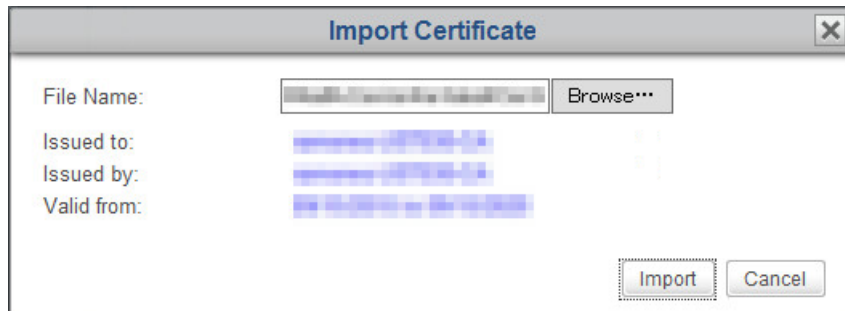
Cancel

5. Click **Browse** to locate the certificate file to import, and then click **Open** to confirm.

Note

Certificate files in the PEM or DER format can be selected.

- Click **Import** to start import.



- On completion, the imported certificate file appears as an entry in the Certificate list.

[Delete Certificate](#)
[Import Certificate](#)

Issued to	Issued by	Expired on	Valid
...	...	2025-11-30	Valid
...	...	2020-09-15	Valid

Deleting certificates

To delete a certificate file imported to ADM, please do the following:

- On **System** tab, click **Deployment > Certificate**.
- The Certificate list appears.
- Select the certificate file to delete, and then click **Delete Certificate**.

Note To select more than one certificate, Ctrl-click to select multiple certificates.

- The Delete Certificate window appears prompting for confirmation.
- Click **Delete** to confirm.
- The selected certificate file is removed from the Certificate list.

3.2.8 Configuring Remote Deployment Settings

You can deploy, maintain, and upgrade your thin clients from a remote computer with ADM. All required files (firmware, snapshot, or package files) can come from the same computer where your ADM is installed, or another computer with the needed files.

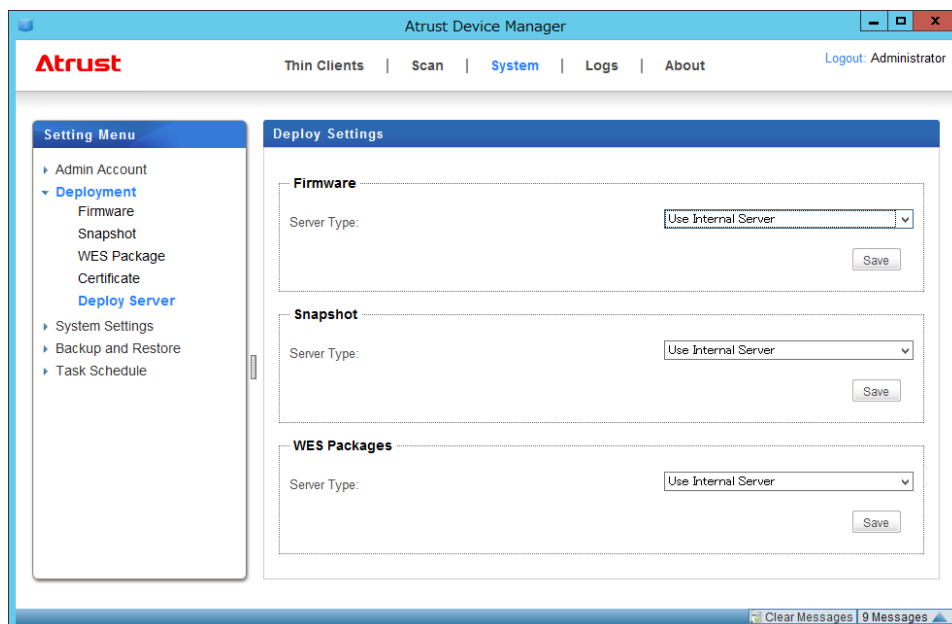
Remote Deployment Configuration		
Option	Required Actions	Note
Using local updates and snapshots	Import or create all required files on the same computer where the governing ADM is installed	Default
Using remote updates and snapshots	Configure settings to get all needed files from another computer	Imports or copies all needed files to another computer where ADM is installed.

Note In ADM, the local updates and snapshots are used by default.

Maintaining or Deploying Clients with Local Updates or Snapshots

To maintain or deploy clients with internal updates or snapshots, please do the following:

1. On **System** tab, click **Deployment > Deploy Server**.
2. The Deploy Server pane appears in Management area.



3. Click the drop-down menu on each section (**Firmware**, **Snapshot**, and **WES Packages**) to select **Use Internal Server**, and then click **Save** to apply.

Maintaining or Deploying Clients with Remote Updates or Snapshots

To maintain or deploy clients with external updates or snapshots, please do the following:

1. On **System** tab, click **Deployment > Deploy Server**.
2. The Deploy Settings pane appears in Management area.
3. Click the drop-down menu on a section (**Firmware**, **Snapshot**, or **WES Packages**) to select **Use External Server**, new fields appear for configuration.

Firmware

Server Type:	Use External Server ▼
Firmware URL:	*http://YourServerIP:10080/firmware
Username:	* <input type="text"/>
Password:	* <input type="password"/>

Save

Snapshot

Server Type:	Use External Server ▼
Snapshot URL:	*http://YourServerIP:10080/snapshot
Username:	* <input type="text"/>
Password:	* <input type="password"/>

Save

WES Packages

Server Type:	Use External Server ▼
WES Packages URL:	*http://YourServerIP:10080/packages
Username:	* <input type="text"/>
Password:	* <input type="password"/>

Save

4. In Firmware/Snapshot/WES Packages URL field, replace **YourServerIP** in the original URL with the IP address of another computer where you want to get updates and snapshots, type in the default credentials — **user** as the username and **secret** as the password, and then click **Save** to apply.

Firmware

Server Type:

Firmware URL:

Username:

Password:

Snapshot

Server Type:

Snapshot URL:

Username:

Password:

WES Packages

Server Type:

WES Packages URL:

Username:

Password:

3.2.9 Selecting the Service IP of ADM

To select the service IP address of your ADM, please do the following:

1. On **System** tab, click **System Settings > General Settings**.
2. Click the drop-down list of **Service IP Address** to select the desired IP address.



Atrust Device Manager

Service IP Address: 192.168.7.1

Save

3. Click **Save** to apply.

Note

- It is strongly recommended to use a fixed IP address as the service IP of ADM. The change of the service IP may make all the managed clients become unmanageable. In case that the IP address of the computer where ADM is installed is changed, ensure that you make the Service IP setting here consistent with the new IP address.
- In case that the service IP changes, your ADM will prompt you to select a new service IP when you log in to the management console.

3.2.10 Configuring Auto-Logout for ADM

ADM allows you to configure its auto-logout to enhance the security of the management console. When configured, your session will be ended automatically when it's idle for a specific amount of time.

Note By default, your administrative session will not be logged out automatically.

To configure auto-logout for ADM, please do the following:

1. On **System** tab, click **System Settings > General Settings**.
2. Click the drop-down menu to select the desired amount of inactivity time.



The screenshot shows a configuration box titled "Auto Logout". Inside the box, there is a label "Auto Logout After:" followed by a dropdown menu currently set to "Never". Below the dropdown, there is a faint, partially visible text "Inactivity Time". To the right of the dropdown, there is a "Save" button.

3. Click **Save** to apply.

3.2.11 Configuring Auto Registration

This function enables you to register a client as a managed terminal automatically on ADM when the client is online.

Important US310e does not support auto registration.

Note

- Auto registration is not configured by default.
- To use this function, the setting in System > Details > Enable auto registration must be selected in ACS on the client side. This function does not operate with the ADM side settings only.

To configure auto registration, please do the following:

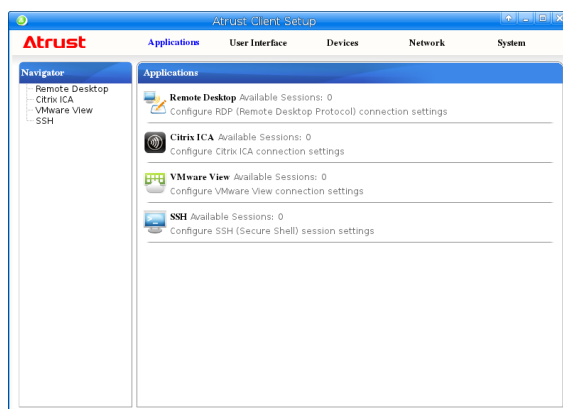
1. On **System** tab, click **System Settings > General Settings**.
2. Select Enable Auto Registration.



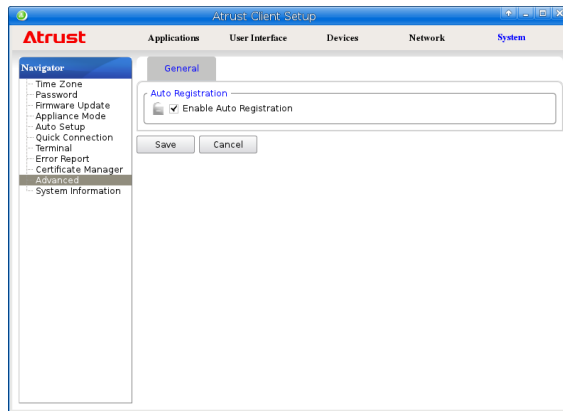
3. Click **Save** to apply.



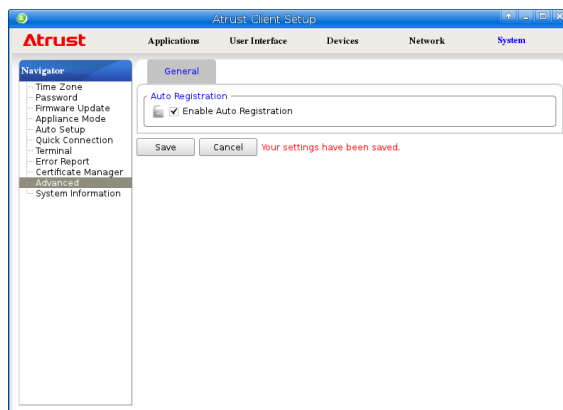
4. Configuration on the ADM side is now complete. To use this function, configuration is also required on the client side. Start ACS for clients.



5. Select **System > Advanced > Enable Auto Registration**.



6. Click **Save** to apply.



7. Close Atrust Client Setup. The client side configuration is now complete.
8. The client is automatically registered as a managed terminal when the client starts up next time. Automatically registered clients are registered in the Thin Client - <Ungrouped> group. For automatically registered clients, the value "Auto-registered" is set in Description.

<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	Atrust-033EB2	192.168.7.111	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC	N/A	Auto-registered

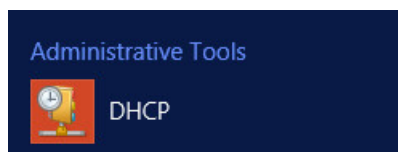
To use auto registration, you need to configure the DHCP server or DNS server:

To configure the DHCP server for auto registration, please do the following:

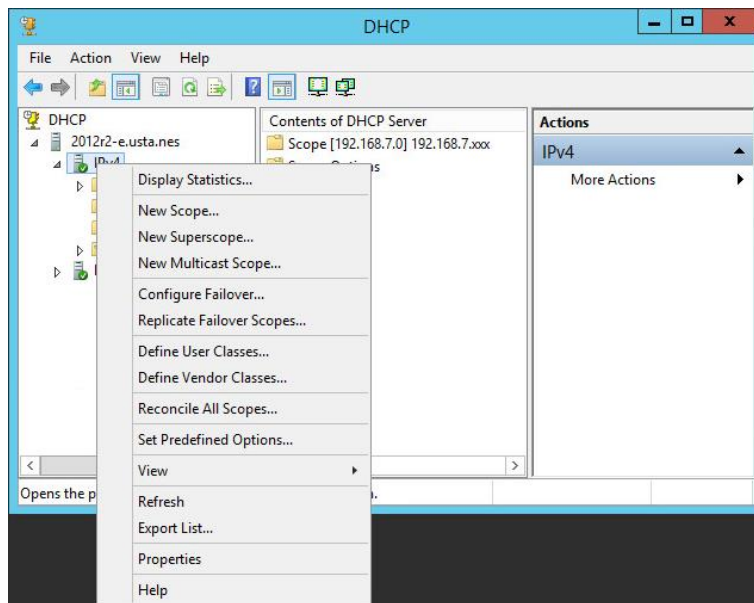
Note

This document describes the procedure for configuring the DHCP server built on Windows Server 2012 R2 as an example. The configuration procedure may vary on different operating systems or editions.

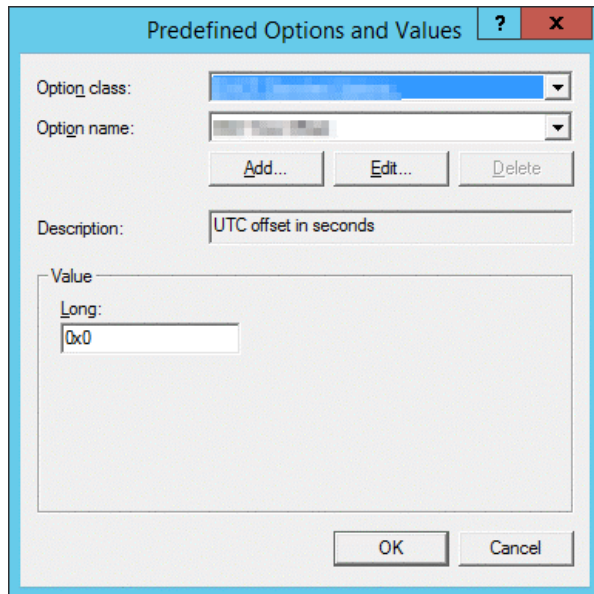
1. Sign in to the DHCP server with the Administrator account.
2. Click **Start > All apps > Administrative Tools > DHCP**.



3. Select IPv4 in the left pane on the DHCP window, and click **Set Predefined Options** on the right-click menu.

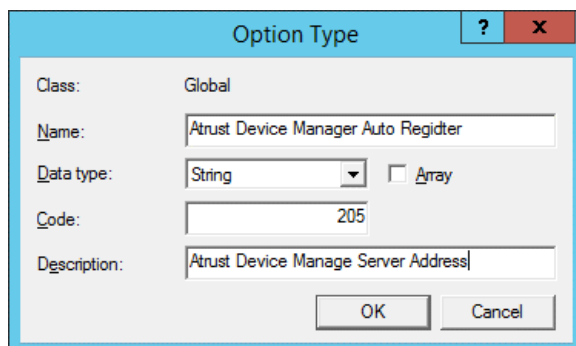


4. Click **Add**.



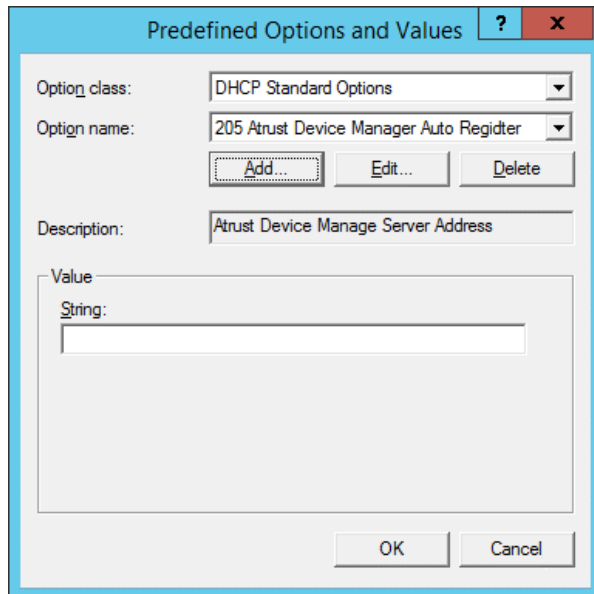
5. On Option type window, enter the following information.

- Name : <Any name>
- Data type : String
- Code : 205
- Description : <Any>

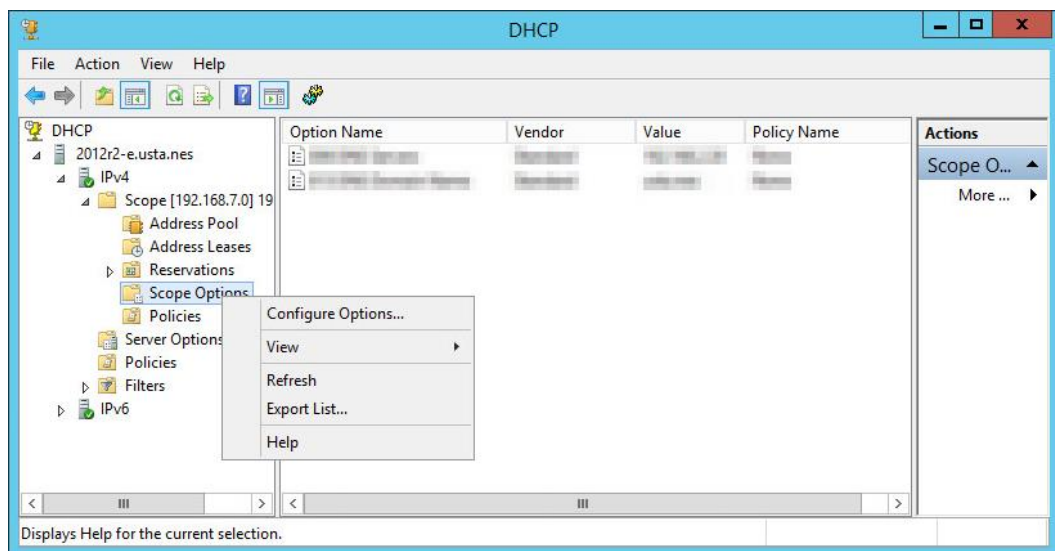


6. Click **OK**.

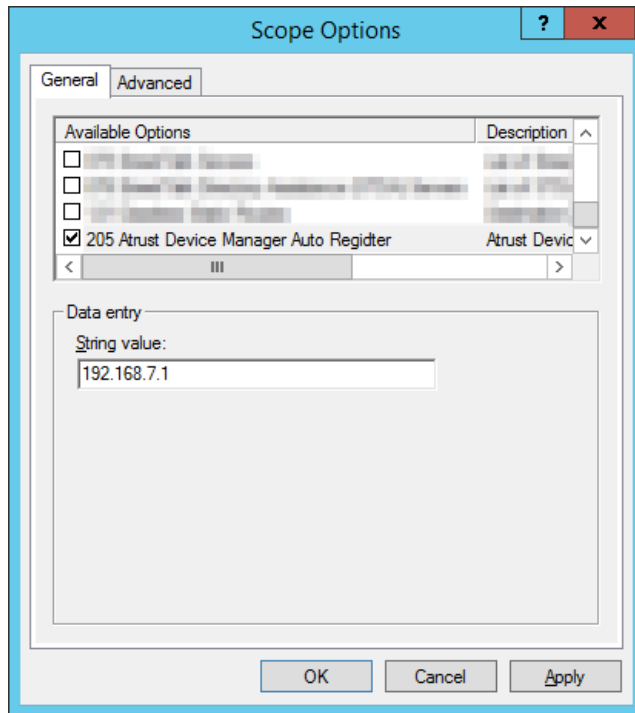
7. On Predefined Options and Values window, click **OK**.



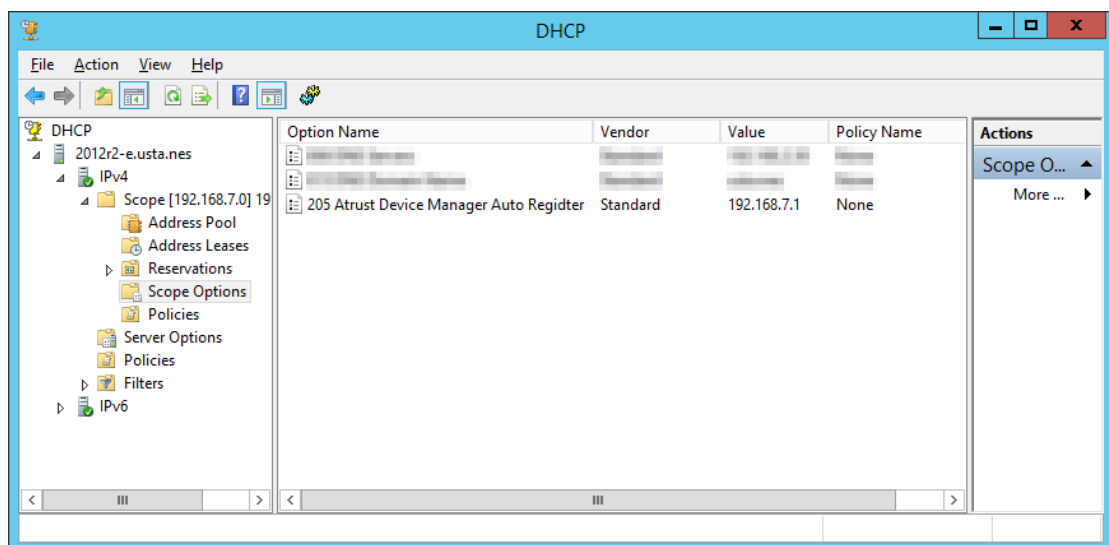
8. Select Scope - Scope Options in the left pane on the DHCP window, and click **Configure Options** on the right-click menu.



9. In the list in Available Options on the General tab, select "205" registered in steps 3 through 7, and type in the IP address of ADM in Data entry (String value).



10. Click **Apply**, and then click **OK**.
11. Check that it is displayed in the list of registered scope options in the center pane.

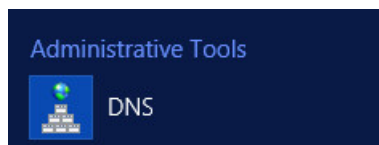


To configure the DNS server for auto registration, please do the following:

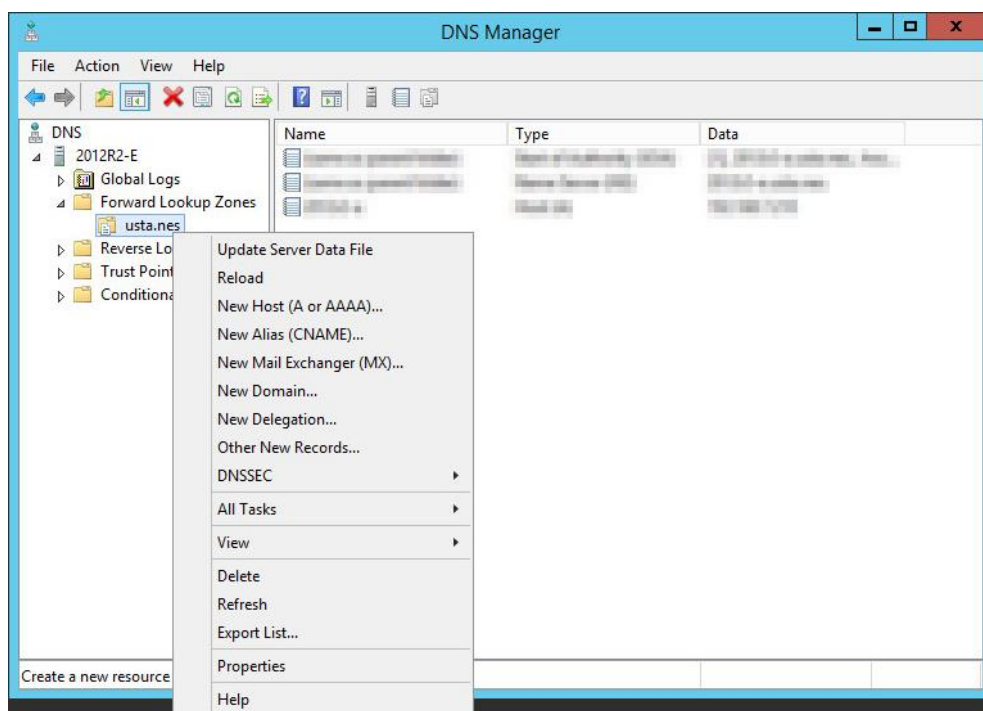
Note

This document describes the procedure for configuring the DNS server built on Windows Server 2012 R2 as an example. The configuration procedure may vary on different operating systems or editions.

1. Sign in to the DHCP server with the Administrator account.
2. Click **Start > All apps > Administrative Tools > DNS**.

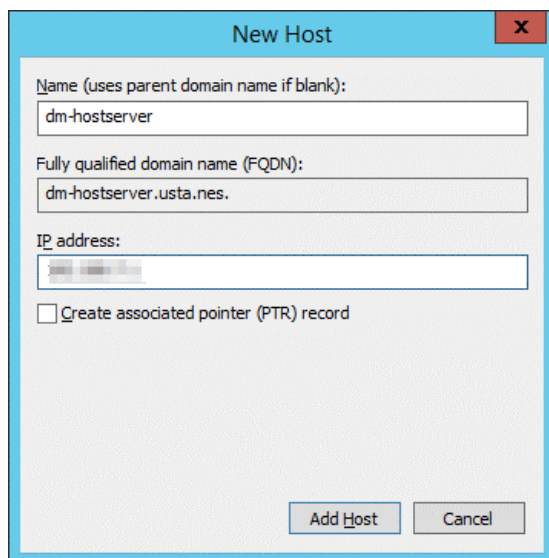


3. In the left pane of the DNS Manager window, click to select Forward Lookup Zones - <Domain Node>, and then click **New Host (A or AAAA)**.



4. On Option Host window, enter the following information.

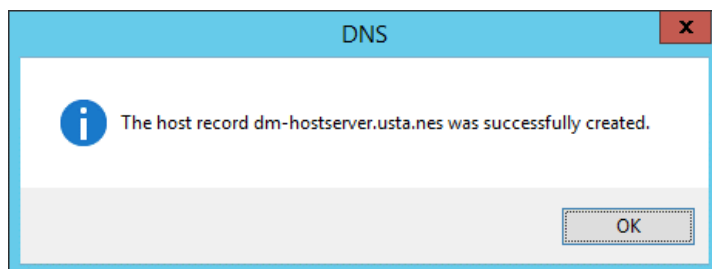
- Name : dm-hostserver
- IP Address : <IP address of the ADM server>



The 'New Host' dialog box is shown with a light blue title bar and a red close button. It contains three text input fields: 'Name (uses parent domain name if blank):' with 'dm-hostserver', 'Fully qualified domain name (FQDN):' with 'dm-hostserver.usta.nes.', and 'IP address:' with a placeholder IP address. Below these fields is a checkbox labeled 'Create associated pointer (PTR) record' which is unchecked. At the bottom right are 'Add Host' and 'Cancel' buttons.

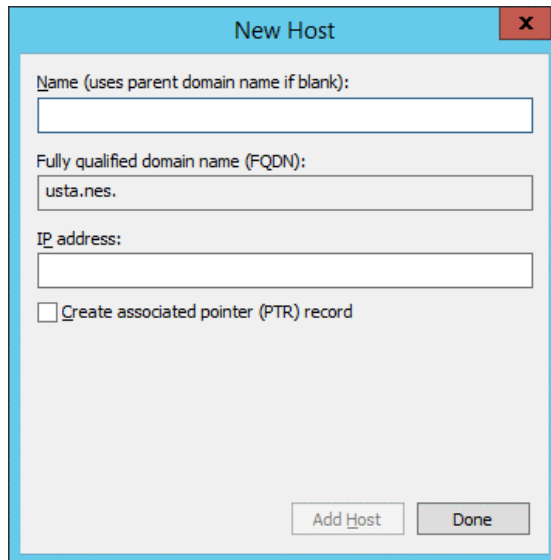
5. Click **Add Host**.

6. A message appears indicating that the host record has been created correctly. Click **OK**.



The 'DNS' message box has a light blue title bar and a red close button. It features an information icon (a blue circle with a white 'i') followed by the text 'The host record dm-hostserver.usta.nes was successfully created.' At the bottom right is an 'OK' button.

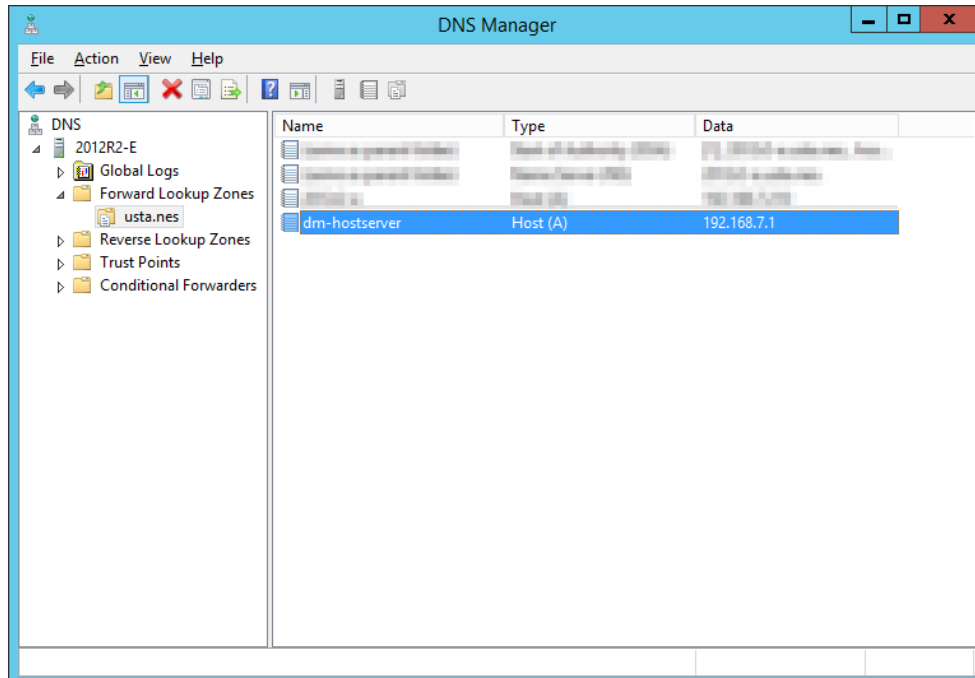
7. On New Host window, click **Done**.



The 'New Host' dialog box is shown with the following fields and options:

- Name (uses parent domain name if blank):** An empty text box.
- Fully qualified domain name (FQDN):** A text box containing 'usta.nes'.
- IP address:** An empty text box.
- ☐ **Create associated pointer (PTR) record**
- Buttons:** 'Add Host' and 'Done' at the bottom right.

8. Check that the host created in steps 3 through 7 is displayed in the Host list.



3.2.12 Configuring Password Protection for Managed Devices

Password Protection is the function to restrict that another ADM server detects the thin client managed already on ADM server. This function is possible to prevent terminal managed on your ADM from being controlled by malicious ADM.

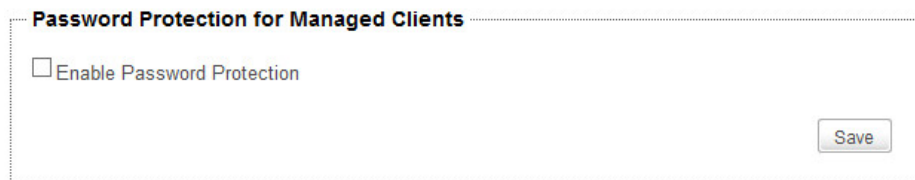
Devices that have been password-protected on ADM cannot be discovered without entering the password on the ADM server. Scan operation which **Include Protected Clients** is valid enables to detect password-protected device. For scanning and registering password-protected terminals, please refer to "3.3.8 Discovering Clients Including Password-Protected Devices".

Note

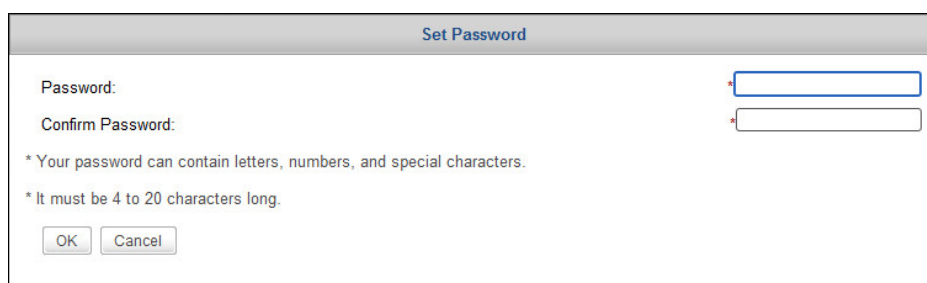
- Password protection is supported only by US320f and US120f. This function cannot be set on US310e.
- You can't register US310e already managed by another ADM.
- New devices registered after password protection is configured are automatically password-protected.

To configure password protection, please do the following:

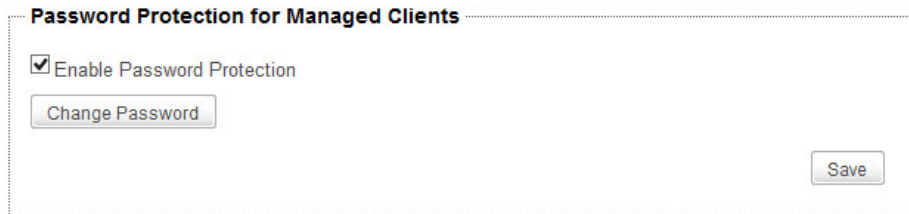
1. On **System** tab, click **System Settings> General Settings**.
2. Select **Enable password protection**.



3. The Set Password dialog starts up automatically. Type in the desired password, and then click **OK**.



4. Click **Save**.



The screenshot shows a dialog box titled "Password Protection for Managed Clients". It contains a checked checkbox labeled "Enable Password Protection". Below the checkbox is a button labeled "Change Password". In the bottom right corner of the dialog is a button labeled "Save".

5. The Apply Password Protection dialog appears. Click **Yes**.



The screenshot shows a dialog box titled "Apply Password Protection". It contains the text "Do you want to apply these changes?". At the bottom right are two buttons: "Yes" and "No".

6. A dialog appears indicating the result of application. Check the result, and then click **Close** to close the dialog.

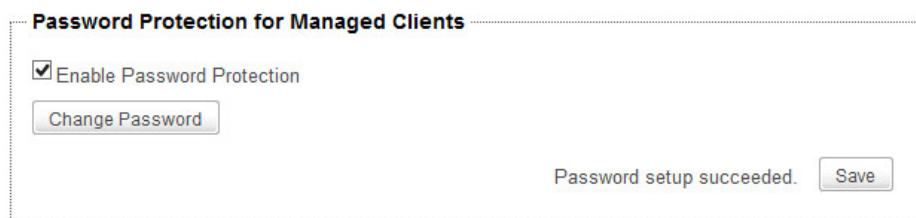


The screenshot shows a dialog box titled "Push Password Protection". It contains a "Status:" label followed by a blue progress bar. To the right of the progress bar, the text reads "1 client(s) succeeded" and "2 client(s) failed!". At the bottom right is a button labeled "Close".

Note

Application of password protection fails if managed terminals include US310e to which password protection cannot be applied because the password protection setting is sent to all managed terminals (including US310e) registered in ADM. This is not a problem.

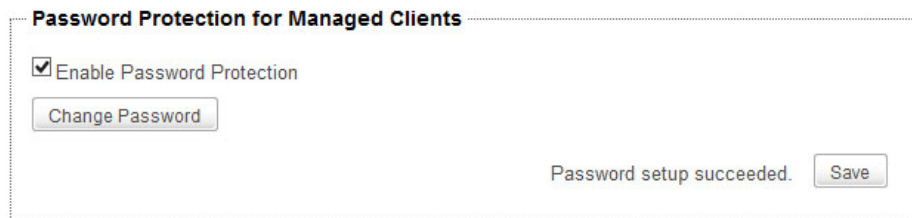
7. Check that the message "Password setup succeeded." is displayed.



The screenshot shows the same "Password Protection for Managed Clients" dialog box as in step 4. It contains the checked checkbox "Enable Password Protection" and the "Change Password" button. In the bottom right corner, the text "Password setup succeeded." is displayed next to the "Save" button.

To configure password protection, please do the following:

1. On **System** tab, click **System Settings> General Settings**.
2. Click **Change Password**.

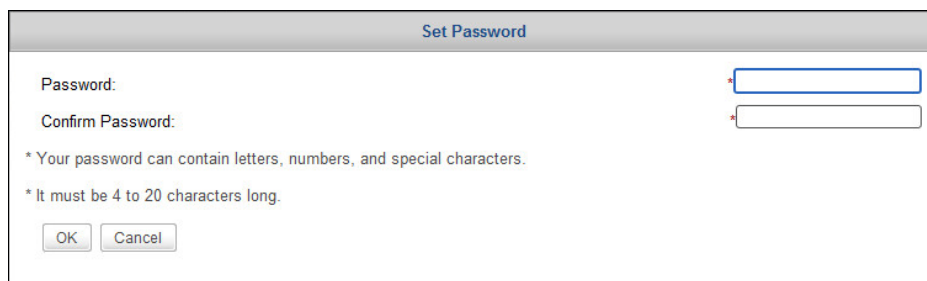


Password Protection for Managed Clients

☒ Enable Password Protection

Password setup succeeded.

3. The Set Password dialog starts up automatically. Type in the desired password, and then click **OK**.



Set Password

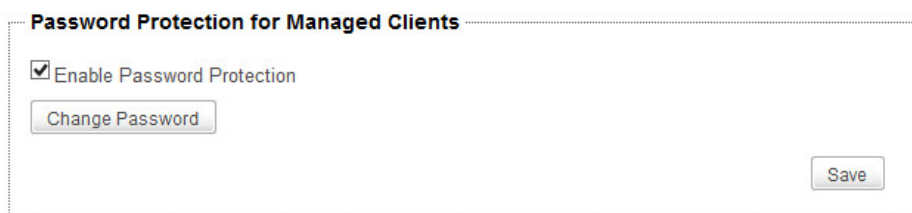
Password:

Confirm Password:

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

* It must be 4 to 20 characters long.

4. Click **Save**.



Password Protection for Managed Clients

☒ Enable Password Protection

5. The Apply Password Protection dialog appears. Click **Yes**.



Apply Password Protection

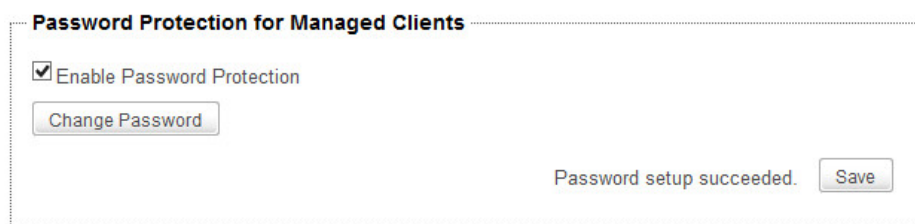
Do you want to apply these changes?

6. A dialog appears indicating the result of application. Check the result, and then click **Close** to close the dialog.

**Note**

Application of password protection fails if managed terminals include US310e to which password protection cannot be applied because the password protection setting is sent to all managed terminals (including US310e) registered in ADM. This is not a problem.

7. Check that the message "Password setup succeeded." is displayed.



3.2.13 Configuring the Database Source of ADM

ADM offers two ways to store its management database: one is to store the database on the same computer where ADM is installed; the other is on a different computer. By default, the management database is stored on the computer where ADM is installed.

Using Local Management Database

To use the local management database, please do the following:

1. On **System** tab, click **System Settings > External Database**.
2. The External Database pane appears in Management area.
3. Click the drop-down menu to select **No**.

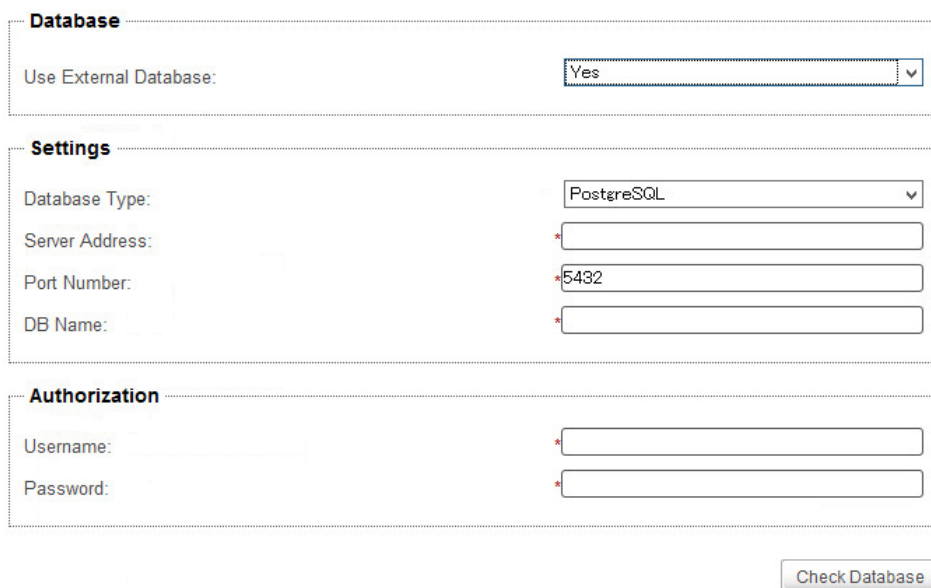


The screenshot shows a configuration window titled "Database". Inside, there is a label "Use External Database:" followed by a dropdown menu currently displaying "No". A "Save" button is located at the bottom right of the pane.

Using External Management Database

To use the external and centralized management database, please do the following:

1. On **System** tab, click **System Settings > External Database**.
2. The External Database pane appears in Management area.
3. In Database section, click the drop-down menu to select **Yes**.
4. New sections with new fields appear for configuration.



The screenshot shows the "Database" configuration window with "Use External Database" set to "Yes". Below this, there are two sections: "Settings" and "Authorization".
The "Settings" section contains:
- "Database Type:" with a dropdown menu showing "PostgreSQL".
- "Server Address:" with a text input field.
- "Port Number:" with a text input field containing "5432".
- "DB Name:" with a text input field.
The "Authorization" section contains:
- "Username:" with a text input field.
- "Password:" with a text input field.
A "Check Database" button is located at the bottom right of the window.

Note

- The supported External Database is MsSQL (Microsoft SQL Server). When using other database (PostgreSQL, MySQL, or Oracle), verify it to ensure that it operates without problem in advance.
- Ensure that you have set up the desired database management system.

5. In Settings section, click the drop-down menu to select the type of your database management system, type the IP address of the database server, the port number, and the name of the database.
6. In Authorization section, type the user name and password for access of database.
7. Click **Check Database** to connect to the remote database.

3.2.14 Selecting the Interface Language of ADM

To select the interface language of your ADM, please do the following:

1. On **System** tab, click **System Settings > Language**.
2. The System Language pane appears in Management area.
3. Click the drop-down list of available languages to select the desired interface language.
4. Click **Save** to apply.

3.2.15 Backing Up the Management Database

To back up the management database of ADM, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Database Backup section, type the desired file name prefix.

The screenshot shows a web form titled "Internal Database Backup". It contains two text input fields: "Directory:" with the value "C:\Program Files (x86)\Atrust\#dbarchive#" and "Append File Name with:" with the value "ADM". A "Backup" button is located at the bottom right of the form.

Note

The backup file is stored in the default directory as shown in Directory field. If you want to change the name of a backup file, locate the file and change its name.

3. Click **Backup** to store a copy of management database and client certificates.
4. On completion, the backup file appears at the top of the Archive File drop-down menu in Database Archive Management section.

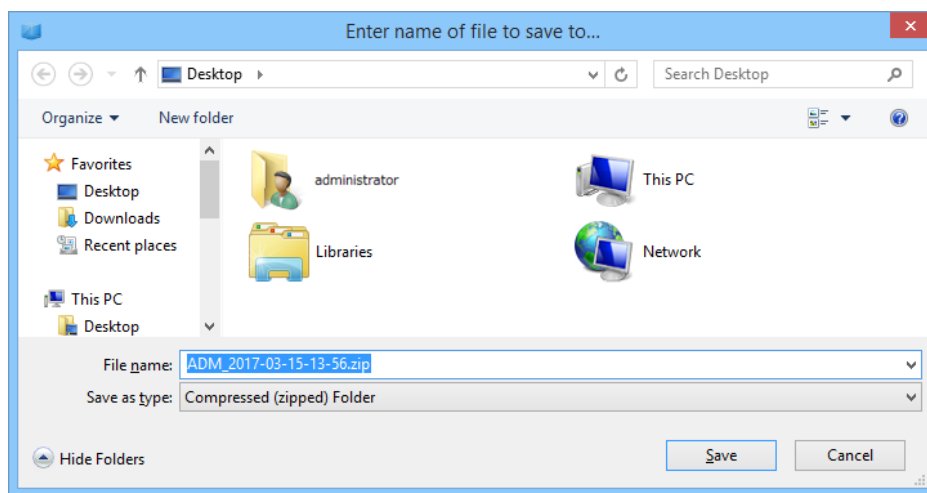
The screenshot shows a web form titled "Internal Database Archive Management". It features a "Select an Archive File:" label and a dropdown menu displaying "ADM_2017-03-15-13-36.zip". Below the dropdown are four buttons: "Download", "Upload", "Delete", and "Restore".

3.2.16 Managing Database Archive Files

Downloading a Database Archive File

To download a database archive file, please do the following:

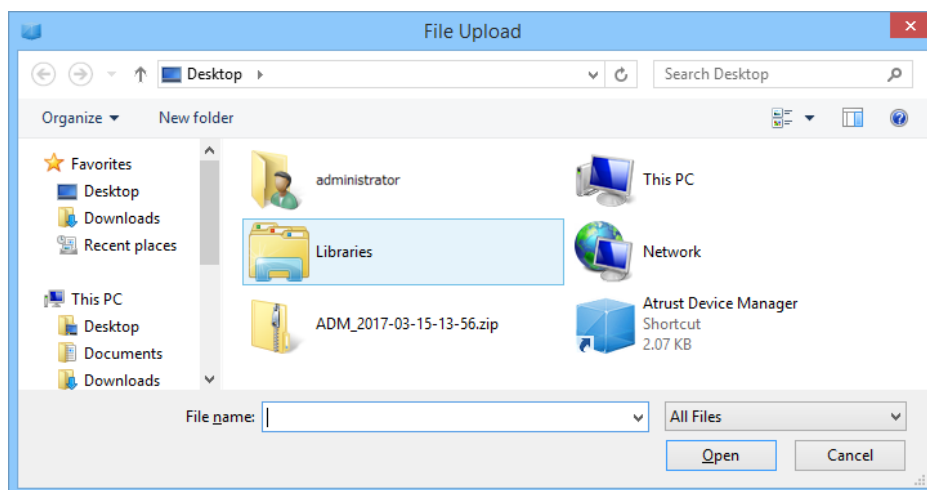
1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click the **Archive File** drop-down menu to select the desired database archive file, and then click **Download**.
3. A window appears prompting you to choose the save destination of the downloaded database archive file. Save the database archive file at the desired location.



Uploading a Database Archive File

To upload a database archive file, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click **Upload** to open the File Upload window.



3. Locate the desired database archive file, and then click **OK** to confirm.
4. The file is added to the Archive File drop-down menu.

Deleting a Database Archive File

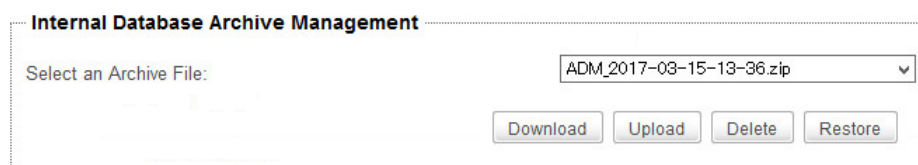
To delete a database archive file, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click the drop-down menu to select the desired archive file.
3. Click **Delete** to remove the selected file.

3.2.17 Restoring a Database Archive File

To restore a database archive file, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click the Archive File drop-down menu to select the desired archive file.



The screenshot shows a web interface titled "Internal Database Archive Management". Below the title, there is a label "Select an Archive File:" followed by a dropdown menu. The dropdown menu is open, showing the selected file "ADM_2017-03-15-13-36.zip" with a downward arrow. Below the dropdown menu, there are four buttons: "Download", "Upload", "Delete", and "Restore".

3. Click **Restore** to return the management database of ADM to the desired state.

3.2.18 Scheduling Automatically Performed Tasks

ADM enables you to schedule tasks performed automatically at a specific time, allowing scheduled and automatic maintenance tasks for managed endpoint devices.

To schedule an automatically performed task, please do the following:

1. On **System** tab, click **Task Schedule**.
2. The Task list appears in Management area.

+ Add Edit Delete View Log

	Schedule	Comment	Next Schedule	Prev Schedule	Status
✓	Daily	TEST	2017-03-16 00:00		

Note The Task list might be empty, if you have never created automatically performed tasks.

3. Click **Add** on the top of the Task list.
4. The Add Task Schedule pane appears in Management area.

Add Task Schedule

☒ Enable Task Schedule

Schedule

Details

Perform: Daily

Execute every 1 day(s).

Start Date: 2017-3-15 Select

Start Time: 00 : 00

Comment:

Previous:

Next:

Previous Result:

Save

Cancel

5. On **Schedule** tab, type in or click to select the start date, time, the way to repeat, task comment, etc.

The screenshot shows the 'Add Task Schedule' dialog box with the 'Schedule' tab selected. The 'Enable Task Schedule' checkbox is checked. The 'Perform' dropdown is set to 'Daily'. The 'Execute every' field is set to '1' day(s). The 'Start Date' is '2017-3-15' with a 'Select' button. The 'Start Time' is '16:00'. The 'Comment' field contains 'TEST Schedule'. The 'Previous:', 'Next:', and 'Previous Result:' fields are empty. 'Save' and 'Cancel' buttons are at the bottom right.

Add Task Schedule	
<input checked="" type="checkbox"/> Enable Task Schedule	
Schedule Details	
Perform: Daily	
Execute every 1 day(s).	
Start Date: 2017-3-15 Select	
Start Time: 16 : 00	
Comment: TEST Schedule	
Previous:	
Next:	
Previous Result:	
Save Cancel	

6. On **Details** tab, click **Add** to specify the action(s).

The screenshot shows the 'Add Task Schedule' dialog box with the 'Details' tab selected. The 'Enable Task Schedule' checkbox is checked. The 'Schedule' tab is also visible. The 'Details' tab contains a table with columns 'Module Name', 'Action', and 'Comment'. Above the table are buttons for '+ Add', 'Edit', and '- Delete'. The 'Comment' field contains 'TEST Schedule'. The 'Previous:', 'Next:', and 'Previous Result:' fields are empty. 'Save' and 'Cancel' buttons are at the bottom right.

Add Task Schedule				
<input checked="" type="checkbox"/> Enable Task Schedule				
Schedule Details				
+ Add Edit - Delete				
<table border="1"><thead><tr><th>Module Name</th><th>Action</th><th>Comment</th></tr></thead><tbody></tbody></table>		Module Name	Action	Comment
Module Name	Action	Comment		
Comment: TEST Schedule				
Previous:				
Next:				
Previous Result:				
Save Cancel				

Note One task consists of one or more actions.

7. On Add window, type in or click to select the action order, type, performed action, action comment, etc., and then click **OK** to confirm.

Add

Enable: ☒

Order: 1

Module Name: Client: Power Control

Action: Wake On LAN

Clients:

☒ Groups ☐ Ungrouped

Select All

Unselect All

Comment:

OK Cancel

Add

Enable: ☒

Order: 1

Module Name: Task: Wait

Wait 1 minute(s)

Comment:

OK Cancel

8. After completion, the action(s) will be added to the Action list.

Add Task Schedule

☒ Enable Task Schedule

Schedule Details

+ Add Edit - Delete

Module Name	Action	Comment
Power Control	Wake On LAN	TEST

Comment: TEST Schedule


Previous:


Next:


Previous Result:


Save Cancel



9. Click **Save** to confirm. The task entry will be added to the Task list.

 Add

 Edit

 Delete

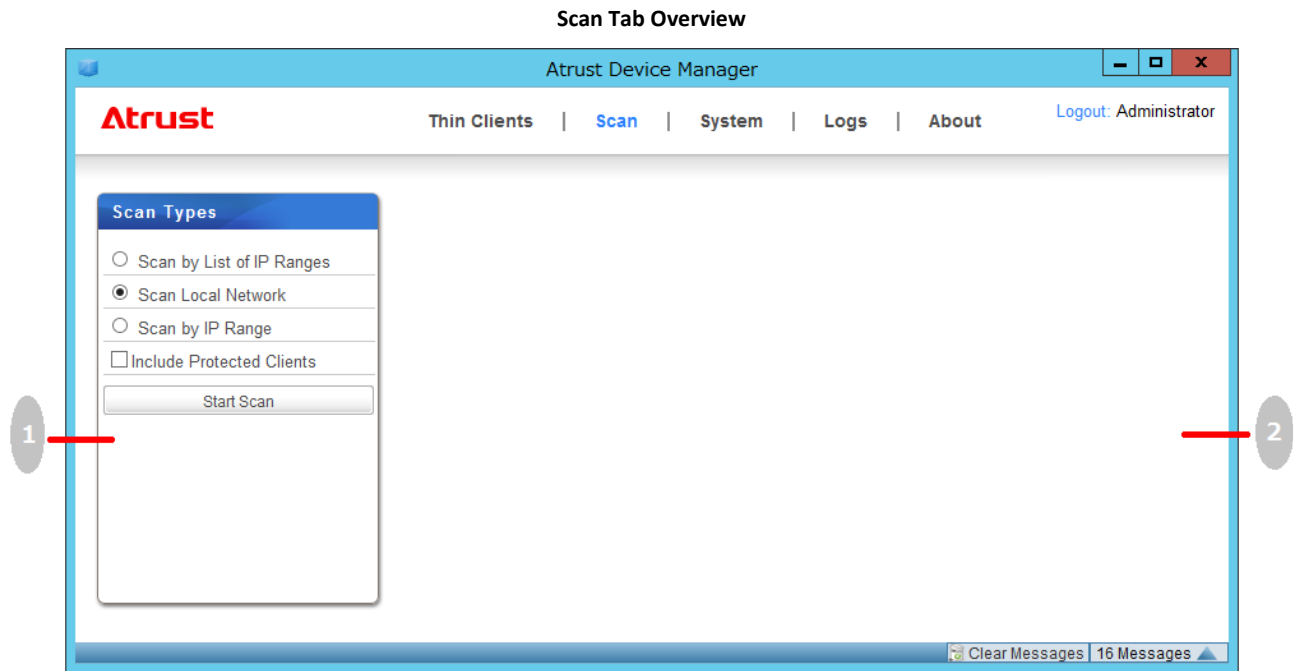
 View Log

	Schedule	Comment	Next Schedule	Prev Schedule	Status
	Daily	TEST	2017-03-16 00:00		
	Daily	TEST Schedule	2017-03-15 16:00		

3.3 Adding Clients into a Managed Group

3.3.1 Scan Tab Overview

Scan tab enables you to search thin clients your ADM isn't managing on the local network. To access the functionality of Scan tab, click the tab on ADM.



Interface Elements		
No.	Name	Description
1	Navigation Area	Select the desired client detection method.
2	Management Area	Manage IP Range lists or discovered clients.

3.3.2 Available Tasks at a Glance

No.	Available Task	Section
1	Discovering clients in the whole range of a local network	3.3.4 Discovering Clients in the Whole Range of a Local Network
2	Discovering clients in a specified range of IP addresses	3.3.5 Discovering Clients in a Specified Range of IP Addresses
3	Discovering clients using predefined IP range lists	3.3.6 Creating and Managing an IP Range List 3.3.7 Discovering Clients using a Predefined IP Range List
4	Including password-protected terminals	3.3.8 Discovering Clients Including Password-Protected Devices

3.3.3 Client Detection and Management

Your client is not managed by any ADM by factory default. To manage your clients with ADM, you need to first detect unmanaged clients over your local network, and then add them into a managed group under your ADM. You can add US320f and US120f managed by another ADM to your ADM. Moreover, ADM which have added the thin client takes over control from the other one. Control of the terminal is released from the other one in this case, and note that target thin client remains in Client list.

US310e which is already managed by another ADM can't make an addition to your ADM.

Important Your thin client will not be detected when it is powered up. You need to perform a manual scan on ADM.

- Note**
- You can also register the client on ADM automatically by enabling auto registration on the thin client and ADM. For details, please refer to "3.2.11 Configuring Auto Registration".
 - To restrict registration operation of another ADM from the already managed client, use password protection for managed devices. Please refer to "3.2.12 Configuring Password Protection for Managed Devices" for detail.

To look for a thin client over your local network, you can use different client detection options available under the **Scan** tab.

The following table shows prerequisites and methods for detecting clients over your local network:

Model	Prerequisites	Method
US320f	<ul style="list-style-type: none"> Clients are connected to the local network Clients are powered up 	Manual Scan
US310e	<ul style="list-style-type: none"> Clients are connected to the local network Clients are powered up 	Manual Scan
US120f	<ul style="list-style-type: none"> Clients are connected to the local network Clients are powered up 	Manual Scan

Note After adding clients into a managed group under your ADM, you can start remote management of clients. For details on how to manage your clients remotely, please refer to section "3.4 Managing All Your Clients".

3.3.4 Discovering Clients in the Whole Range of a Local Network

To discover unmanaged clients in the whole range of a local network and add the desired client(s) into a managed group under your ADM, please do the following:

1. On **Scan** tab, select **Scan Local Network**.

2. Click **Start Scan**.
3. On completion, the found clients are listed in Management area.

+ Put in group Ungrouped |
 Unselect All |
 Select All

Name	IP	Mac Address	Model	Firmware	Managed
Atrust-033EB2	192.168.7.112	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC	No
atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL	No

4. Select the desired client(s), the preferred client group from the drop-down menu on the top of the Client list, and then click **Put in group**.

Note

- The default client group is Ungrouped. You can change the group of a client at a later time. To create new client groups, please refer to section "3.4.3 Creating Client Groups".
- To select multiple clients, just click to select each individual client. You can also use Select All and Unselect All on the top of the Client list to select/unselect clients.

5. On completion, the client(s) is managed by your ADM.

Note

Whichever group you add a client to (including Ungrouped), once Put in group is executed successfully, the client will be managed by your ADM.

3.3.5 Discovering Clients in a Specified Range of IP Addresses

To find unmanaged clients in a specified range of IP addresses and add the desired client(s) into a managed group under your ADM, please do the following:

1. On **Scan** tab, select **Scan by IP Range**.
2. The IP range fields appear.

Scan Types

☐ Scan by List of IP Ranges
☐ Scan Local Network
☒ Scan by IP Range
☐ Include Protected Clients

From IP: 192 . 168 . 7 . 110
 To IP: 192 . 168 . 7 . 119

Start Scan

3. Type in the desired IP range, and then click **Start Scan**.
4. On completion, the found clients are listed in Management area.

Atrust Device Manager

Thin Clients | **Scan** | System | Logs | About

Logout: Administrator

Scan Types

☐ Scan by List of IP Ranges
☐ Scan Local Network
☒ Scan by IP Range
☐ Include Protected Clients

From IP: 192 . 168 . 7 . 110
 To IP: 192 . 168 . 7 . 119

Start Scan

Put in group: Ungrouped | Unselect All | Select All

Name	IP	Mac Address	Model	Firmware	Managed
Atrust-033EB2	192.168.7.112	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC	No
atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL	No
atrust-03772C	192.168.7.116	00:1F:D8:03:77:2C	US120f	ARM Linux 8.43-IAKC	Yes

Page 1 / 1 | Displaying 1 to 3 of 3 items

Clear Messages | 17 Messages

5. Select the desired client(s), the preferred client group from the drop-down menu on the top of the Client list, and then click **Put in group**.

Note

- The default client group is Ungrouped. You can change the group of a client at a later time. To create new client groups, please refer to section "3.4.3 Creating Client Groups".
- To select multiple clients, just click to select each individual client. You can also use Select All and Unselect All on the top of the Client list to select/unselect clients.

6. On completion, the client(s) is managed by your ADM.

Note

Whichever group you add a client to (including Ungrouped), once Put in group is executed successfully, the client will be managed by your ADM.

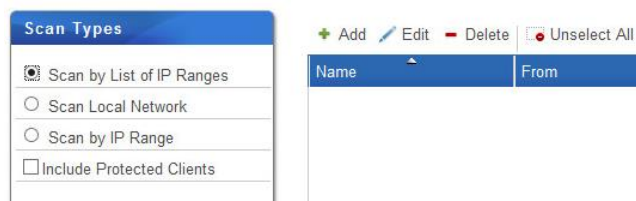
3.3.6 Creating and Managing an IP Range List

You can define different IP ranges for your local network, and then find unmanaged clients within a specific range of IP addresses when needed.

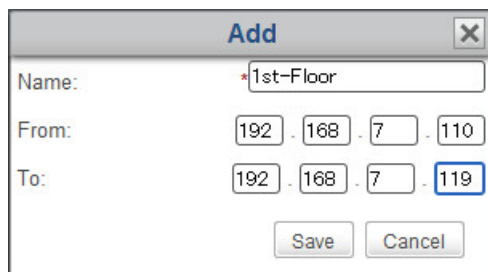
Creating an IP Range List

To create an IP Range list, please do the following:

1. On **Scan** tab, select **Scan by List of IP Ranges**.
2. Click **Add** on the top of the IP Range list.



3. The Add window appears.
4. Type in the name for this entry of IP range, and specify the desired IP range using **From** and **To** fields.



5. Click **Save** to add this range entry.
6. Repeat steps 2 through 5 to add other range entries to your IP Range list.

Managing the IP Range List

To manage your IP Range list, please do the following:

1. On **Scan** tab, select **Scan by List of IP Ranges**.
2. The IP Range list appears in Management area.
3. Click **Add**, **Edit**, or **Delete** to make changes to your IP Range list.

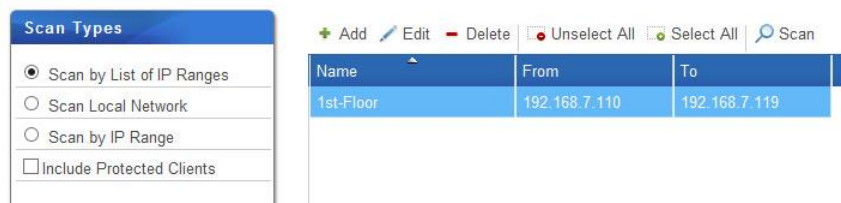
3.3.7 Discovering Clients using a Predefined IP Range List

To find unmanaged clients using a predefined IP Range list and add the desired client(s) into a managed group under ADM, please do the following:

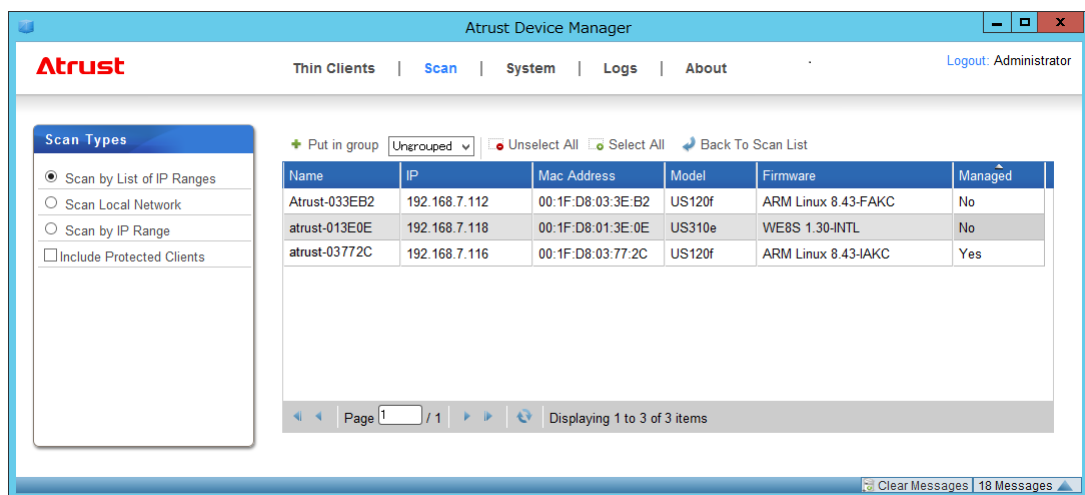
Note

If you have not created any IP Range list, please refer to "3.3.6 Creating and Managing an IP Range List" for detail.

1. On **Scan** tab, select **Scan by List of IP Ranges**.
2. The IP Range list appears.
3. Click to select the desired IP range, and then click **Scan** to look for unmanaged clients within the range.



4. On completion, the found clients are listed in Management area.



5. Select the desired client(s), the preferred client group from the drop-down menu on the top of the client list, and then click **Put in group**.

Note

- The default client group is Ungrouped. You can change the group of a client at a later time. To create new client groups, please refer to section "3.4.3 Creating Client Groups".

- To select multiple clients, just click to select each individual client. You can also use Select All and Unselect All on the top of the Client list to select/unselect clients.

6. On completion, the client(s) is managed by your ADM.

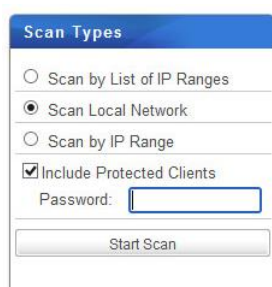
Note

Whichever group you add a client to (including Ungrouped), once Put in group is executed successfully, the client will be managed by your ADM.

3.3.8 Discovering Clients Including Password-Protected Devices

Select **Include Protected Clients** box when finding clients including password-protected terminals.

When it is selected, a password entry field appears. Type in the password set for the terminal.

**Note**

- The Including password-protected terminals option can be used with various scan tasks.
- For information on password protection, please refer to "3.2.12 Configuring Password Protection for Managed Devices".

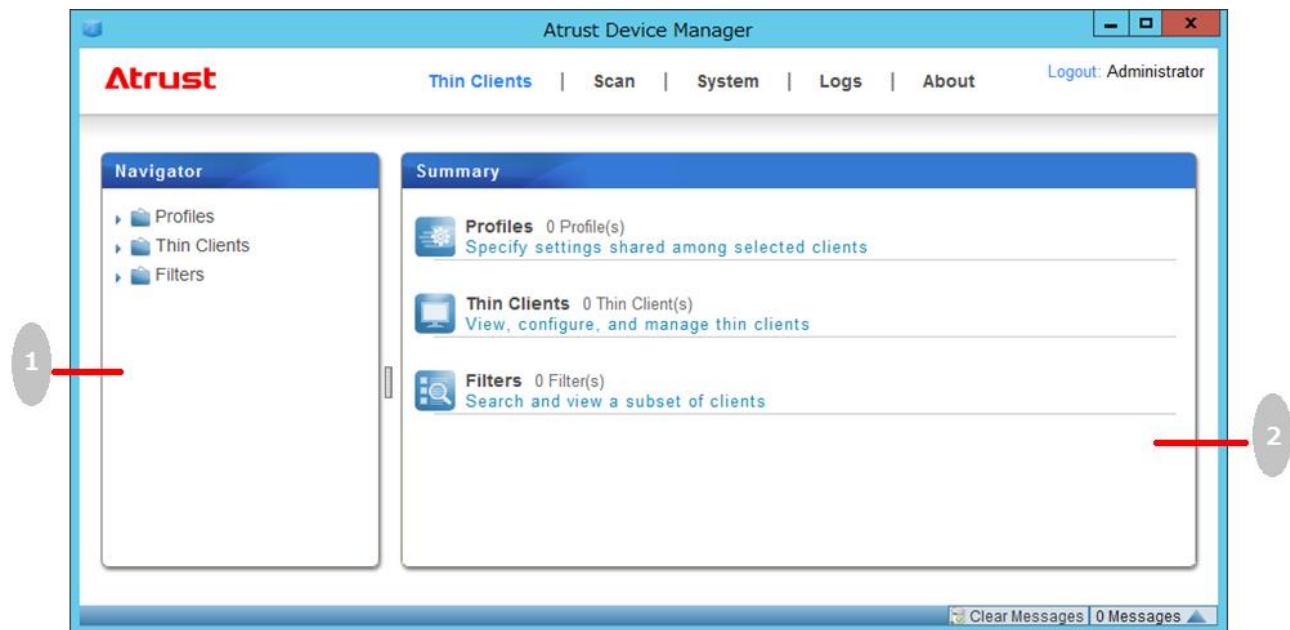
After typing in the password, click **Start Scan**.

3.4 Managing All Your Clients

3.4.1 Thin Clients Tab Overview

Thin **Clients** tab helps you to manage all your clients. To access the functionality of **Thin Clients** tab, click the tab on ADM.

Thin Clients Tab Overview



Interface Elements

No.	Name	Description
1	Navigation Area	Click to access the desired management item.
2	Management Area	Select to perform desired tasks, configure desired settings, or view related information available under a selected item.

3.4.2 Available Tasks at a Glance

No.	Available Task	Section
1	Creating client groups	3.4.3
2	Managing client groups	3.4.4
3	Managing clients in a group	3.4.5 3.4.6
4	Creating setting profile groups	3.4.9
5	Managing setting profile groups	3.4.10
6	Creating client setting profiles	3.4.11
7	Managing client setting profiles	3.4.12
8	Using individualized client settings	3.4.13
9	Using hybrid client settings	3.4.14
10	Pushing settings to clients through your local network	3.4.15
11	Pulling settings from clients through your local network	3.4.16
12	Pushing certificates of remote computers to clients	3.4.17
13	Sending messages to clients	3.4.18
14	Editing or viewing basic information about a client	3.4.19
15	Rebooting clients through your local network	3.4.20
16	Shutting down clients through your local network	3.4.21
17	Starting Up Clients through Your Local Network	3.4.22
18	Updating client firmware	3.4.23
19	Installing and Uninstalling Software Packages	3.4.24
20	Taking client snapshots	3.4.25
21	Restoring client snapshots	3.4.26
22	Using the Shadow Feature	3.4.27
23	Exporting client data	3.4.28
24	Digging out profiles or managed clients with Quick Search	3.4.29
25	Digging out managed clients with filters	3.4.30
26	Managing your client filters	3.4.31

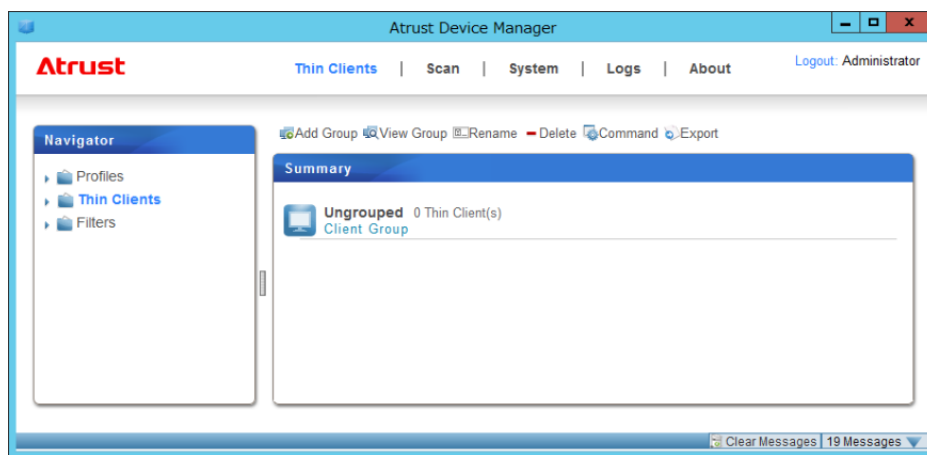
3.4.3 Creating Client Groups

You can create a client group for putting a set of clients together for ease of management.

Note The default client group is Ungrouped. You can change a client's group if needed.

To create a client group, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. Click **Add Group** on the top of the Management area.

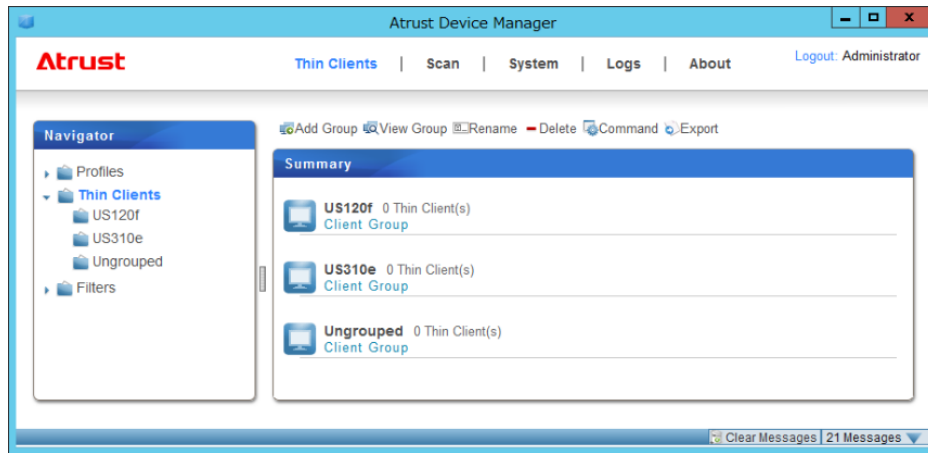


3. The Add Thin Client Group window appears prompting you for the name of the group.



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

5. The newly created group then appears in the Client Group list.



3.4.4 Managing Client Groups

Renaming a Client Group

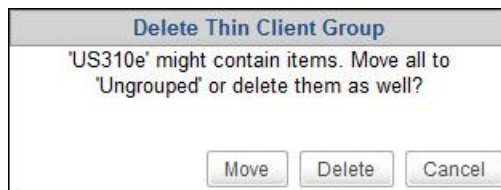
To rename a client group, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. In the Client Group list, click to select the desired client group, and then click **Rename** on the top of the Client Group list.
3. The Rename window appears prompting you for the new name of the selected client group.
4. Type in the new name for the group, and then click **OK** to confirm.

Deleting a Client Group

To delete a client group, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. In the Client Group list, click to select the desired client group, and then click **Delete** on the top of the Client Group list.
3. The Delete window appears prompting for confirmation.



Note

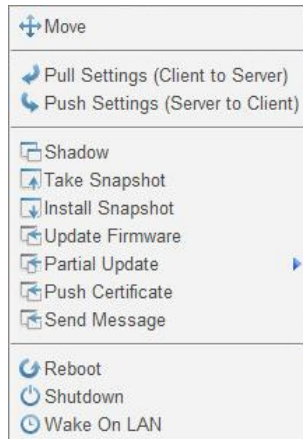
- To keep all clients in this group, leave Delete All Subitems cleared, and then click Move to confirm. All clients in this group will be moved to Ungrouped (the system default).
- To delete all clients in this group as well, select Delete All Subitems, and then click Delete to confirm. All clients in this group will be removed from your ADM.
- Removing a client from your ADM will release the client from the management of ADM.

4. The client group is deleted.

3.4.5 Moving Clients to Another Group

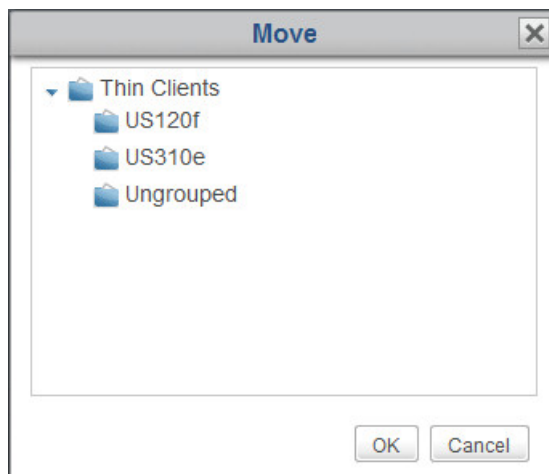
To move a client to another group, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. Click to select the desired client, and then click **Command** on the top of the Client list to open the Command menu.

**Note**

To select more than one client, Ctrl-click or use Select All to select multiple clients.

3. Click **Move** to open the Move window.



4. Click to select the desired group, and then click **OK** to confirm.

3.4.6 Deleting Clients from a Group

To delete a client from a group, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. Click to select the desired client, and then click **Delete** on the top of the Client list.

Note

To select more than one client, Ctrl-click or use Select All to select multiple clients.

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

Note

Removing a client from your ADM will release the client from the management of ADM.

3.4.7 Client Status Icons

In the client list of a client group or a filter, a client status icon is placed in front of each client to indicate the current state of the client.

Delete

Edit



Edit Configuration

Command

Select All

Unselect All

Export

	Name	IP Address	Mac Address	Model	Firmware
	atrust-033EB2	192.168.7.112	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

Note

With filters, you can access and manage a specific set of clients quickly on ADM. For more information on filters, please refer to section "3.4.30 Digging Out Clients with Filters".

The status icon changes according to different states of a client. Six types of icons are available:

Understanding Client Status Icons		
State	Icon	Description
Online		Indicates that the client is turned on at the moment.
Offline		Indicates that the client is turned off at the moment.
Reboot needed		Indicates that you need to reboot the client for a configuration change to take effect.
Modified		Indicates that a client configuration change has been made on ADM and you need to push the change to the client.
Pushed		Indicates that ADM has pushed a configuration change to the client.
Unknown		Indicates that the managed client is now added and managed by another instance of ADM.

Note

- On a Linux-based client, the icons are displayed with the letter L. () ()
- On a Windows Embedded-based client, the icons are displayed with the letter W. () ()
- The Configuration distributed icon () indicates that configuration has been distributed from ADM to the client. It does not indicate whether the application succeeded or failed.
- A tooltip pops up if you hover your mouse pointer over an icon.
- The icon indicates that ADM has sent setting changes to the client regardless of whether it succeeded or not. A pop-up message notifies you of whether the task succeeded or failed. If the task was performed on the thin client side, the thin client moves to the next state, and another status icon is displayed.

3.4.8 Client Settings

The desktop virtualization solution is available in various forms: user state virtualization, application virtualization, session based virtualization, virtual machine based virtualization, or even a hybrid approach. NEC thin clients can meet a wide range of forms and needs. However, to get your client device ready for use in your IT infrastructure, you might need to customize client settings to meet the specific needs in your desktop virtualization plan.

Additionally, for thin client devices of different divisions, departments, or areas, you might want to offer different computing resources and access privileges. To meet the specific types of policies on computing resources and access privileges, you might need to customize client settings as well.

Note

The available tabs and setting items may vary, depending on: the client model, firmware version, and the used operating system. For more details, please see "Chapter 4 Configuring Client Settings".

Remote and Local Management of Client Settings

You can configure your client settings locally or remotely. With ADM, you can configure client settings remotely through your local network. With ACS, client settings can be configured locally on a specific client.

Note

The ACS console is a built-in tool for almost all Atrust client products. This tool allows you to configure client settings locally on clients.

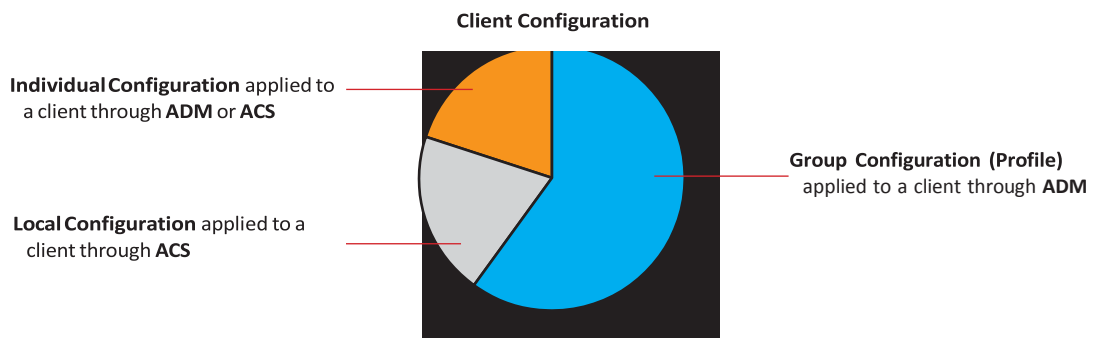
Some client settings are only available locally on clients. You can configure those settings locally through the ACS console. For a detailed list of client settings that are only locally available, please refer to section "4.2 Client Settings at a Glance".

Group Configuration and Individual Configuration

ADM enables you to apply a group configuration (profile), an individual configuration, or a hybrid of both to a client to set up its operating environment. With ACS, you can also make a desired individual configuration for a client.

Note




- A group configuration (profile) is a set of client settings shared by a set of clients.
- An individual configuration is a set of client settings applied only to a single client.
- A hybrid configuration is a mix of both group and individual configuration.





Method	Configuration Type	Console	Section
Local	Local configuration	ACS	4.2 Client Settings at a Glance 4.6 Configuring Client Settings with ACS
	Individual configuration	ACS	4.2 Client Settings at a Glance 4.6 Configuring Client Settings with ACS
Remote	Group configuration	ADM	3.4.11 Creating Client Setting Profiles
	Individual configuration	ADM	3.4.13 Using Individualized Client Settings

Please refer to related sections as shown above for detailed instructions on client configuration.

Locking Setting Values

ADM also allows you to lock setting values. When configuration with a locked setting value is pushed to thin clients, the gray lock icon () displayed next to the setting value of ACS on the thin client side will become the closed blue () or orange () lock icon.

The blue lock icon () indicates that the setting value is locked in profile settings, and the orange lock icon () indicates that it is locked in individual settings of the thin client.

If client settings are managed by the local ACS of the client, setting values cannot be locked.

3.4.9 Creating Setting Profile Groups

A setting profile (group configuration) is a set of client settings shared by a set of clients. Through a setting profile (group configuration), you can configure client settings in groups.

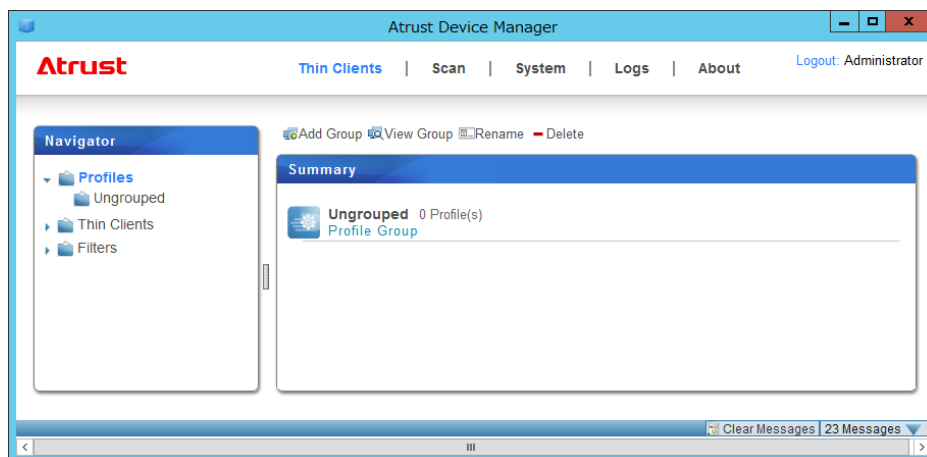
A setting profile group is a set of profiles grouped together for ease of management.

Note

To create a setting profile, first you need to select or create the profile group to which the new profile belongs. You can use the system default (Ungrouped), and then change the group of the profile at a later time if necessary.

To create a setting profile group, please do the following:

1. On **Thin Clients** tab, click **Profiles**.
2. The Profile Group list appears.

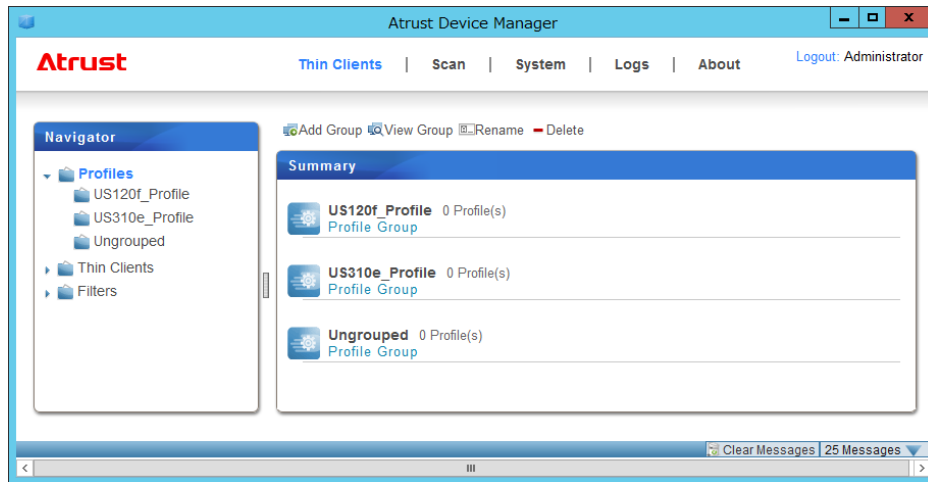
**Note**

Ungrouped is the system default group.

3. Click **Add Group** on the top of the Profile Group list.
4. The Add Profile Group window appears prompting for the name of the profile group.
5. Type in the desired name for the profile group, and then click **OK** to confirm.



6. The newly created profile group appears in the Profile Group list now.

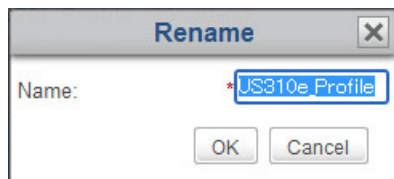


3.4.10 Managing Setting Profile Groups

Renaming a Setting Profile Group

To rename a setting profile group, please do the following:

1. On **Thin Clients** tab, click **Profiles**.
2. In the Profile Group list, click to select the desired profile group, and then click **Rename** on the top of the list.
3. The Rename window appears prompting for the new name.



4. Type in the new name for the profile group, and then click **OK** to confirm.

Deleting a Setting Profile Group

To delete a setting profile group, please do the following:

1. On **Thin Clients** tab, click **Profiles**.
2. In the Profile Group list, click to select the desired profile group, and then click **Delete** on the top of the list.
3. The Delete window appears prompting for confirmation.



Note

- To move profile settings registered in a profile group to "Ungrouped", click the Move button.
- To delete profile settings including settings registered in a profile group, click the Delete button.
- A setting profile is a set of client settings shared by a set of clients. Deleting a setting profile will change client settings of the corresponding clients.

3.4.11 Creating Client Setting Profiles

A setting profile (group configuration) is a set of client settings shared by a group of clients. Through a setting profile, you can remotely configure client settings in groups.

Note

To have a basic understanding of client configuration, please refer to section "3.4.8 Client Settings".

A simple picture of how to create a well-defined setting profile can be given by two steps:

Step 1: Create a set of shared client settings (group configuration)

Step 2: Specify the applicable scope of the setting profile

STEP 1: Create a set of shared client settings

To create a client setting profile (group configuration), please do the following:

1. On **Thin Clients** tab, click **Profiles** to expand the Profile Group tree, and then click to select the profile group.

Note

You need to select the profile group to which the new profile belongs first. You can use the system default (Ungrouped), and change the group at a later time if necessary. For detailed instructions on how to create a profile group, please refer to section "3.4.9 Creating Setting Profile Groups".

2. Click **Add** on the top of the Profile list.

+ Add - Delete ✎ Edit ⚙ Edit Configuration ↔ Move 📄 Copy				
Name	Platform	Model	Description	Number of Clients

3. The Add window appears prompting for the name, description, applicable platform, and models.

Add

✕

Name:

*

Description:

Platform:

Windows Embedded 8 Standard

▼

Model:

US310e

▼

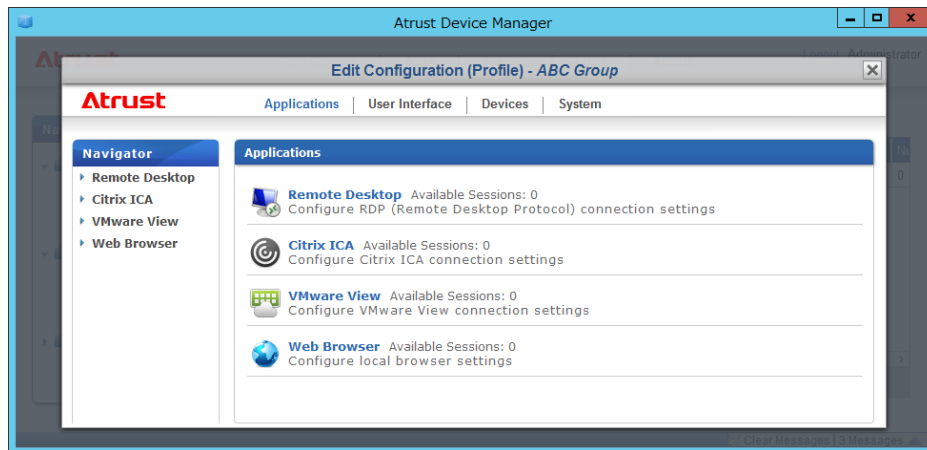
Save

Cancel

Note

A field marked with an asterisk is the required field.

4. Type in the desired name, description, choose the applicable platform and models, and then click **Save** to confirm.
5. The Edit Configuration window for the profile (group configuration) appears.

**Note**

The information displayed in the Configuration (Profile) window may be different from the image above depending on the selected platform/model. In this document, US310e is selected for Model as an example.

6. Use this window to edit client settings of this profile.

Note

The Edit Configuration window for the profile (group configuration) is just like a remote version of Atrust Client Setup on a client. You can simply edit client settings for this setting profile through this window. For detailed instructions on how to configure client settings, please refer to "Chapter 4 Configuring Client Settings".

7. After completion, close the window.
8. The newly created setting profile is added to the Profile list.

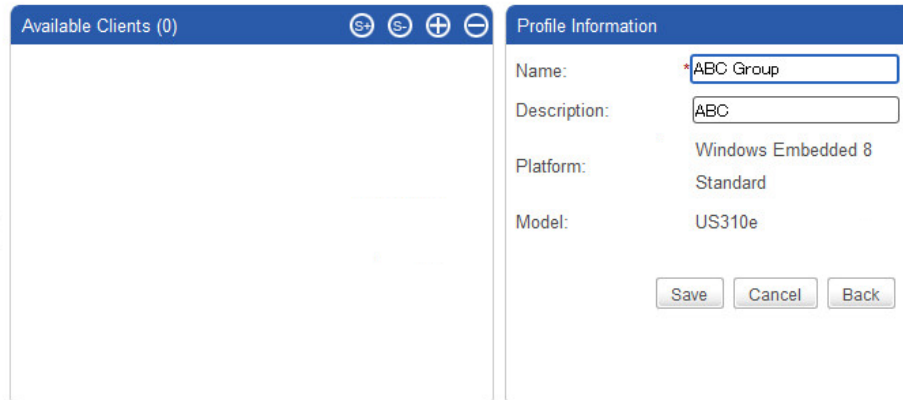
+ Add - Delete ✎ Edit ⚙ Edit Configuration ↔ Move 📄 Copy				
Name	Platform	Model	Description	Number of Clients
ABC Group	Windows Embedded 8 Standard	US310e	ABC	0


STEP 2: Specify the applicable scope of the setting profile

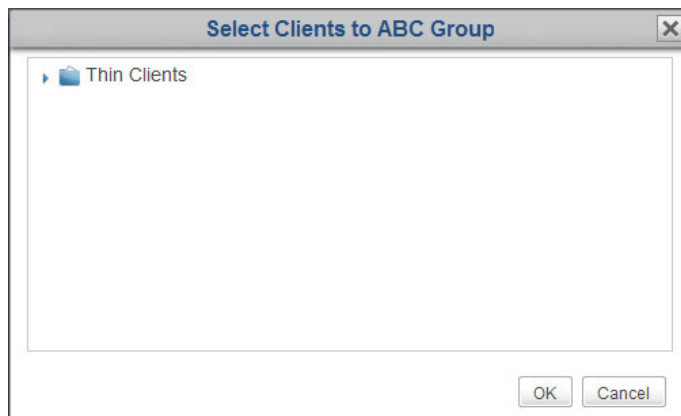
To specify the applicable scope of the setting profile, please do the following:

1. Click to select the newly created profile, and then click **Edit** on the top of the Profile list to specify the applicable scope of the profile.

- Both the Profile Information and Available Clients panes appear in Management area.



- Click () at the right top of the Available Clients pane.
- The Select Clients window appears. A tree view of client groups and individual clients is provided in this window for specifying the applicable scope of this setting profile.



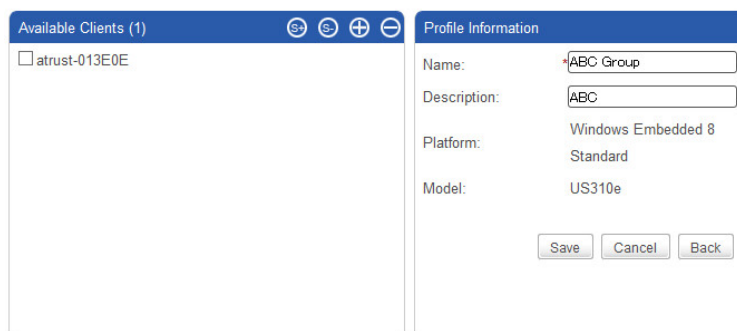
5. Click on arrows to expand the tree and click to select the desired client group or individual clients.



Note

- To select all clients under a client group, click to select the group.
- To select multiple clients under a client group, Ctrl-click to select the desired clients.
- The tree view of client groups and individual clients corresponds exactly to client groups and individual clients established under Thin Clients tab. For information on how to create client groups and add clients to a group, please refer to "3.4.3 Creating Client Groups" and "3.3.3 Client Detection and Management".
- A client can only be associated with a setting profile. If you associate a client with a new setting profile, it will be automatically removed from the old one.
- Associating a client with a profile does not actually change the settings of the client. You need to push settings to the client for the change to take effect (a reboot may be required as well). For instructions on how to push settings to a client, please refer to section "4.4 Editing or Adjusting an Individual Configuration".

6. After completion, click **OK** to confirm the selection of applicable clients.
7. Click **Save** in the Profile Information pane to complete the specification of applicable scope.



3.4.12 Managing Client Setting Profiles

Adjusting a Setting Profile

To edit a setting profile (group configuration), please do the following:

1. On **Thin Clients** tab, click Profiles to expand the Profile Group tree, and then click the profile group to which the desired setting profile belongs.
2. The Profile list appears in Management area.

Add Delete Edit Edit Configuration Move Copy					
Name	Platform	Model	Description	Number of Clients	
ABC Group	Windows Embedded 8 Standard	US310e	ABC	1	

3. Click to select the desired setting profile.
4. Select **Edit Configuration** to adjust client settings for the selected profile or select **Edit** to adjust the profile information and/or the applicable scope of the selected profile.

Note

- To adjust client settings, change desired settings directly in the opened Edit Configuration window.
- To adjust profile information, make changes in the Profile Information pane, and then click Save to apply.
- For detailed instructions on the adjustment of client settings or profile information, please refer to section "3.4.11 Creating Client Setting Profiles"
- To adjust the applicable scope of this profile, use (), (), (), () to make desired changes, and then click Save to apply.

Button	Description
	Click to select all clients in the client list.
	Click to unselect all clients in the client list.
	Click to add new clients.
	Click to remove the selected clients.

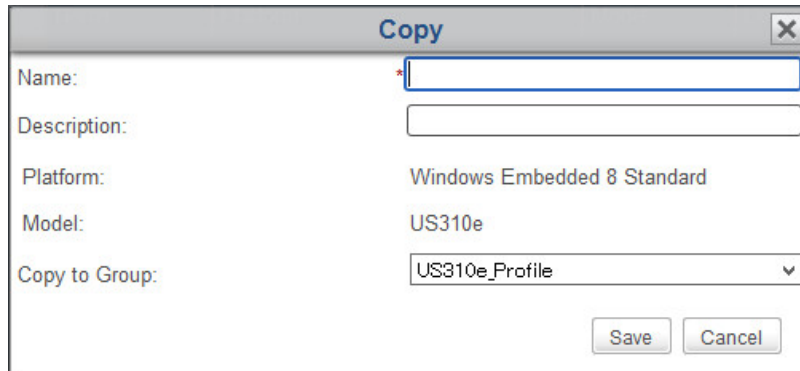
Copying a Setting Profile

To copy a setting profile (group configuration), please do the following:

1. On **Thin Clients** tab, click **Profiles** to expand the Profile Group tree, and then click the profile group to which the desired setting profile belongs.
2. The Profile list appears in Management area.

Add Delete Edit Edit Configuration Move Copy					
Name	Platform	Model	Description	Number of Clients	
ABC Group	Windows Embedded 8 Standard	US310e	ABC	1	

3. Click to select the desired setting profile, and then click **Copy**.
4. The Copy window appears prompting for the name, description, and profile group.



Copy [X]

Name: *

Description:

Platform: Windows Embedded 8 Standard

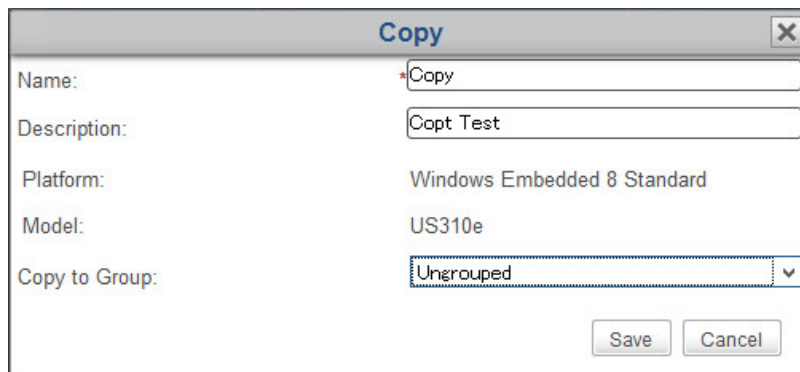
Model: US310e

Copy to Group: US310e_Profile ▼

Save Cancel

Note A field marked with an asterisk is the required field.

5. Provide the required data, and then click **Save** to confirm.



Copy [X]

Name: *Copy

Description: Copy Test

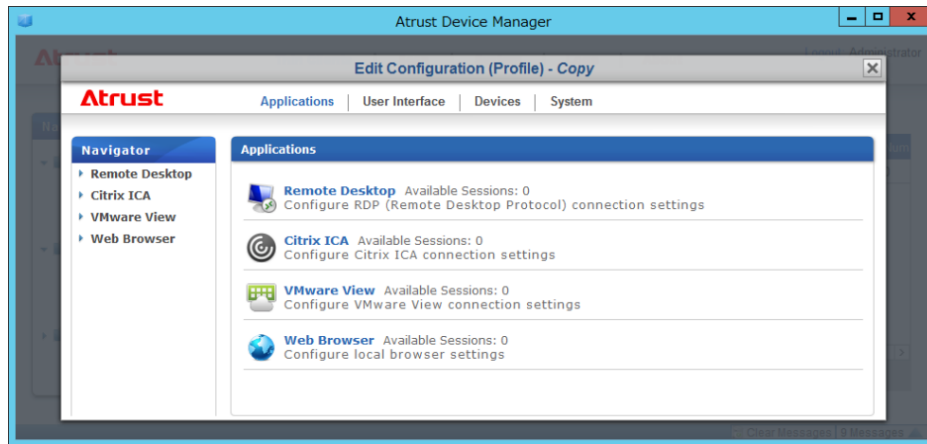
Platform: Windows Embedded 8 Standard

Model: US310e

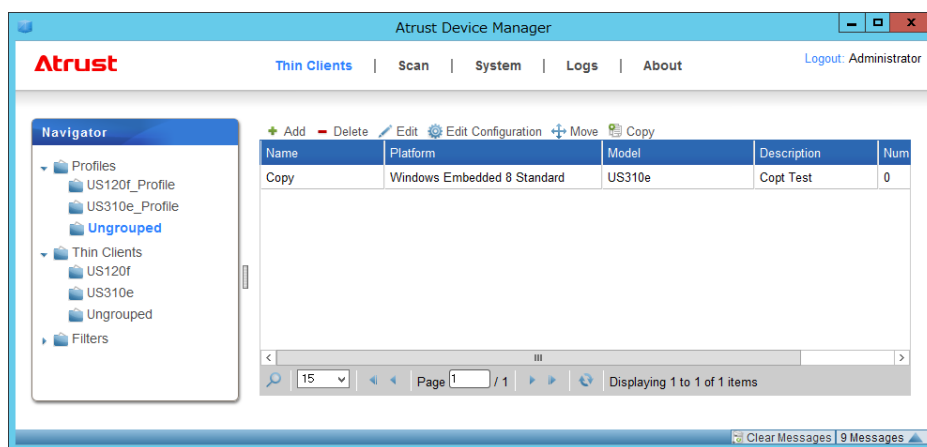
Copy to Group: Ungrouped ▼

Save Cancel

6. The Edit Configuration window for the profile (group configuration) appears.




7. Use this window to edit client settings of this profile.
 8. After completion, close the window.
 9. The newly created setting profile is added to the Profile list.

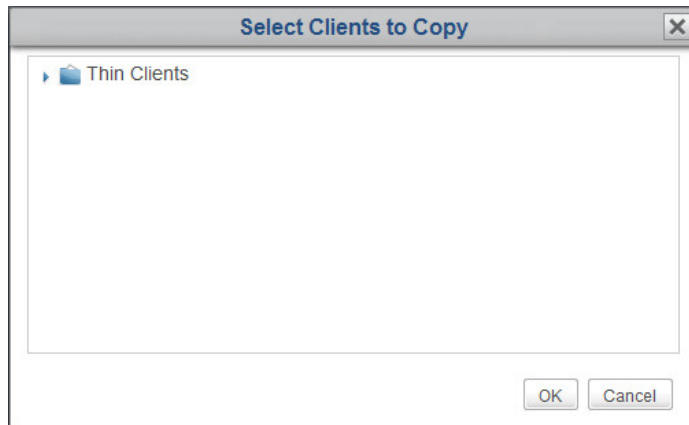


Note

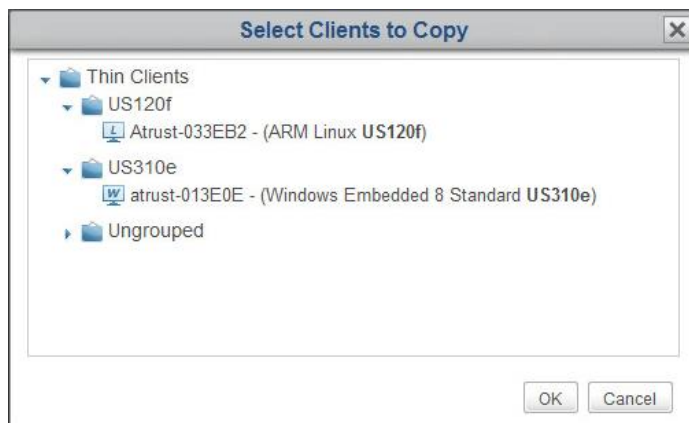
If you create a new profile by copying a well-defined setting profile, only the part of client settings is copied. The applicable scope of the original profile is not included.

10. Click to select the newly created profile, and then click **Edit** on the top of the Profile list.
 11. Both the Profile Information and Available Clients panes appear in Management area.
 12. Click () at the right top of the Available Clients pane.

13. The Select Clients window appears. A tree view of client groups and individual clients is provided in the window for specifying the applicable scope of this setting profile.



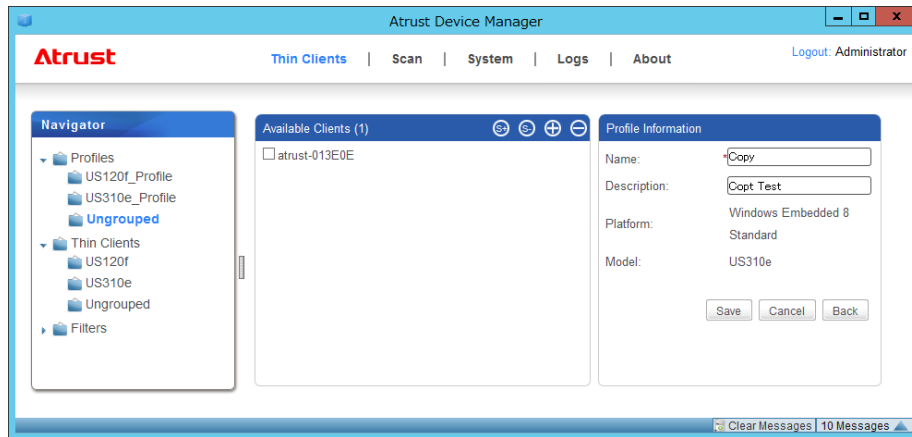
14. Click on arrows to expand the tree and click to select the desired client group or clients.

**Note**

- To select all clients under a client group, click to select the client group.
- To select multiple clients under a client group, Ctrl-click to select the desired clients.

15. After completion, click **OK** to confirm the selection of applicable clients.

16. Click **Save** in Profile Information pane to complete the specification of applicable scope.



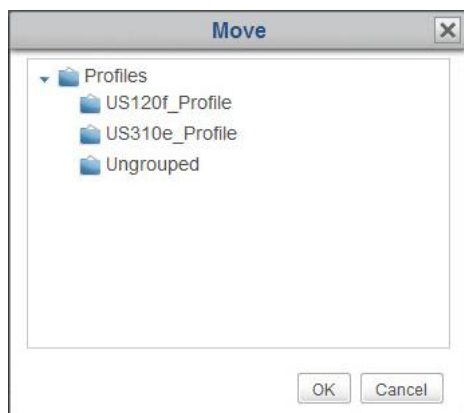
Moving a Setting Profile

To move a setting profile (group configuration) to another profile group, please do the following:

1. On **Thin Clients** tab, click **Profiles** to expand the Profile Group tree, and then click the profile group to which the desired setting profile belongs.
2. The Profile list appears in Management area.

+ Add - Delete ✎ Edit ⚙ Edit Configuration ↔ Move 📋 Copy				
Name	Platform	Model	Description	Number of Clients
ABC Group	Windows Embedded 8 Standard	US310e	ABC	1

3. Click to select the desired setting profile, and then click **Move**.
4. The Move window appears.

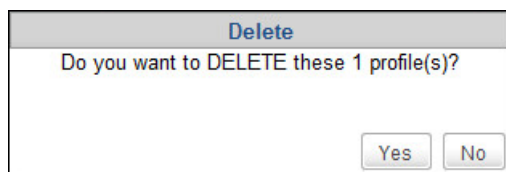


5. Click to select the desired profile group, and then click **OK** to confirm.
6. The selected setting profile is moved to the desired profile group.

Deleting a Setting Profile

To remove a setting profile (group configuration) from a profile group, please do the following:

1. On **Thin Clients** tab, click **Profiles** to expand the Profile Group tree, and then click to select the profile group.
2. The Profile list appears in Management area.
3. Click to select the desired setting profile, and then click **Delete**.
4. The Delete window appears prompting for confirmation.



5. Click **Yes** to confirm.

Note

A setting profile (group configuration) is a set of client settings shared by a set of clients. Deleting a well-defined setting profile will change client settings of the corresponding clients.

3.4.13 Using Individualized Client Settings

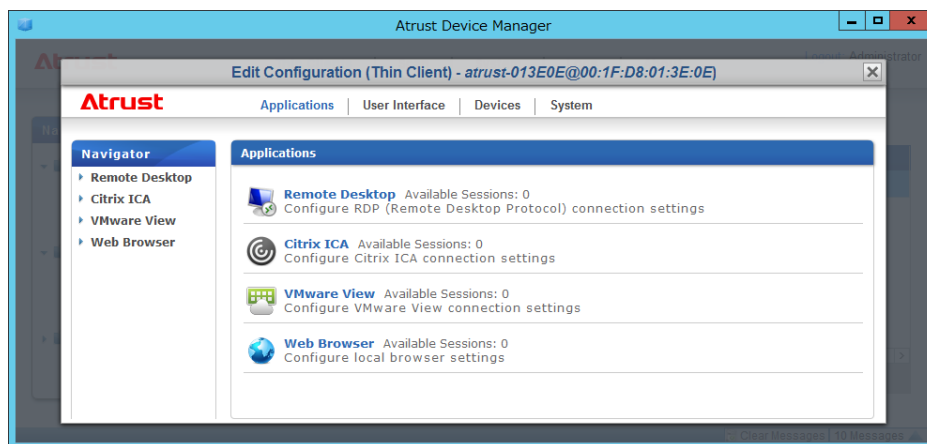
An individual configuration is a set of client settings applied only to a single client.

Note

- To have a basic understanding of client configuration, please refer to section "3.4.8 Client Settings".
- To ensure that your ADM is in sync with the setting values on managed clients, it's recommended to pull client settings from all managed clients for ADM before editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.16 Pulling Client Settings through Your Local Network".

To apply an individual configuration to a client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears in Management area.
3. Click to select the desired client, and then click **Edit Configuration**.
4. The Edit Configuration window for the client appears.

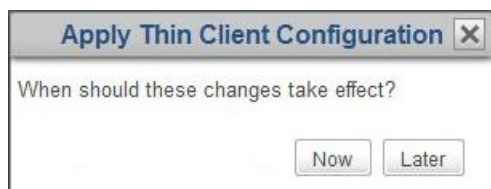


5. Use this window to edit the individual configuration.

Note

- The Edit Configuration window is just like a remote version of ACS. You can simply edit client settings for this client through this window.
- If the lock icon of a setting value is blue, this setting value comes from the group configuration (profile). You can only change the value by modifying/removing the group configuration (profile) or applying a new one.
- A client configuration using both group and individual configurations will be called a hybrid configuration (see section "3.4.14 Using Hybrid Client Settings").
- For detailed instructions on how to configure specific client settings, please refer to "Chapter 4 Configuring Client Settings".

6. After completion, close the window.
7. The Apply Thin Client Configuration window appears prompting for confirmation of when to apply.



8. Click **Now** to apply the configuration immediately or click **Later** to apply at a later time.

Note

If you choose to apply at a later time here, you can apply this individual configuration to the client by using the Pushing Settings feature.

3.4.14 Using Hybrid Client Settings

A hybrid configuration is a combination of a group configuration (profile) and an individual configuration.

Note

To have a basic understanding of client configuration, please refer to section "3.4.8 Client Settings".

A simple picture of how to use a hybrid configuration can be given by two steps:

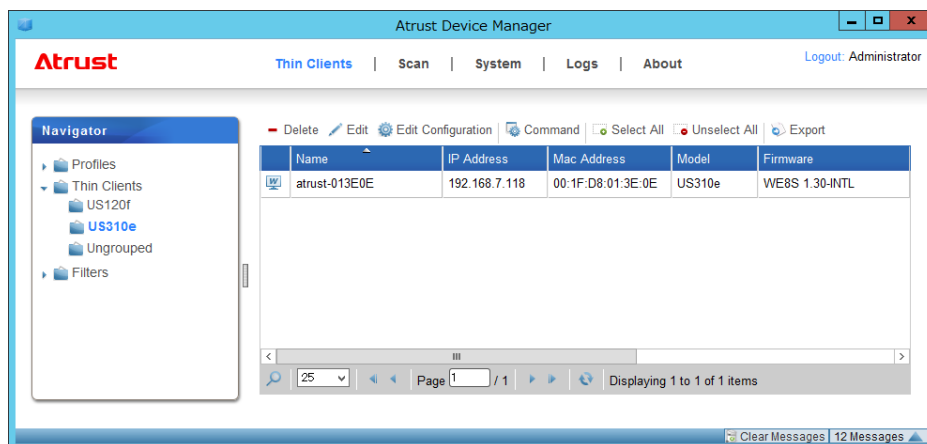
Step 1: Apply a group configuration to the selected client.

Step 2: Apply an individual configuration to the client.

STEP 1: Apply a group configuration to the selected client

To apply a group configuration to a client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.



3. Click to select the desired client, and then click **Edit**.

4. The Thin Client Information pane appears in Management area.

The screenshot shows the Atrust Device Manager interface. On the left is a Navigator pane with a tree view containing Profiles, Thin Clients (with sub-items US120f, US310e, and Ungrouped), and Filters. The main area is titled 'Thin Client Information - (atrust-013E0E)'. It contains several input fields: Name (atrust-013E0E), Description, Profile (No Profile), Asset ID, IP Address (192.168.7.118), MAC Address (00:1F:D8:01:3E:0E), Serial Number (NA), Model Name (US310e), Last Boot Time (2017-03-17 16:07:31), and Firmware (WEBS 1.30-INTL). Below these is a Packages table with columns Name, Version, and Installed Date. The table contains one entry: Japanese Language Package, version 1.4, installed on 2017-03-14 12:42:08(UTC+09:00). At the bottom right are buttons for Save, Cancel, and Back. A status bar at the very bottom shows 'Clear Messages' and '12 Messages'.

5. Click the Profile drop-down menu to select the desired group configuration (profile), associating the selected client with this configuration, and then click **Save** to apply.

This screenshot is similar to the previous one, but the 'Profile' dropdown menu is open, showing a list of options: No Profile, No Profile, ABC Group, and Copy. The 'No Profile' option is currently selected. All other fields and the Packages table remain the same as in the previous screenshot. The status bar at the bottom still shows 'Clear Messages' and '12 Messages'.

Note

The other way to associate a client with a group configuration (profile) is to add the client to the applicable scope of the desired profile. For more information, refer to section "3.4.11 Creating Client Setting Profiles".

STEP 2: Apply an individual configuration to the client

To apply an individual configuration to the client next, please do the following:

Note

To ensure that your ADM is in sync with the setting values on managed clients, it's recommended to pull client settings from all managed clients for ADM before editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.16 Pulling Client Settings through Your Local Network".

1. Click to select the desired client again, and then click **Edit Configuration** this time.
2. Edit the individual configuration for the selected client.

Note

For more details, please refer to section "3.4.13 Using Individualized Client Settings".

3.4.15 Pushing Settings to Clients through Your Local Network

The **Push Settings** feature enables you to sync up client configuration on a client with the one set up in remote ADM. You can then configure client settings remotely through your local network.

Pushing Settings to a Client

To push settings to a client, please do the following:

Note

To ensure that your ADM is in sync with the setting values on managed clients, it's recommended to pull client settings from all managed clients for ADM before editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.16 Pulling Client Settings through Your Local Network".

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

Delete

Edit

Edit Configuration

Command

Select All

Unselect All

Export

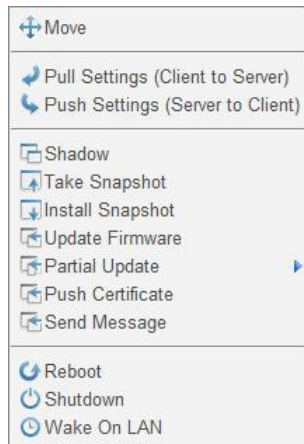
	Name	IP Address	Mac Address	Model	Firmware	Profile
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL	N/A

3. Click to select the desired client, and then click **Command** on the top of the Client list.

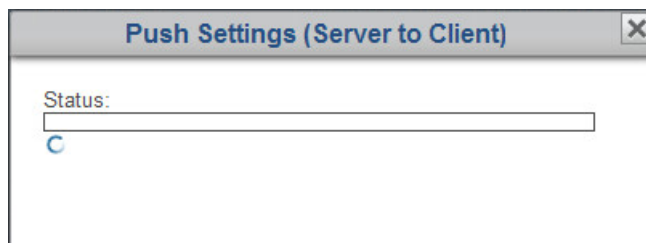
Note

- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that all selected clients are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

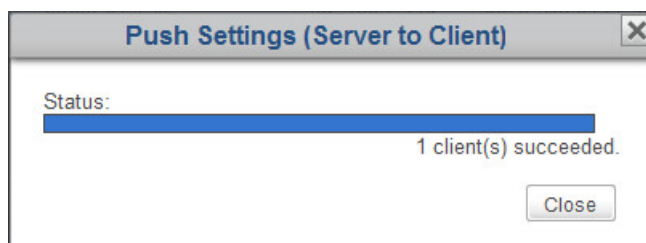
4. The Command menu appears.



5. Click to select **Push Settings**.
6. A window appears prompting for confirmation.
7. Click **OK** to confirm.
8. The Push Settings window appears showing the progress and result of pushing settings.



9. After completion, click **Close** to exit.



10. Check the status of the client through the Status icon in front of it. If needed, restart the client to complete the configuration changes on the client.

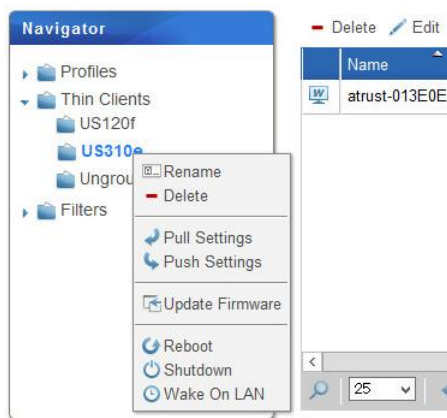
Pushing Settings to a Client Group

To push settings to a client group, please do the following:

Note

To ensure that your ADM is in sync with the setting values on managed clients, it's recommended to pull client settings from all managed clients for ADM before editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.16 Pulling Client Settings through Your Local Network".

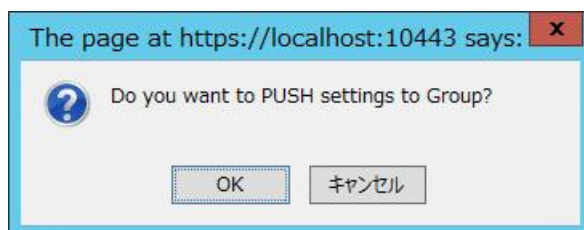
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu, and then click to select **Push Settings**.



Note

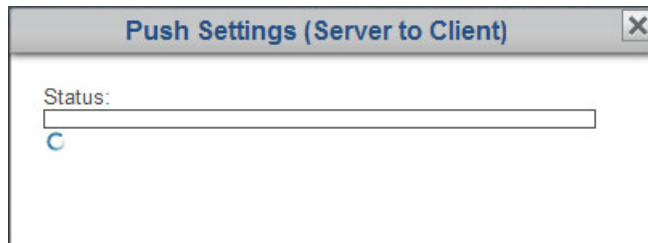
Ensure that all clients in the group are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

3. A window appears prompting for confirmation.

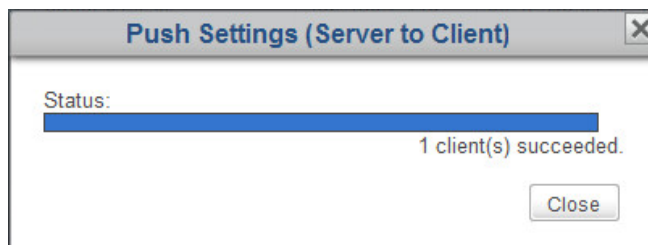


4. Click **OK** to confirm.

5. The Pushing Settings window appears showing the progress and result of pushing settings.



6. After completion, click **Close** to exit.



7. Check the status of clients in the group through the Status icon in front of clients. If needed, restart clients to complete the configuration changes on clients.

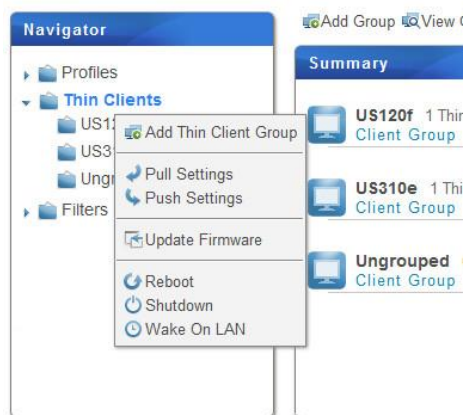
Pushing Settings to All Client Groups

To push settings to all client groups, please do the following:

Note

To ensure that your ADM is in sync with the setting values on managed clients, it's recommended to pull client settings from all managed clients for ADM before editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.16 Pulling Client Settings through Your Local Network".

1. On **Thin Clients** tab, right-click on **Thin Clients** in Navigation area to open a popup menu.

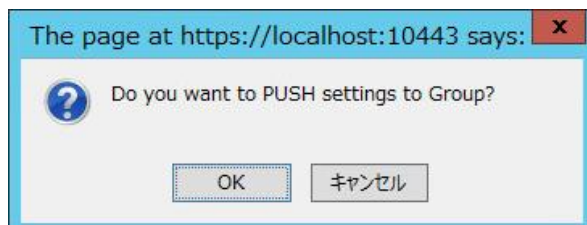


2. Click to select **Push Settings**.

Note

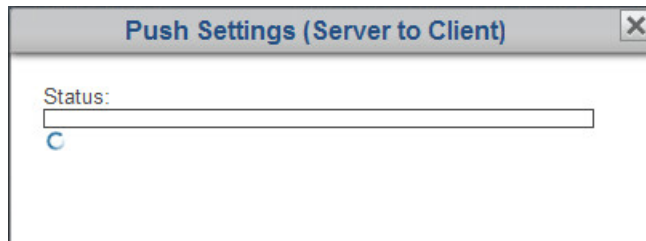
Ensure that all clients in the group are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

3. A window appears prompting for confirmation.

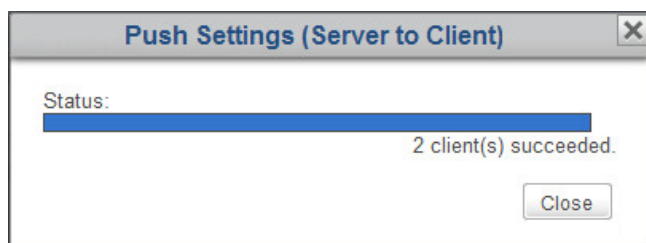


4. Click **OK** to confirm.

5. The Push Settings window appears showing the progress and result of pushing settings.



6. After completion, click **Close** to exit.



7. Check the status of clients through the Status icon in front of clients. If needed, restart clients to complete the configuration changes on clients.

3.4.16 Pulling Client Settings through Your Local Network

The **Pull Settings** feature enables you to retrieve settings from a client and store in ADM, which help you sync up the client configuration in ADM with the one set up locally on a client.

Pull Settings from a Client

To pull setting from a client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and click to select the client group to which the desired client belongs.
2. The Client list appears.

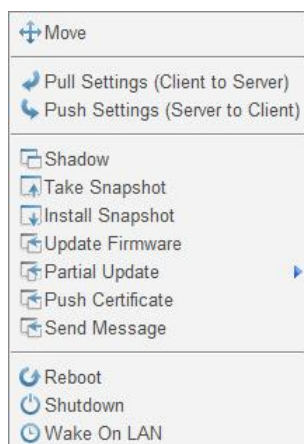
<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** on the top of the Client list.

Note

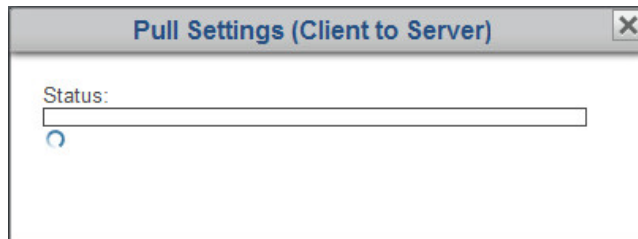
- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that all selected clients are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

4. The Command menu appears.

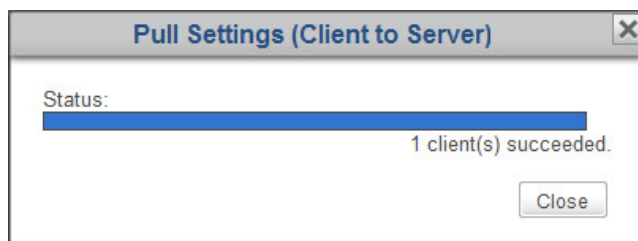


5. Click to select **Pull Settings**.
6. A window appears prompting for confirmation.
7. Click **OK** to confirm.

8. The Pull Settings window appears showing the progress and result of retrieving settings.



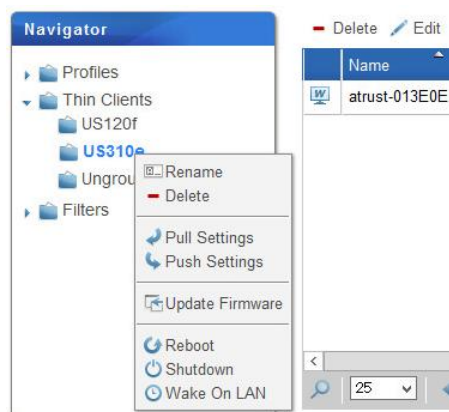
9. After completion, click **Close** to exit.



Pull Settings for a Client Group

To pull settings for a client group, please do the following:

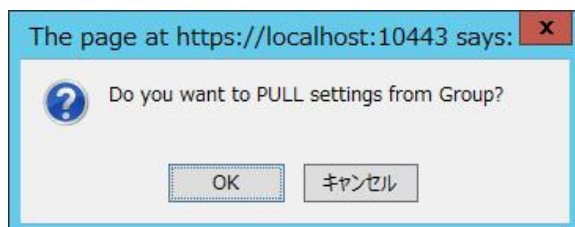
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group list.
2. Right-click on the desired client group to open a popup menu, and then click to select **Pull Settings**.



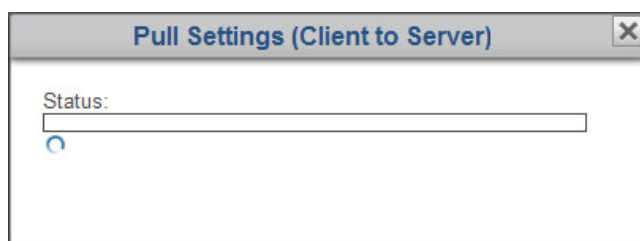
Note

Ensure that all clients in the group are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

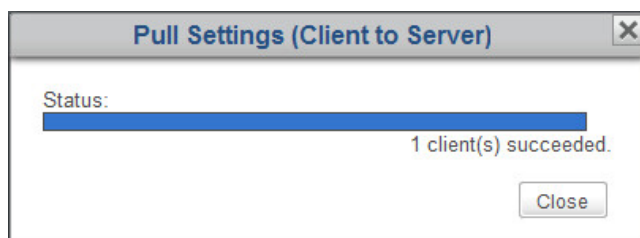
3. A window appears prompting for confirmation.



4. Click **OK** to confirm.
5. The Pull Settings window appears showing the progress and result of retrieving settings.



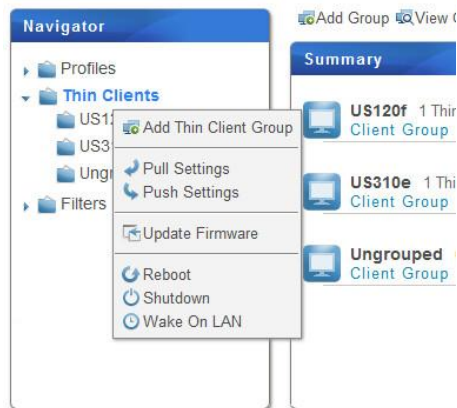
6. After completion, click **Close** to exit.



Pull Settings for all Client Group

To pull settings from all client groups, please do the following:

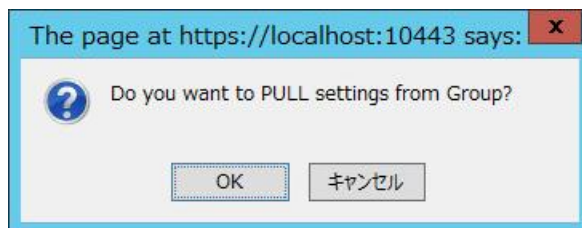
1. On **Thin Clients** tab, right-click on **Thin Clients** in Navigation area to open a popup menu.



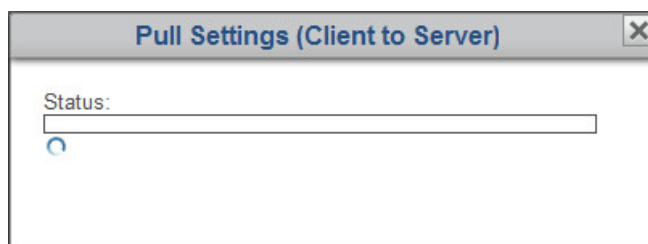
Note

Ensure that all clients in the group are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

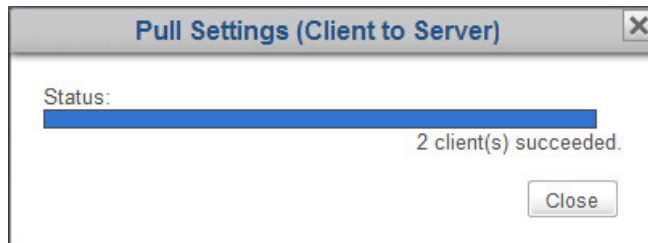
2. Click to select **Pull Settings**.
3. A window appears prompting for confirmation.



4. Click **OK** to confirm.
5. The Pull Settings window appears showing the progress and result of retrieving settings.



6. After completion, click **Close** to exit.



3.4.17 Pushing Certificates

You can push certificates imported on ADM to clients.

Before using this function, the certificates must be installed on ADM. For information on how to import certificates, please refer to "3.2.7 Managing Certificates".

Important The function to push certificates is supported only by US120f. This function is not supported by US320f/US310e.

To push a certificate to clients, please do the following:

Note All the certificates imported to ADM are pushed to the client. You cannot select which certificates to push.

1. On **Thin Clients** tab, click Thin Clients to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

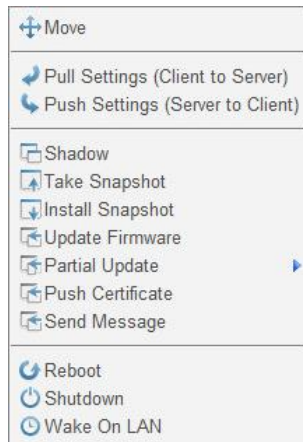
						
	Name	IP Address	Mac Address	Model	Firmware	Profile
	Atrust-033EB2	192.168.7.111	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC	N/A

3. Click to select the desired client, and then click **Command** on the top of the Client list.

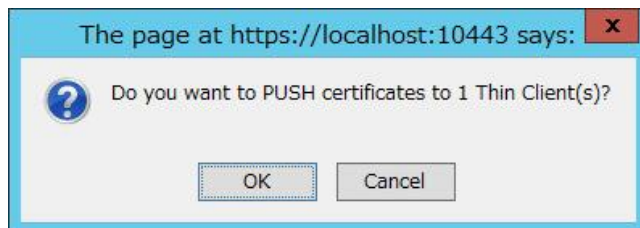
Note

- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that all selected clients are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.7 Client Status Icons".

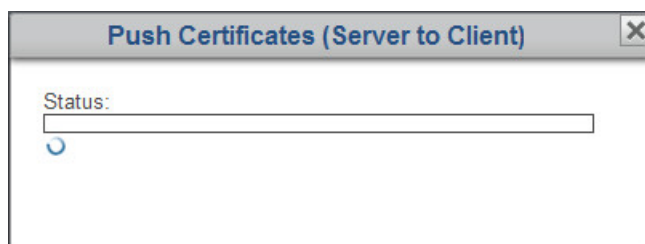
4. The Command menu appears.



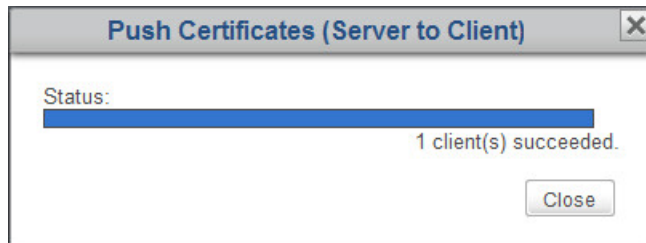
5. Click to select **Push Certificate**.
6. A window appears prompting for confirmation.



7. Click **OK** to confirm.
8. The Push Certificate window appears showing the progress and result of pushing the certificate.



9. After completion, click **Close** to exit.



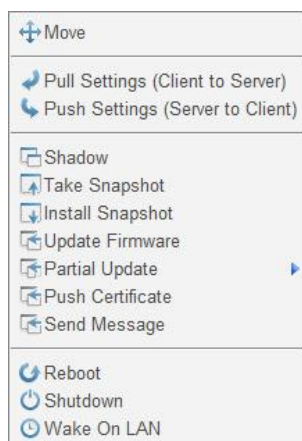
3.4.18 Sending Messages to Clients

To send a message to the managed client(s), please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

Delete Edit Edit Configuration Command Select All Unselect All Export					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client(s), and then click **Command** on the top of the Client list.
4. The Command menu appears.



5. Click to select **Send Message**.
6. A window appears prompting you to type in the countdown second(s) and message.

Send Message

Countdown Second(s):

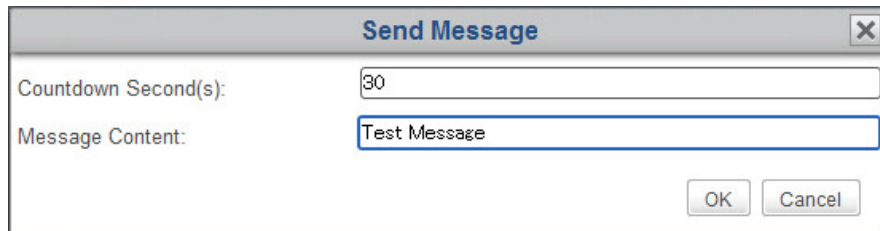
10

Message Content:

OK

Cancel

7. Type in the data, and then click **OK** to confirm.



A screenshot of a 'Send Message' dialog box. The dialog has a title bar with the text 'Send Message' and a close button (X). Inside the dialog, there are two text input fields. The first field is labeled 'Countdown Second(s):' and contains the value '30'. The second field is labeled 'Message Content:' and contains the text 'Test Message'. At the bottom right of the dialog, there are two buttons: 'OK' and 'Cancel'.

8. The message will be sent to the desired client(s).

3.4.19 Editing or Viewing the Basic Information about a Client

To edit or view the basic information about a client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

Delete

Edit

Edit Configuration

Command

Select All

Unselect All

Export

Name	IP Address	Mac Address	Model	Firmware
 atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Edit** on the top of the Client list.
4. The Thin Client Information pane appears.

Thin Client Information - (atrust-013E0E)

Name:

atrust-013E0E

Description:

Profile:

No Profile

Asset ID:

Save

Cancel

Back

IP Address:

192.168.7.118

MAC Address:

00:1F:D8:01:3E:0E

Serial Number:

NA

Model Name:

US310e

Last Boot Time:

2017-03-21 09:34:10

Firmware:

WE8S 1.30-INTL

Packages:

Name	Version	Installed Date
Japanese Language Package	1.4	2017-03-14 12:42:08(UTC+09:00)

5. Adjust the data of the client or view the basic information about the client.

Note

- To adjust the name, comment, profile (group configuration), Asset ID for the client, or type in the new data, and then click Save to apply.
- When selecting a profile (group configuration) from the drop-down menu, you add the client into the applicable scope of the selected profile.
- After viewing the basic information, click Back to return to the Client list.

3.4.20 Rebooting Clients through Your Local Network

The **Reboot** feature enables you to restart multiple clients through your local network without one by one going through the restart procedure. Most of the time, adjusting client settings and updating client firmware require a restart for those changes to take effect. With this feature, you are equipped with a necessary element for remote and centralized management of a large number of endpoint devices.

Rebooting a Client through Your Local Network

To restart a client through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.

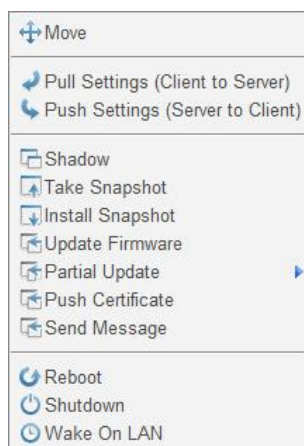
<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** to open the Command menu.

Note

- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that no important tasks are performed on the selected clients.

4. The Command menu appears.



5. Click to select **Reboot**.
6. On the selected client, a warning message appears to notify the user of the planned reboot and allow the user to cancel the action if necessary.
7. After completion, the Status icon will indicate the client is on-line again.

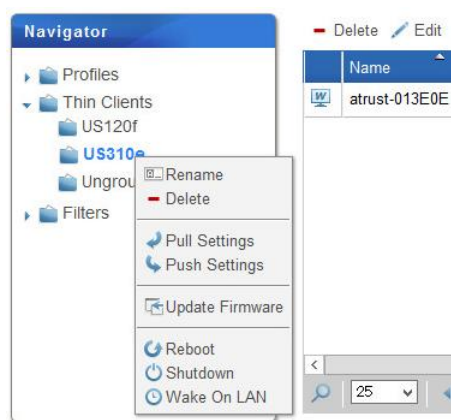
Note

For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

Rebooting a Client Group through Your Local Network

To restart a client group through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu.



3. Click to select **Reboot**.

Note

Ensure that no important tasks are performed on clients in the selected group.

4. On each client of this group, a warning message appears to notify the user of the planned reboot and allow the user to cancel the action if necessary.
5. After completion, the Status icons will indicate clients of this group are on-line again.

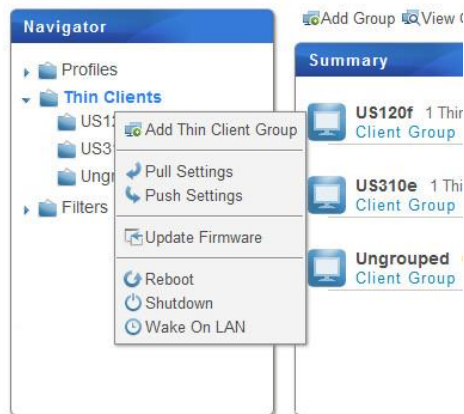
Note

For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

Rebooting All Client Groups through Your Local Network

To restart all client groups through your local network, please do the following:

1. On **Thin Clients** tab, right-click to open a popup menu.



2. Click to select **Reboot**.

Note Ensure that no important tasks are performed on clients in the selected group.

3. On all managed clients, a warning message appears to notify the user of the planned reboot and allow the user to cancel the action if necessary.
4. After completion, the Status icons will indicate all managed clients are on-line again.

Note For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

3.4.21 Shutting Down Clients through Your Local Network

Shutting Down a Client through your Local Network

To shut down a client through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.

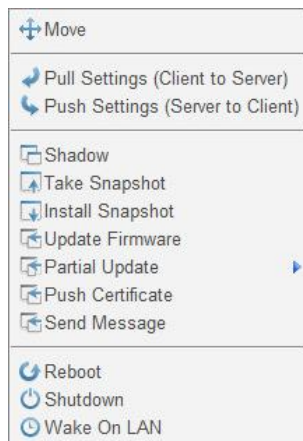
<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** to open the **Command** menu.

Note

- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that no important tasks are performed on the selected clients.

4. The Command menu appears.



5. Click to select **Shutdown**.
6. On the selected client, a warning message appears to notify the user of the planned shutdown and allow the user to cancel the action if necessary.
7. After completion, the Status icon will indicate the client is off-line.

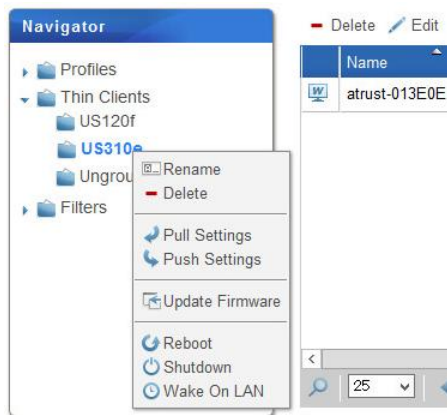
Note

For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

Shutting Down a Client Group through Your Local Network

To shut down a client group through your local network, please do the following:

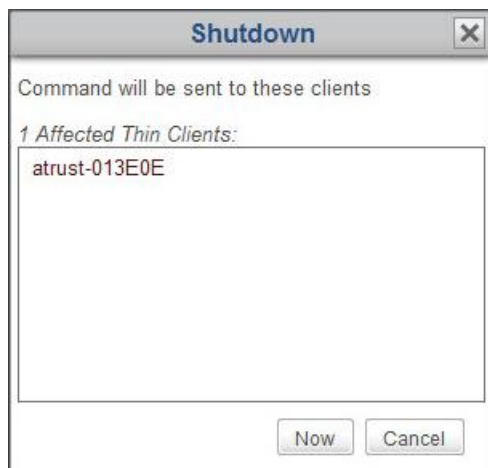
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu.



3. Click to select **Shutdown**.

Note Ensure that no important tasks are performed on clients in the selected group.

4. The Shutdown window appears prompting for confirmation.



5. Click **Now** to confirm.
6. On each client of this group, a warning message appears to notify the user of the planned shutdown and allow the user to cancel the action if necessary.
7. After completion, the Status icons will indicate clients of this group are off-line.

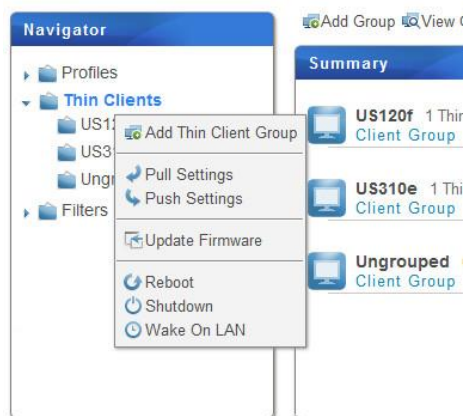
Note

For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

Shutting Down All Client Groups through Your Local Network

To shut down all client groups through your local network, please do the following:

1. On **Thin Clients** tab, right-click to open a popup menu.

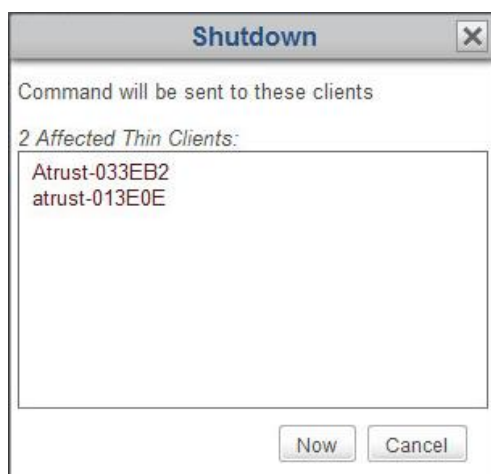


2. Click to select **Shutdown**.

Note

Ensure that no important tasks are performed on clients in the selected group.

3. The Shutdown window appears prompting for confirmation.



4. Click **Now** to confirm.

5. On all managed clients, a warning message appears to notify the user of the planned shutdown and allow the user to cancel the action if necessary.
6. After completion, the Status icons will indicate all managed clients are off-line.

Note

For information on the meanings of the Status icons, please refer to "3.4.7 Client Status Icons".

3.4.22 Starting Up Clients through Your Local Network

The Wake on LAN function can start up multiple clients through your local network if they are connected to a power outlet and the local network.

Important US120f does not support resume from suspend via Wake on LAN.

Starting Up Clients through Your Local Network

To start up a client through your local network, please do the following:

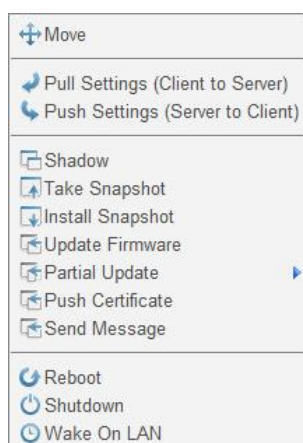
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.

Delete Edit Edit Configuration Command Select All Unselect All Export						
	Name	IP Address	Mac Address	Model	Firmware	Profile
	atrust-013E22	192.168.7.115	00:1F:D8:01:3E:22	US310e	WE8S 1.30-INTL	N/A
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL	N/A

3. Click to select the clients to start, and then click **Command** on the top of the Client list.

Note To select more than one client, Ctrl-click to select multiple clients.

4. The Command menu appears.



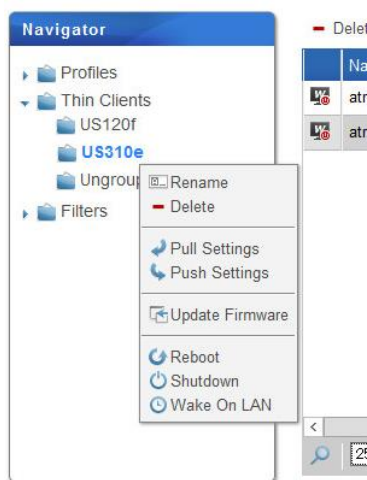
5. Click to select **Wake On LAN**.
6. The selected clients start up.
7. After completion, the Status icon will indicate the clients are on-line.

Note For details on status icons, please refer to "3.4.7 Client Status Icons".

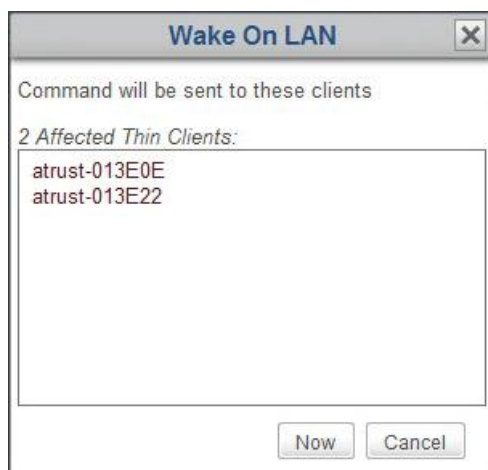
Starting Up a Client Group through Your Local Network

To start up a client group through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu.



3. Click to select **Wake On LAN**.
4. The "Wake On LAN" window is displayed for confirmation.



5. Click **Now** to confirm.
6. The clients in the client group start up.

7. After completion, the Status icon will indicate the clients are on-line.

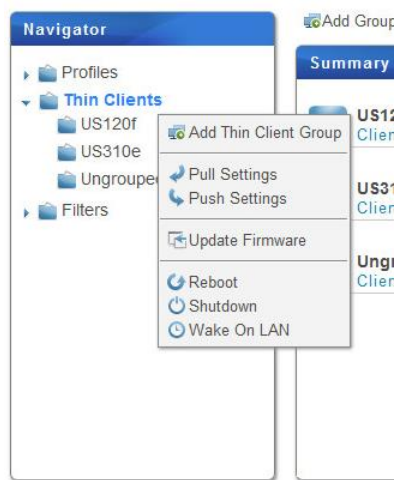
Note

For details on status icons, please refer to "3.4.7 Client Status Icons".

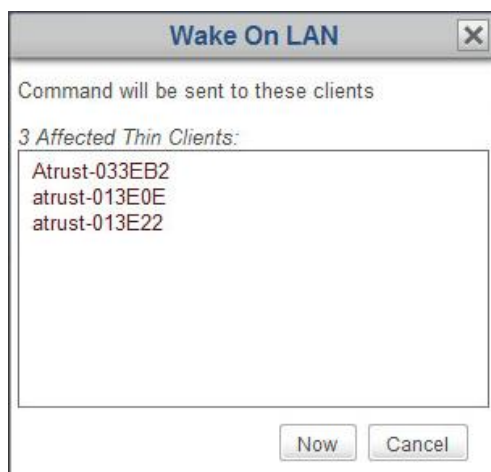
Starting up All Client Groups through Your Local Network

To start up all client groups through your local network, please do the following:

1. On **Thin Clients** tab, right-click to open a popup menu.



2. Click to select **Wake On LAN**.
3. The "Wake On LAN" window is displayed for confirmation.



4. Click **Now** to confirm.
5. All clients start up.

-
6. After completion, the Status icon will indicate the clients are on-line.

Note For details on status icons, please refer to "3.4.7 Client Status Icons".

3.4.23 Updating Client Firmware

To update the firmware for your client, please do the following:

Note

- To install a client firmware, the client firmware must be installed on A, or the client firmware must be taken. For information on how to import firmware, please refer to "3.2.4 Managing Thin Client Firmware Files".
- Updating client firmware will NOT erase any client configuration.

Updating client firmware through Your Local Network

To updating client firmware through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

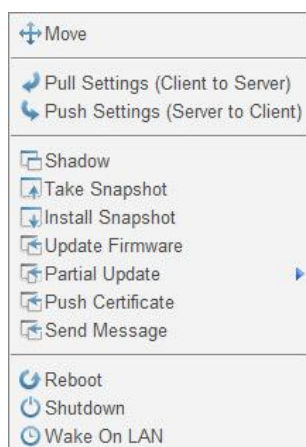
<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** on the top of the Client list.

Note

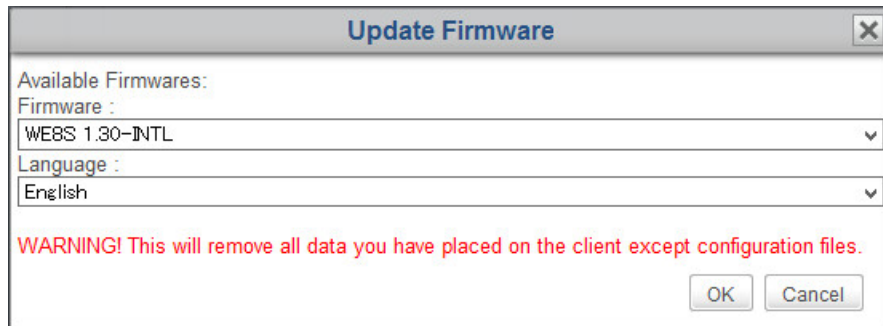
- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that no important tasks are performed on the selected clients.

4. The Command menu appears.

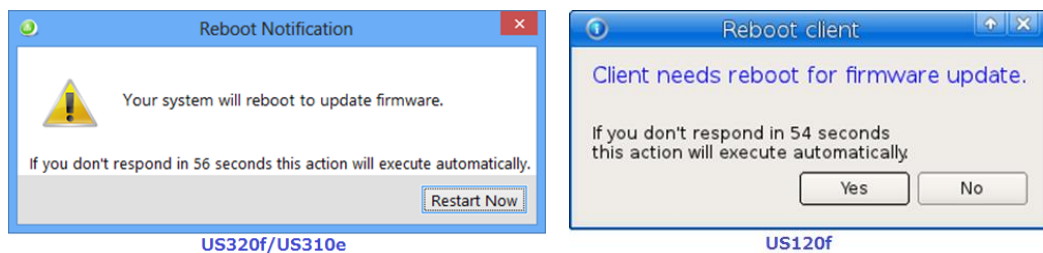


5. Click to select **Update Firmware**.

6. The Update Firmware window appears prompting you to select the firmware version and system language.



7. Click drop-down menus to select the desired firmware version and system language, and then click **OK** to confirm.
8. A warning message to notify the user of the planned reboot appears on the selected client. In US120f, the user is able to reboot later if necessary.

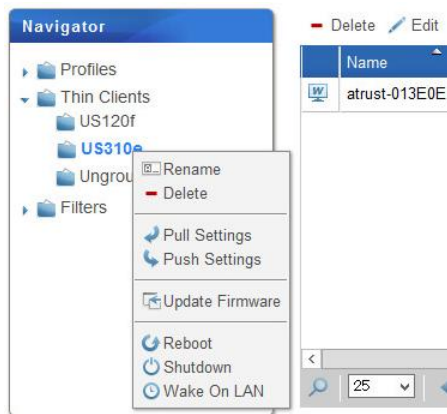


9. After completion, the client is updated with the desired firmware and system language.

Updating the Firmware of a Client Group through Your Local Network

To update the firmware of a client group through your local network, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu.

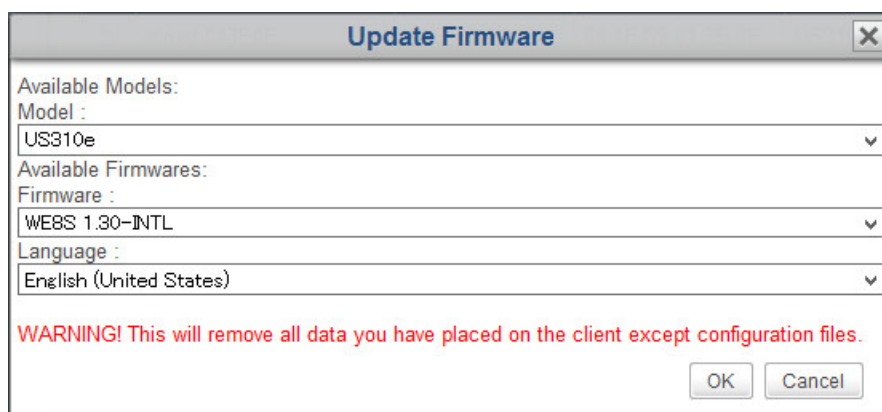


3. Click to select **Update Firmware**.

Note

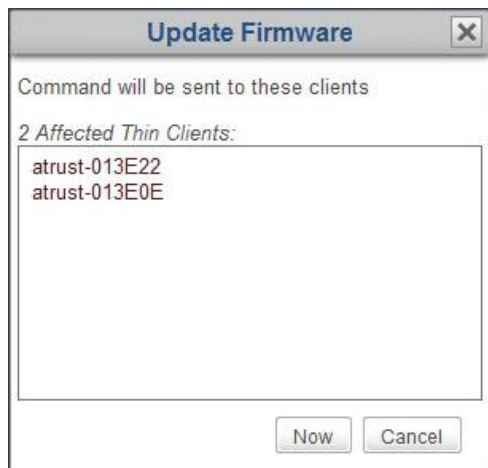
Ensure that no important tasks are performed on the clients registered in the selected client group.

4. The Update Firmware window appears prompting you to select the model, firmware, and language.

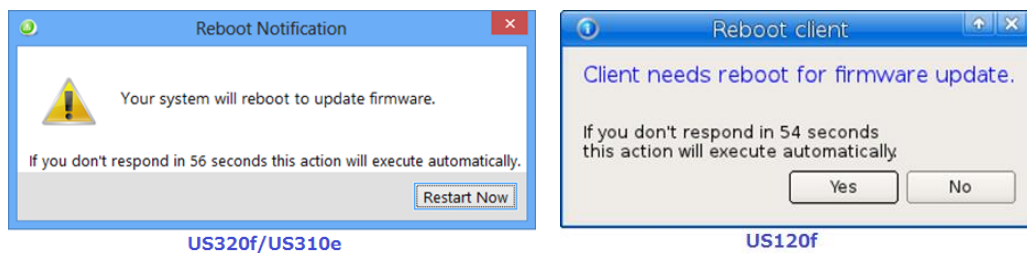


5. Click drop-down menus to select the desired model, firmware, and language, and then click **OK**.

6. The Update Firmware window appears prompting for confirmation



7. Click **Now** to confirm.
8. A warning message to notify the user of the firmware update appears on the selected client.



9. After reboot, the client is updated with the desired firmware and system language.


3.4.24 Installing and Uninstalling Software Packages

To install or uninstall a software package on a client, please do the following:

Important US120f does not support distribution of WES packages.

Note The WES packages must be installed on ADM. For information on how to import WES packages, please refer to "3.2.5 Managing WES Package Files".

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

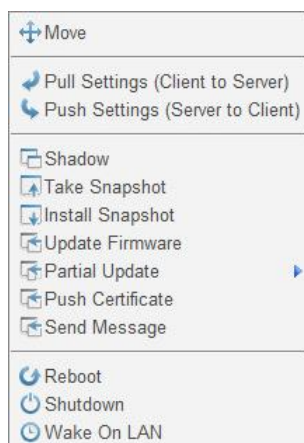
						
Name	IP Address	Mac Address	Model	Firmware		
 atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL		

3. Click to select the desired client, and then click **Command** on the top of the Client list.

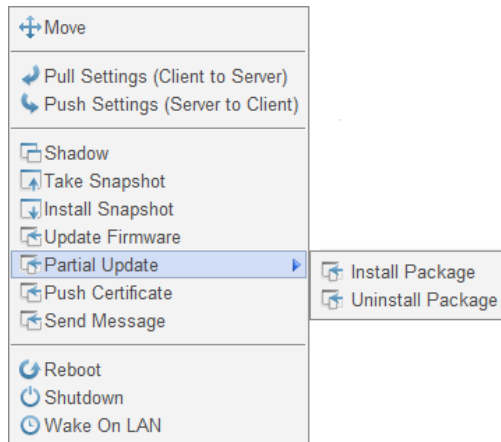
Note

- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that no important tasks are performed on the selected clients.

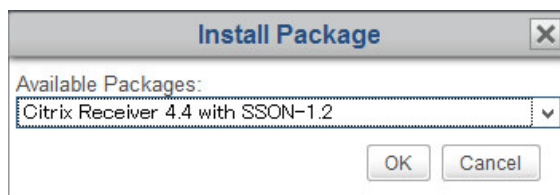
4. The Command menu appears.



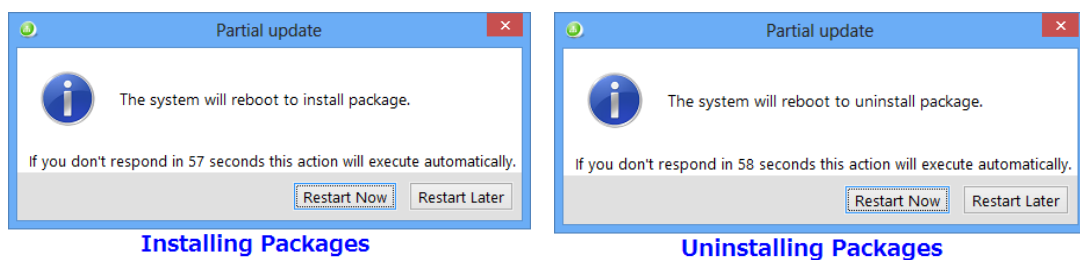
5. Click to select **Partial Update > Install Package** or **Uninstall Package**.



6. In the opened window, select the desired software package to install or uninstall, and then click **OK**.



7. A warning message to notify the user of the planned reboot appears on the selected client. The user is able to reboot later if necessary. Multiple reboots are required to complete this task.



8. After completion, the WES package is installed on the selected client.

Tips

To check if package distribution is complete remotely, click to select the client, and then click Edit to view the basic information of the client. For details, please refer to "3.4.19 Editing or Viewing the Basic Information about a Client".

3.4.25 Taking Client Snapshots

A snapshot is the system copy of a client at a specific point of time, which you can use for mass deployment, system backup, and recovery.

Important US120f does not support taking snapshots.

To take a system snapshot for a client, please do the following:

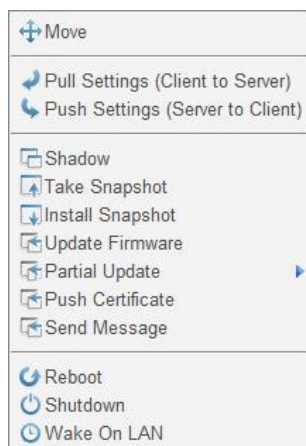
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.

Delete Edit Edit Configuration Command Select All Unselect All Export					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** on the top of the Client list.

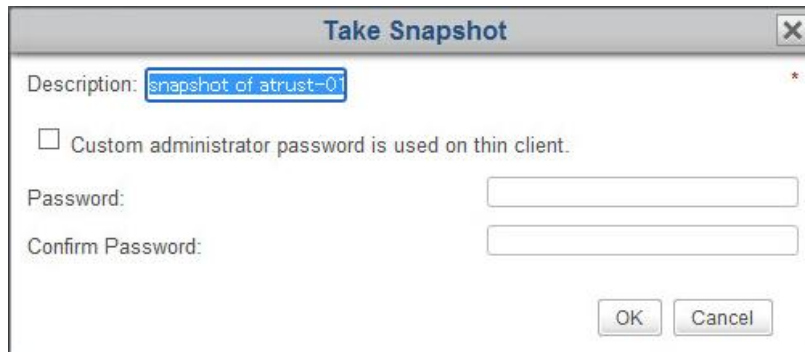
Note You can take system snapshot for only one client at a time.

4. The Command menu appears.



5. Click to select **Take Snapshot**.

6. The Take Snapshot window appears prompting you to provide the name of the system snapshot.

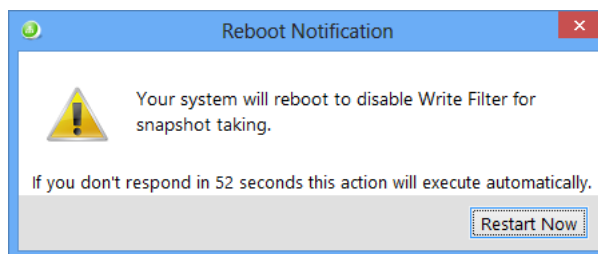


7. Type the name for the snapshot or use the default, and then click **OK** to confirm.

Note

In the case of changing the US310e built-in Administrator account default password, enable "Custom administrator password is used on thin client" and specify the changed password.

8. A warning message to notify the user of the planned reboot appears on the selected client..



9. After completion, taking the snapshot starts. Wait for a while until the process is complete.
10. After completion, the taken snapshot is added to the Snapshot list.

Note

- To access the Snapshot list, click System tab, and then click Deployment > Snapshot.
- Refer to section "3.2.6 Managing Client Snapshots" for instructions on how to manage your snapshots.

3.4.26 Installing Client Snapshots

To install a client snapshot, please do the following:

Important US120f does not support installation of snapshots.

Note To install a client snapshot, the client snapshot must be installed on ADM, or the client snapshot must be taken. For information on how to import snapshots, please refer to "3.2.6 Managing Client Snapshots". For information on how to take client snapshots, please refer to "3.4.25 Taking Client Snapshots".

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.

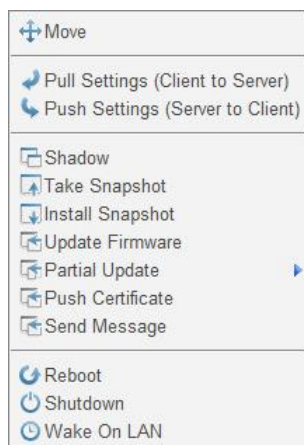
<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>					
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** on the top of the Client list.

Note

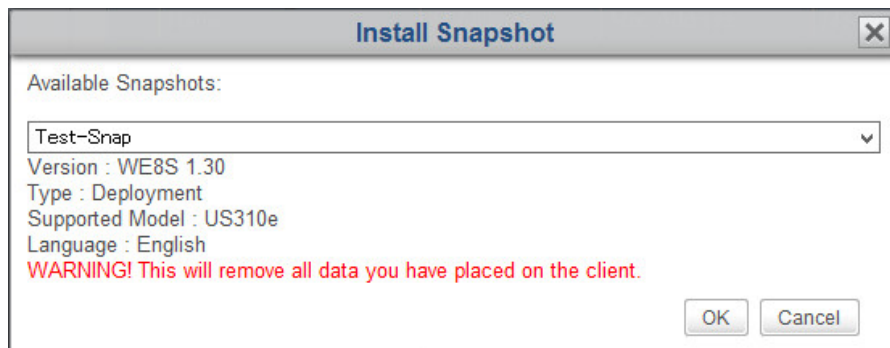
- To select more than one client, Ctrl-click to select the desired clients.
- Ensure that no important tasks are performed on the selected clients.

4. The Command menu appears.

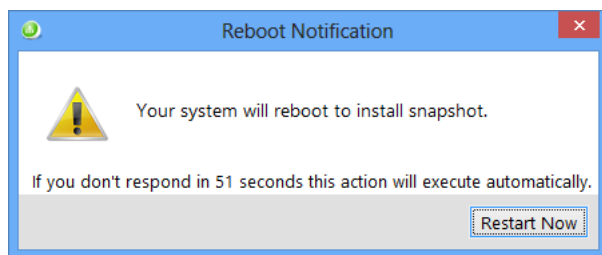


5. Click to select **Install Snapshot**.

6. The Install Snapshot window appears prompting you to select a snapshot.



7. Click the drop-down menu to select the desired snapshot, and then click **OK** to confirm.
8. A warning message to notify the user of the planned reboot appears on the selected client.



9. After completion, installation of the snapshot starts. Wait for a while until the installation is complete.

3.4.27 Using the Shadow Feature

The **Shadow** feature can be used to connect to a client to directly view or operate the client's desktop or sessions. The Shadow feature enables you to assist client users in resolving problems or configuring local settings.

Note To use the Shadow feature, it must be enabled on ACS of the client.

To connect to a client by using the Shadow feature, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.

Delete

Edit

Edit Configuration

Command

Select All

Unselect All

Export

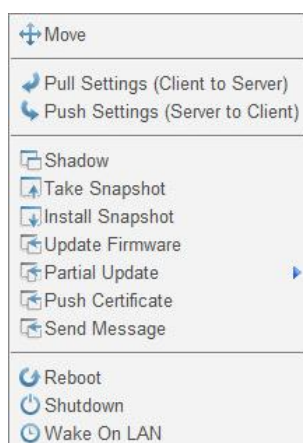
	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

3. Click to select the desired client, and then click **Command** on the top of the Client list.

Note

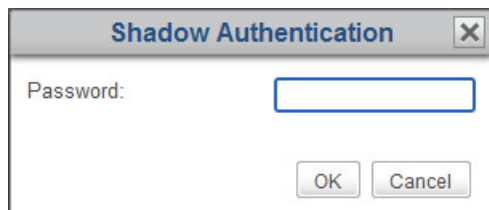
- You cannot use the Shadow feature with multiple clients specified.
- However, you can specify and connect to another client during connection using the Shadow feature.

4. The Command menu appears.

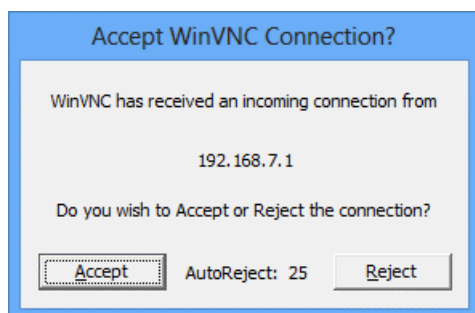


5. Select **Shadow**.

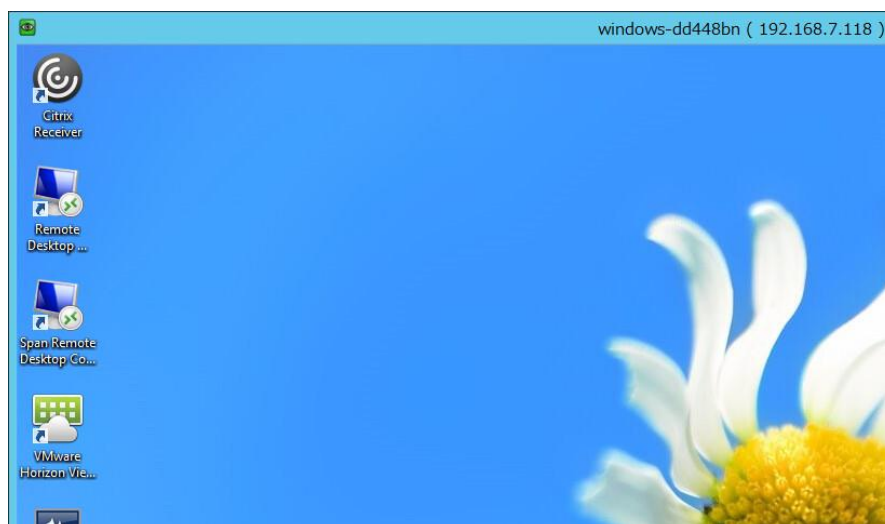
6. The "Authentication" window is displayed.



7. Enter the password of the shadow, and click **OK**.
8. A window appears prompting you to choose whether to accept shadow connection on the selected client. Click **Accept** if connection can be accepted without problem. In this document, connection is accepted.



9. The desktop screen of the selected client appears.

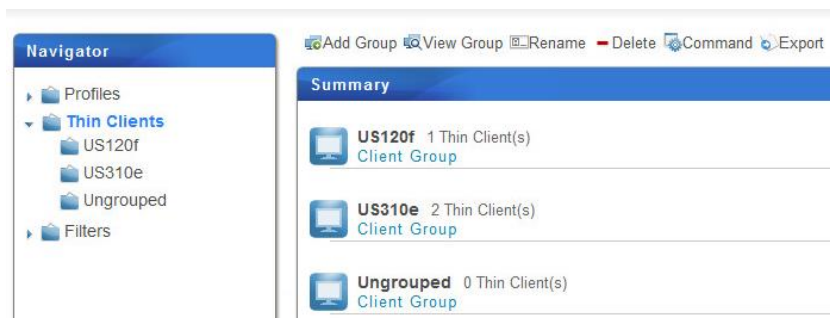


3.4.28 Exporting Client Data

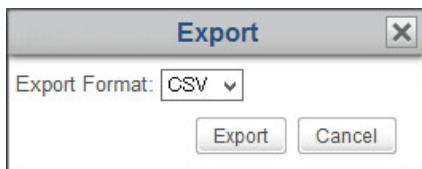
The **Export** feature available on the top of the Client Group list or the Client list allows you export an inventory of managed clients.

To export an inventory of managed clients, please do the following:

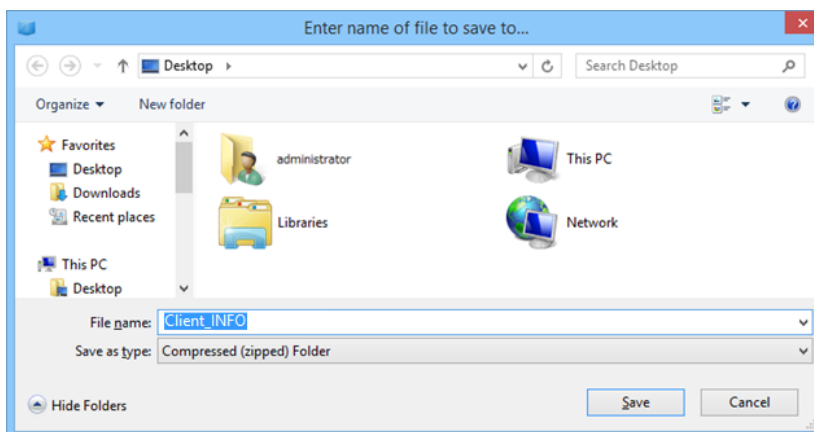
1. On **Thin Clients** tab, click to select the desired group in the Navigation area.
2. Click **Export** on the top of the Client Group list or the Client list.



3. A window appears prompting you to select the Export format: **CSV** or **XML**.



4. Click the drop-down menu to select the desired format, and then click **Export**.
5. A window appears prompting you to choose the save destination of the exported file. Save the exported file at the desired location.



3.4.29 Digging Out Profiles, Clients, or Event Logs with Quick Search

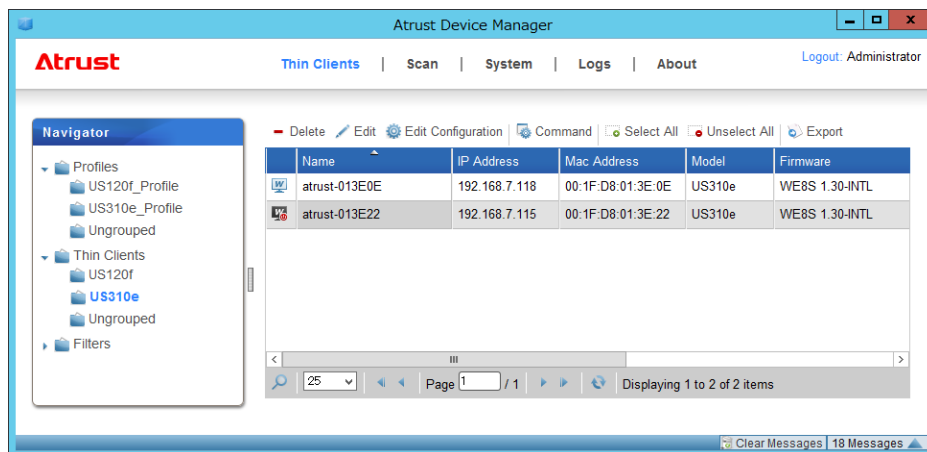
Quick Search allows you to detect profiles, thin clients, and logs.


Note

You can also use filters to find out the desired clients within the managed clients. For details, please refer to section "3.4.30 Digging Out Clients with Filters".

To dig out the desired profile, client, or event log on a Profile, Client, Event Log list, please do the following:

1. Open the Profile, Client, or Log List.
2. The Profile, Thin Client, or Log list appears in Management area. In this document, Thin Client is selected as an example.



3. At the bottom of the list, click the Quick Search button ().



4. The Quick Search bar appears.



5. Click the drop-down menu to select the desired search type and enter the desired search keyword.
6. Click **Search** to start searching for profiles, clients, or event logs.

7. On completion, the Result list appears above the Quick Search bar.

Delete

Edit


Edit Configuration

Command

Select All

Unselect All

Export

	Name	IP Address	Mac Address	Model	Firmware
	atrust-013E0E	192.168.7.118	00:1F:D8:01:3E:0E	US310e	WE8S 1.30-INTL

<

III

>

Quick Search

IP Address

118

Search

Clear

25

Page 1 / 1

Displaying 1 to 1 of 1 items

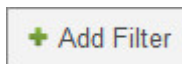
3.4.30 Digging Out Clients with Filters

ADM enables you to create filters for digging out clients from all managed clients. With filters, you can access and manage a specific set of clients quickly.

Adding a Filter

To add a filter, please do the following:

1. On **Thin Clients** tab, right click on the **Filters** in Navigation area.
2. A popup menu appears.
3. Click to select **Add Filter**



4. The Add New Filter and Filter Preview panes appear in Management area.

Add New Filter

Name: *

Field Name	Operator	Value	Action
Name	equals	<input type="text"/>	Add

Condition List

Preview

Save

Cancel

Filter Preview

Name	Group
Filter Preview	

5. Type in the desired name for this filter.
6. Click to select the desired field name, operator, and then type in the value for a filter condition.

Note

Most information about a client, which can be used as filter conditions, is available in the Thin Client Information pane. To access Thin Client Information pane, please refer to section "3.4.19 Editing or Viewing the Basic Information about a Client" for detail.

7. Click **Add** to add a condition to a filter.
8. Repeat steps 6 through 7 to add a new condition.

9. Click **Preview** to view the result of a filter. The result is displayed in the Filter Preview pane.

Add New Filter

Name:

Field Name	Operator	Value	Action
Model	equals	US310e	Add

Condition List

Model	equals	US310e	Delete
-------	--------	--------	--------

Preview Save Cancel

Filter Preview

Name	Group
atrust-013E22	US310e
atrust-013E0E	US310e

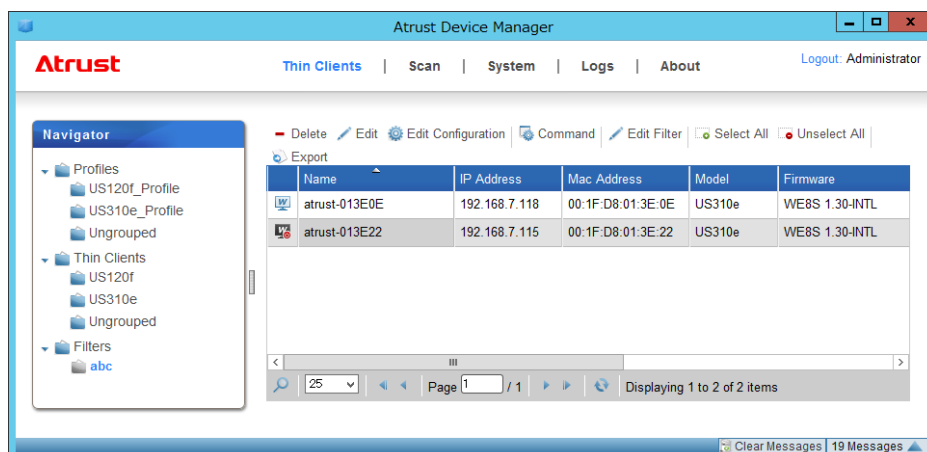
10. Click **Save** to create the filter.

Using a Client Filter

Once client filters are created, you can access the desired client list quickly just by clicking the corresponding filter. All clients which meet the defined conditions will be specified in the client list.

To use a client filter, please do the following:

1. On **Thin Clients** tab, click **Filters** to expand the Filter tree.
2. Click to select the desired filter.
3. The desired Client list appears.

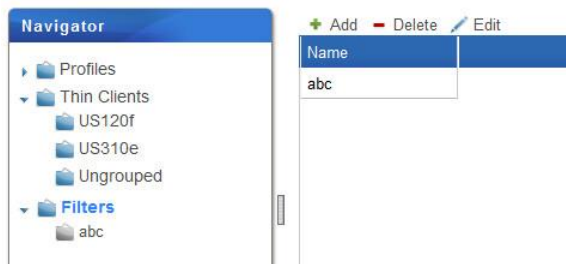


3.4.31 Managing Your Filters

Deleting a Filter

To delete a filter, please do the following:

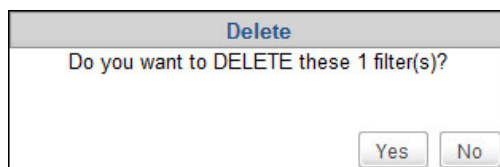
1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.



3. Click to select the desired filter, and then click **Delete** on the top of the Filter list.

Note To delete more than one filter, Ctrl-click to select multiple entries in the Filter list.

4. The Delete window appears prompting for confirmation.

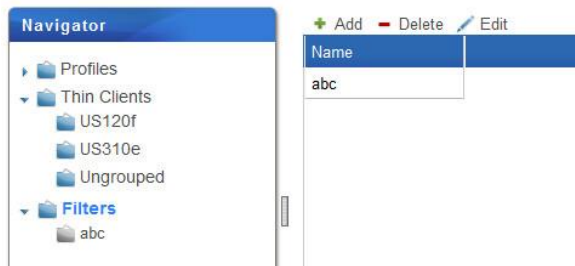


5. Click **Yes** to confirm.

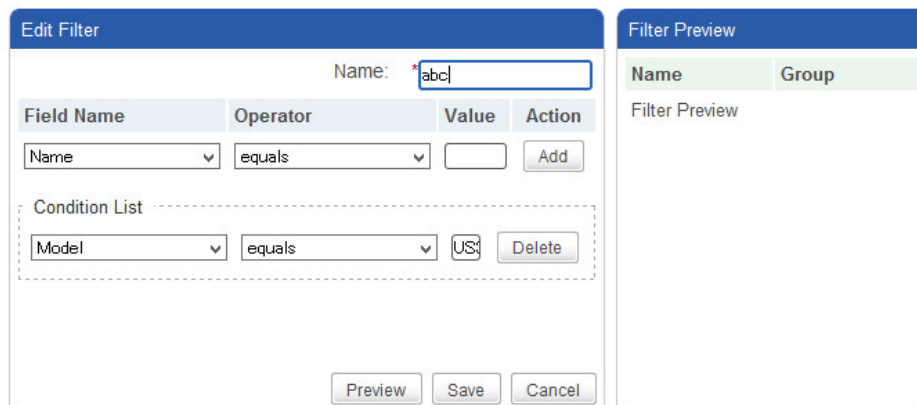
Adjusting a Filter

To adjust a filter, please do the following:

1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.



3. Click to select the desired filter, and then click **Edit** on the top of the Filter list.
4. The Filter Condition List and Filter Preview panes appear in Management area.

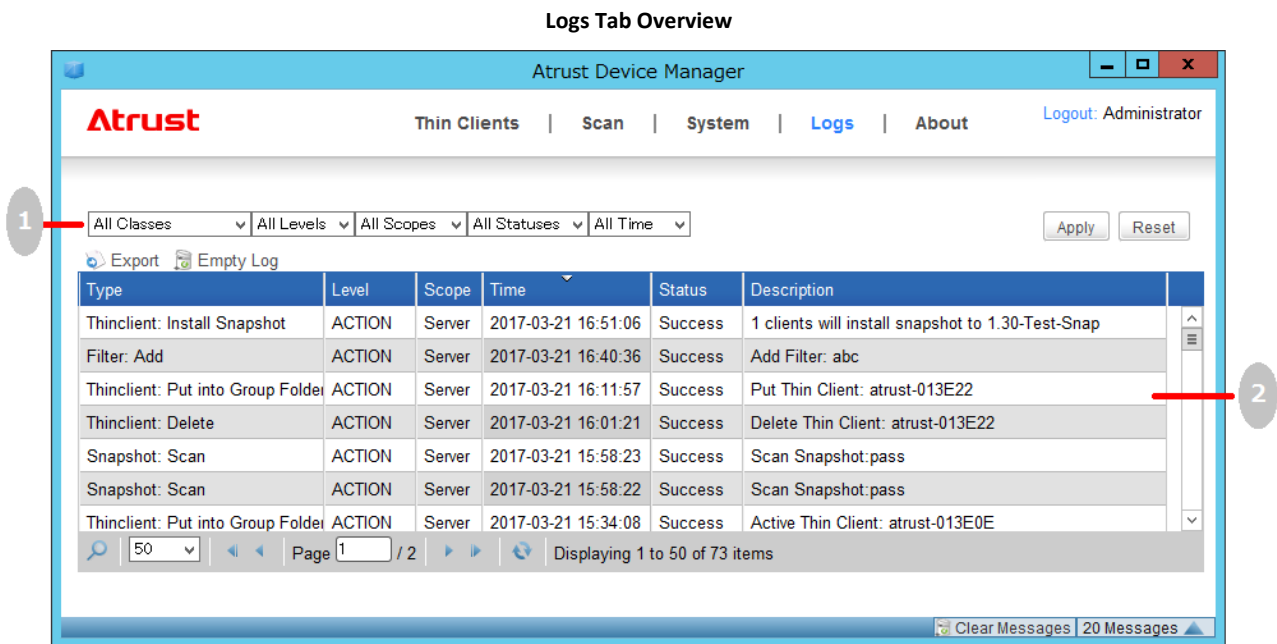


5. Adjust conditions for the filter, and then click **Save** to apply.

3.5 Viewing and Managing Event Logs

3.5.1 Logs Tab Overview

Logs tab enables you to view event logs about the management of your clients. To access the functionality of **Logs** tab, click the tab on ADM.



Interface Elements

No.	Name	Description
1	Navigation Bar	Click to select the desired type and scope of event logs.
2	Management Area	Manage event logs.

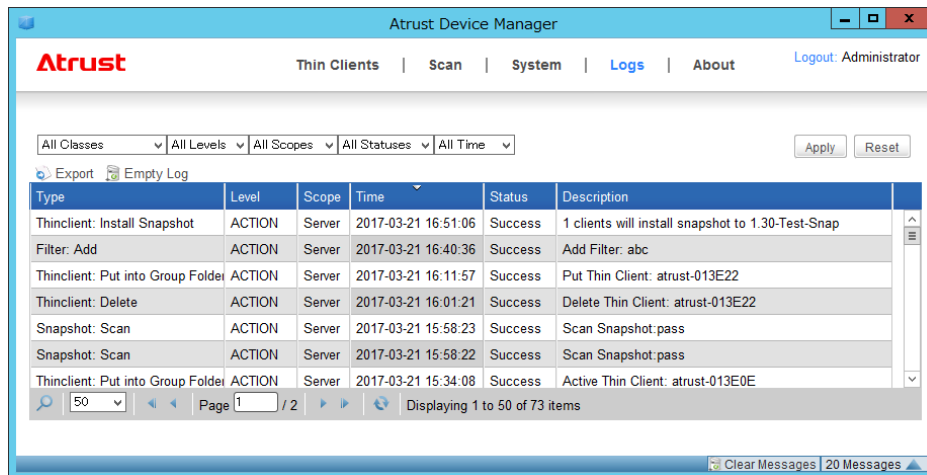
3.5.2 Available Tasks at a Glance

No.	Available Task	Section
1	Viewing your event logs	3.5.3 Viewing Event Logs
2	Exporting your event logs	3.5.4 Exporting Event Logs
3	Emptying your event logs	3.5.5 Emptying Event Logs

3.5.3 Viewing Event Logs

To review event logs of ADM, please do the following:

1. On ADM, click **Logs** tab.
2. The Log list appears.



Note

- To view log entries on different pages, click () () () () to change to the first/previous/next/last page.

50 Page 1 / 2 Displaying 1 to 50 of 73 items

- To view log entries within a specific scope, click the drop-down menus to limit the scope, and then click Apply to confirm.

All Classes All Levels All Scopes All Statuses All Time

3.5.4 Exporting Event Logs

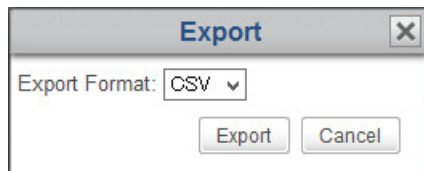
To export event logs of your system, please do the following:

1. On ADM, click **Logs** tab.
2. The Log list appears.

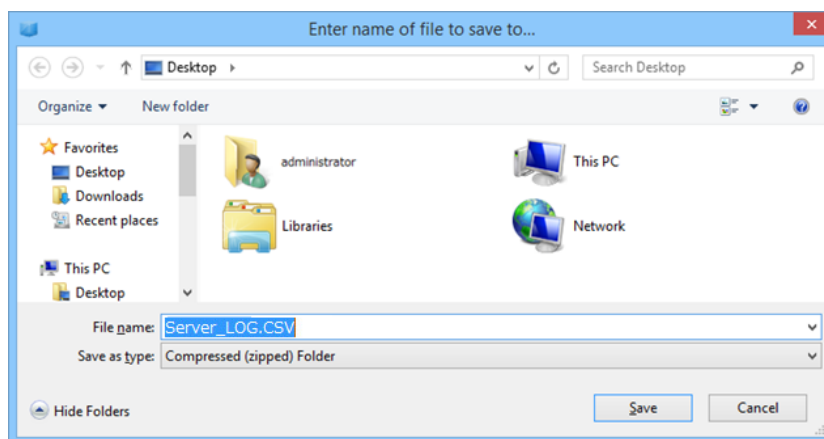
Note

- To export log entries within a specific scope, click the drop-down menus to define the scope, and then click Apply to confirm.
- You can click Reset, and then click Apply to get the complete log entries.

3. Click **Export**.
4. The Export window appears prompting you to select the desired export format.



5. Click the drop-down menu to select the desired format (.CSV or .XML), and then click **Export** to continue.
6. A window appears prompting you to choose the save destination of the exported file. Save the exported file at the desired location.



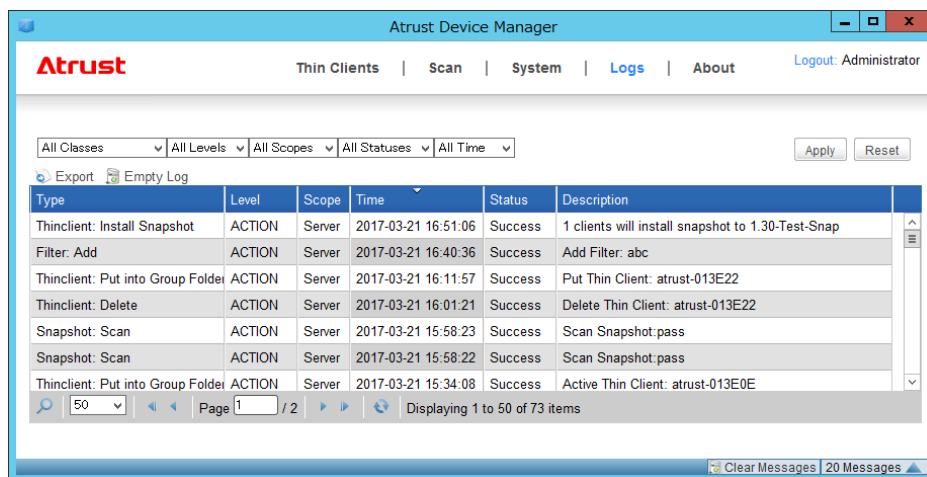
3.5.5 Emptying Event Logs

To empty event logs of your system, please do the following:

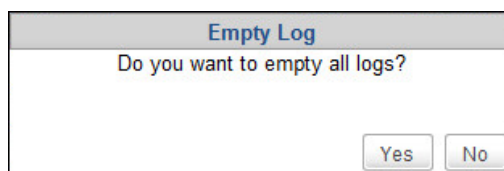
Important Emptying log will delete all log entries. Ensure that you do not need the information in the future before proceeding.

Note You cannot partially delete log entries.

1. On ADM, click **Logs** tab.
2. The Log list appears.

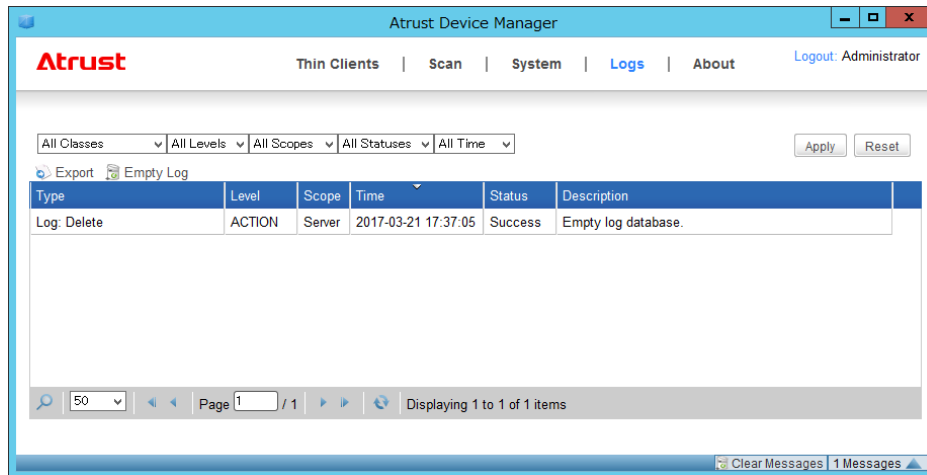


3. Click **Empty Log** on the top of the Log list.
4. The Empty Log window appears prompting for confirmation.



5. Click **Yes** to confirm.

6. All log entries are deleted from ADM.

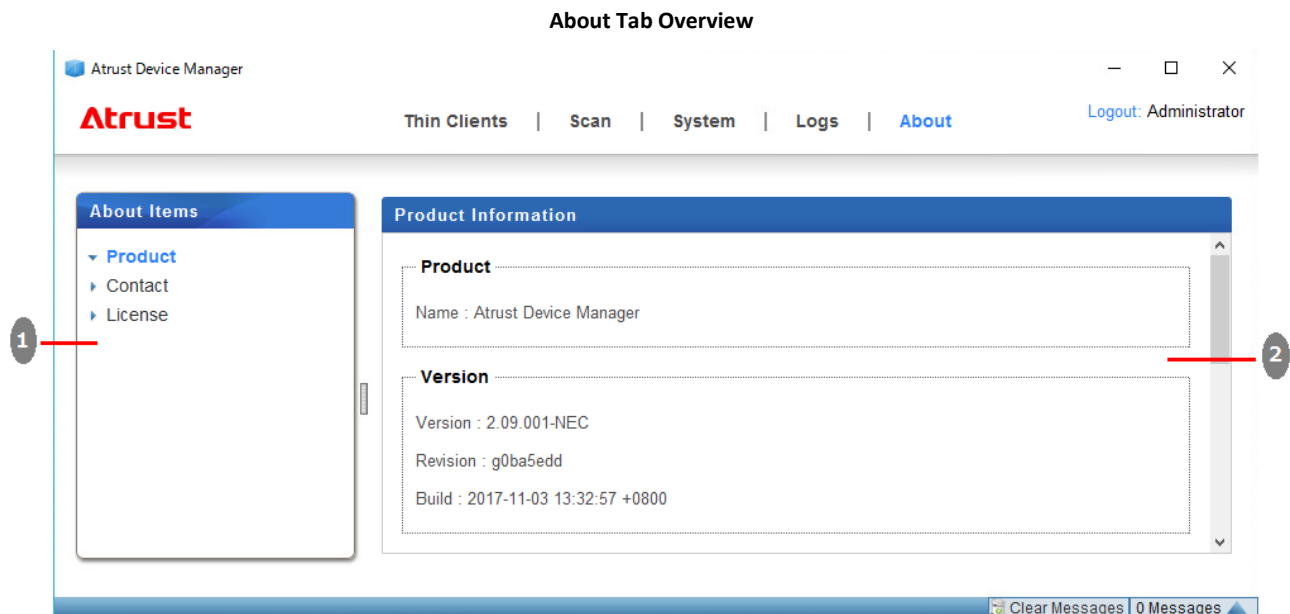


Note A new log entry about emptying log will be added to the Log list.

3.6 Viewing Software Information

3.6.1 About Tab Overview

About tab provides the information about ADM and Atrust Computer Corporation. To access the information of **About** tab, click the tab on ADM.



Interface Elements		
No.	Name	Description
1	Navigation Area	Click to access the desired information.
2	Information Area	Displays the selected item.

3.6.2 Available Tasks at a Glance

No.	Available Task	Section
1	Viewing information on ADM	3.6.3 Viewing Information on ADM
2	Viewing Atrust contact information	3.6.4 Viewing ADM Contact Information
3	Viewing Atrust Software License Agreement	3.6.5 Viewing ADM Software License Agreement

3.6.3 Viewing Information on ADM

To view information on ADM, please do the following:

1. On **About** tab, click **Product** in Navigation area.
2. The version of ADM, the supported client models, and imported firmware versions are shown in Information area.

3.6.4 Viewing ADM Contact Information

To view ADM contract information, please do the following:

1. On **About** tab, click **Contact** in Navigation area.
2. Our website address and contact information are shown in Information area.

3.6.5 Viewing ADM Software License Agreement

To view Software License Agreement, please do the following:

1. On **About** tab, click **License** in Navigation area.
2. Software License Agreement is shown in Information area

Chapter 4 Configuring Client Settings

This chapter provides basic instructions on client configuration.

4.1 Desktop Virtualization and Client Configuration

Endpoint configuration in a desktop virtualization infrastructure

4.2 Client Settings at a Glance

Available client setting items on ADM

4.3 Editing or Adjusting a Group Configuration

How to edit or adjust a group configuration (profile) shared by a group of clients

4.4 Editing or Adjusting an Individual Configuration

How to edit or adjust an individual configuration applied only to a single client

4.5 Using Custom Wallpapers on Clients with ADM

Using Custom Wallpapers on Clients with ADM

4.6 Configuring Client Settings with ACS

How to configure client settings with ACS

4.1 Desktop Virtualization and Client Configuration

The desktop virtualization is available in various forms: user state virtualization, application virtualization, session based virtualization, virtual machine based virtualization, or even a hybrid approach.

NEC thin client can meet a wide range of desktop virtualization forms and needs. To get your client device ready for use in your IT infrastructure, you might need to customize client settings to meet the specific needs in your desktop virtualization plan.

4.2 Client Settings at a Glance

The following table provides brief descriptions of client setting items that can be configured from ADM.










Setting items that can be configured are different on US320f and US310e and US120f.

Note

The available tabs and setting items may vary, depending on: the client model, firmware version, and the used operating system.

4.2.1 US320f











The setting items that can be configured for US320f from ADM are as follows.

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure Remote Desktop connection settings and create connection entries for Remote Desktop on the local desktop.
	Citrix ICA		Click to configure Citrix ICA connection settings and create connection entries for Citrix ICA on the local desktop.
	VMware View		Click to configure VMware View connection settings and create connection entries for VMware View on the local desktop.
	Web Browser		Click to create browser connection sessions on the local desktop. Or click to configure global settings of the browser.
User Interface	Desktop		Click to configure icons displayed on the local desktop.
Devices	USB Storage		Click to configure settings for USB storage devices.
	Audio		Click to configure settings for audio devices.
System	Password		Click to configure settings to require a password when accessing ACS and Shadow settings.
	Appliance Mode		Click to configure Appliance mode settings. If Appliance mode is enabled, the client automatically connects to the specified session upon startup, and automatically shuts down when the user logs off the session.

	UWF		Click to configure Unified Write Filter (hereafter called UWF) settings.
	Advanced		Click to configure detailed settings such as auto registration settings.













4.2.2 US310e










The setting items that can be configured for US310e from ADM are as follows.

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure Remote Desktop connection settings and create connection entries for Remote Desktop on the local desktop.
	Citrix ICA		Click to configure Citrix ICA connection settings and create connection entries for Citrix ICA on the local desktop.
	VMware View		Click to configure VMware View connection settings and create connection entries for VMware View on the local desktop.
	Web Browser		Click to create browser connection sessions on the local desktop. Or click to configure global settings of the browser.
User Interface	Desktop		Click to configure icons displayed on the local desktop.
Devices	USB Storage		Click to configure settings for USB storage devices.
	Audio		Click to configure settings for audio devices.
System	Password		Click to configure settings to require a password when accessing ACS and Shadow settings.
	Appliance Mode		Click to configure Appliance mode settings. If Appliance mode is enabled, the client automatically connects to the specified session upon startup, and automatically shuts down when the user logs off the session.
	UWF		Click to configure Unified Write Filter (hereafter called UWF) settings.

4.2.3 US120f

The setting items that can be configured for US120f from ADM are as follows.

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure Remote Desktop connection settings and create connection entries for Remote Desktop on the local desktop and Start menu.
	Citrix ICA		Click to configure Citrix ICA connection settings and create connection entries for Citrix ICA on the local desktop and Start menu.
	VMware View		Click to configure VMware View connection settings and create connection entries for VMware View on the local desktop and Start menu.
	SSH		Click to configure SSH connection settings and create connection entries for SSH on the local desktop and Start menu.
User Interface	Display		Click to configure display settings.
	Desktop		Click to configure settings for display and system language.
	Keyboard		Click to configure keyboard layout and keyboard settings.
	Mouse		Click to configure mouse settings.
	Screen Saver		Click to configure screen saver settings.
Devices	USB Storage		Click to configure settings for USB storage devices.
	Audio		Click to configure settings for audio devices.
Network	Hosts		Click to create IP address mapping to host server names to create a list of failover clusters.

	Wireless		Click to configure wireless network settings.
	Proxy		Click to configure proxy settings.
System	Timezone		Click to configure time zone and time server settings.
	Password		Click to configure settings to require a password when accessing ACS and Shadow settings.
	Appliance Mode		Click to configure Appliance mode settings. If Appliance mode is enabled, the client automatically connects to the specified session upon startup, and automatically shuts down when the user logs off the session.
	Auto Setup		If Auto Setup mode is enabled, a client can obtain preset settings upon startup and automatically enter an appropriate user environment.
	Quick Connection		Click to configure quick connection mode settings.
	Terminal		Click to configure terminal function settings.
	Advanced		Click to configure detailed settings such as auto registration settings.

4.3 Editing or Adjusting a Group Configuration

On ADM, you can edit client settings for a group of clients through the Edit Configuration window for a profile (group configuration). Through this window, all remotely configurable settings can be edited, then you can push settings to the target group of clients defined in that profile through the Push Settings feature.

Note

- To have a basic understanding of client configuration, please refer to section "3.4.8 Client Settings".
- Please note that, although the Edit Configuration window for a profile (group configuration) looks almost the same as the Edit Configuration window for a client (individual configuration), their functions are different. The latter will only affect some specific client when the configuration is applied. For information on the editing or adjusting of an individual configuration for a client.

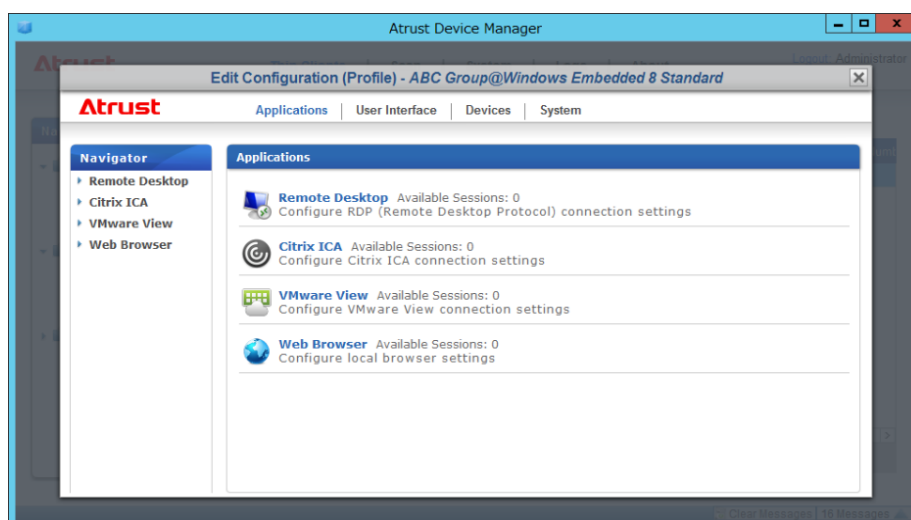
To configure settings in the Configuration (Profile) window (group configuration), please do the following:

1. On **Thin Clients** tab, click **Profiles** to expand the Profile Group tree, and then click the profile group to which the desired profile settings belong.
2. The Profile list appears in Management area.

+ Add - Delete Edit Edit Configuration Move Copy

Name	Platform	Model	Description	Number of Clients
ABC Group	Windows Embedded 8 Standard	US310e	ABC	0

3. Click to select the desired profile setting.
4. Click **Edit Configuration** to display the Configuration (Profile) window.
5. Edit settings on the Configuration (Profile) window.




Note

In this document, the Configuration (Profile) window for US310e is shown as an example. Setting items displayed on the Configuration (Profile) window that can be configured are different on US310e, US320f and US120f.

6. To edit a setting, click the gray icon () near the setting item to enable the item.

Note

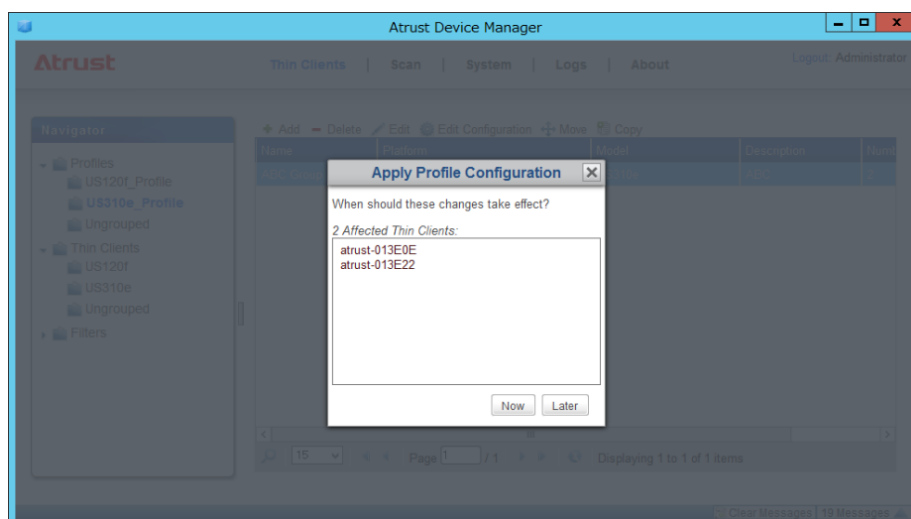
- When an item is enabled, the icon becomes blue ().
- When profile settings are pushed to a client, setting items with a blue icon are locked on ACS of the client and cannot be changed with ACS.

7. After editing settings, click **Save** at the bottom of the Configuration page to save the changes.
8. Repeat steps 6 through 7 to edit all the desired settings.

Note

To push the changes to a client, "Apply Profile Configuration" must be performed for the target group of clients defined in profile settings to push the changes.

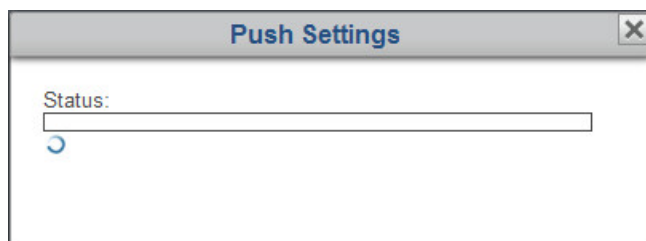
9. After completion, close the Configuration (Profile) window.
10. When the Configuration (Profile) window is closed, the Apply Profile Configuration window appears.

**Note**

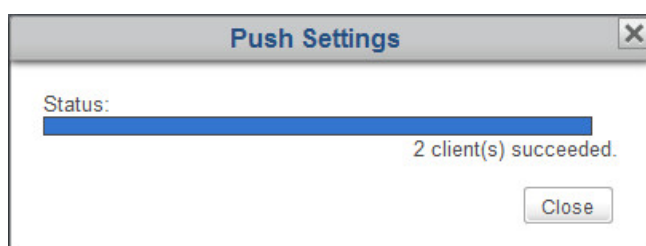
The clients specified as clients to which profile settings are applied are displayed. For information on how to specify clients to which profile settings are applied, please refer to "3.4.9 Creating Setting Profile Groups".

11. Click **Now**.

12. The Push Settings window appears showing the progress and result of pushing profile settings.



13. After completion, click **Close** to exit.



14. Check the status of the client through the Status icon in front of the client to which profile settings are pushed. If needed, reboot the client to complete pushing of profile settings.

Note

- You can check the client status in ADM is Thin Clients tab - Thin Clients - <Client group in which the target client is registered>.
- For details on client status icons, please refer to "3.4.7 Client Status Icons".

4.4 Editing or Adjusting an Individual Configuration

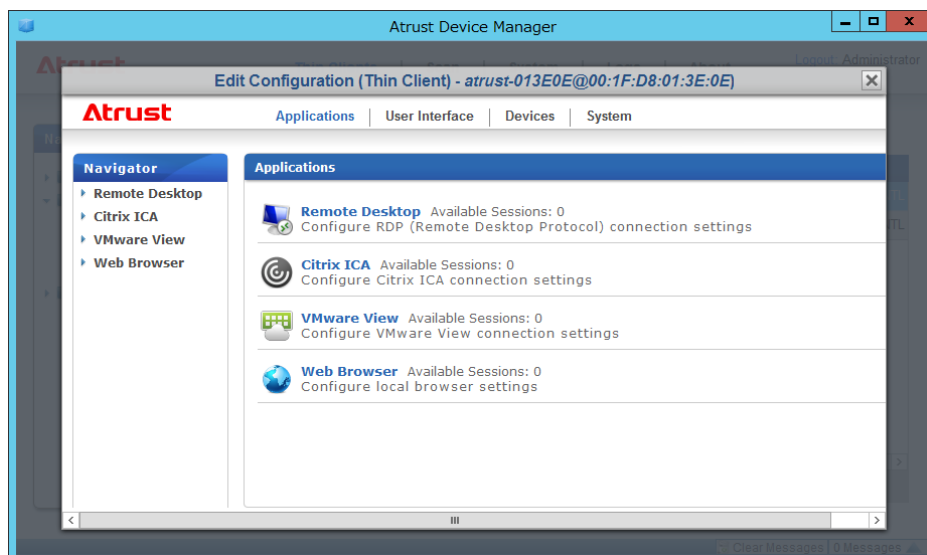
On ADM, you can apply an individual configuration to a client through the Edit Configuration window for that client. Through this window, all remotely configurable settings can be edited, then you can push settings to the client through the Push Settings feature.

Note




- In this section, we will focus on the editing/adjusting of an individual configuration in greater detail. For general instructions on how to create an individual configuration or on how to open the Edit Configuration window for a client, please refer to section "3.4.13 Using Individualized Client Settings".
- The Configuration (Thin Client) window for individual configuration looks almost the same as the Configuration (Profile) window for profile settings. However, note that their functions are different. The Configuration (Thin Client) window for individual configuration pushes settings to the selected client only when settings are applied. In contrast, the Configuration (Profile) window for profile settings pushes settings to all clients defined in profile settings.

To configure settings in the Configuration (Thin Client) window, please do the following:

1. On **Thin Clients** tab, click Thin Clients to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears in Management area.
3. Click to select the desired client.
4. Click **Edit Configuration** to display the Configuration (Thin Client) window.
5. Edit settings on the Configuration (Thin Client) window.



Note

- If the lock icon near a setting item is blue (), the setting value cannot be edited on the Configuration (Thin Client) window because it is configured in profile settings.
- You can lock a setting item by clicking the gray lock icon () near the setting item. When an item is locked, its lock icon becomes orange ().
- When client settings are pushed to a client, setting items with an orange icon are locked on ACS of the client and cannot be changed with ACS.
- In this document, the Configuration (Profile) window for US310e is shown as an example. Setting items displayed on the Configuration (Thin Client) window that can be configured are different on US320f/US310e/US120f.

6. After editing settings, click **Save** at the bottom of the Configuration page to save the changes.

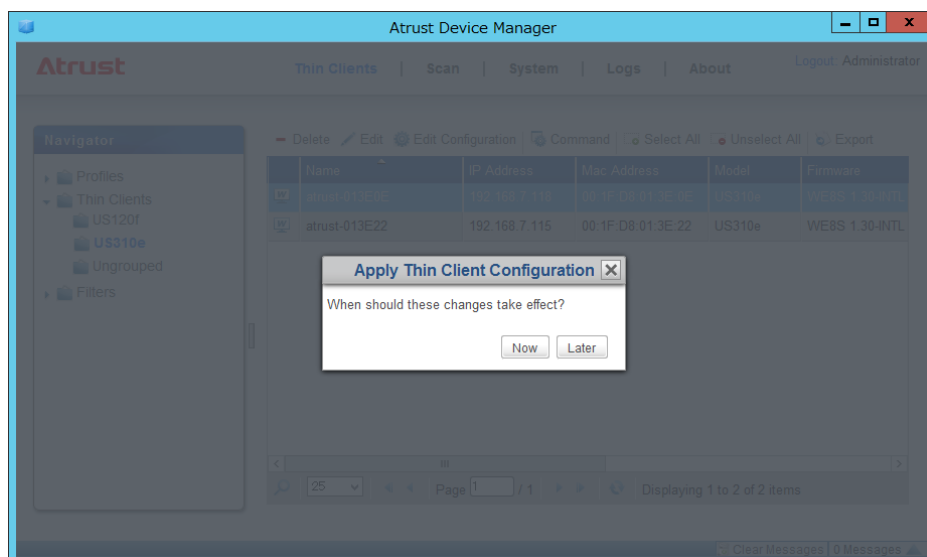
7. Repeat step 6 to edit all the desired settings.

Note

To push the changes to a client, "Apply Thin Client Configuration" must be performed for the client to push the changes.

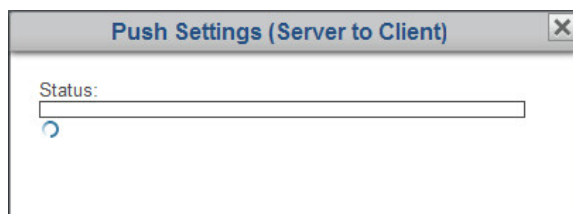
8. After completion, close the Configuration (Thin Client) window.

9. When the Configuration (Thin Client) window is closed, the Apply Thin Client Configuration window appears.

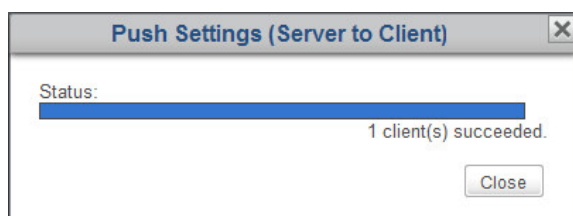


10. Click **Now**.

11. The Push Settings window appears showing the progress and result of pushing client settings.



12. After completion, click **Close** to exit.



13. Check the status of the client through the Status icon in front of it. If needed, reboot the client to complete pushing of client settings.

Note

For details on client status icons, please refer to "3.4.7 Client Status Icons".

4.5 Using Custom Wallpapers on Clients with ADM

ADM allows you to set custom wallpapers on clients.

Important US320f and US310e do not support specification of client custom wallpapers from ADM.

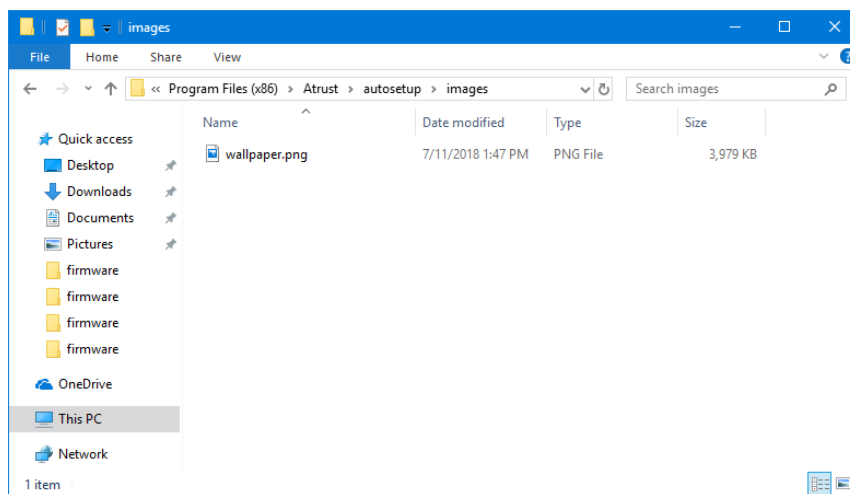
To set a custom wallpaper on a client from ADM, please do the following:

1. On a computer on which ADM is installed, search for the next path.

"C:\Program Files (x86)\Atrust\autosetup\images"

Note The path shown above is for default installation of ADM. If you have changed the path when installing ADM, replace it with an appropriate path.

2. Store the image file you want to use as a wallpaper in the folder in step 1.



Note The supported image file formats are JPG, JPEG, BMP, and PNG. File size is 5 MB or less.

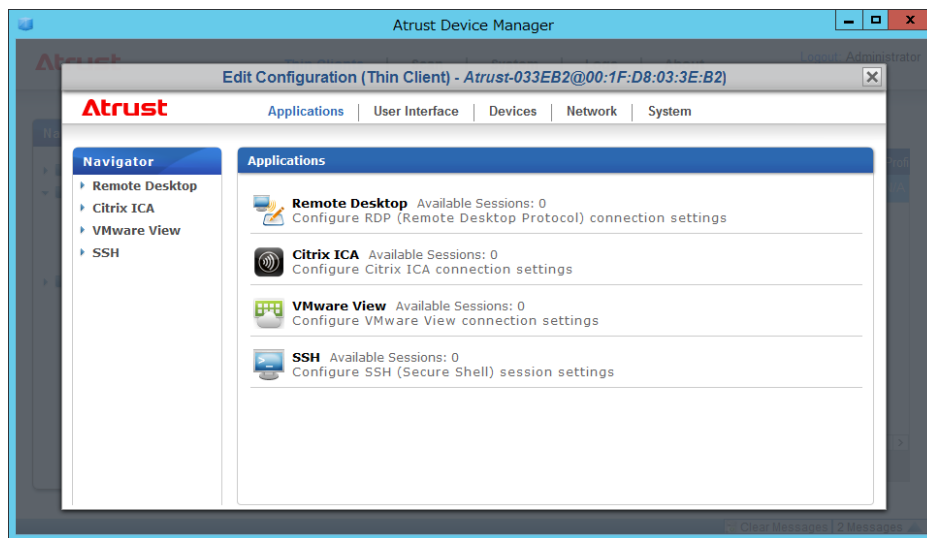
3. On **Thin Clients** tab, click Thin Clients to expand the Client tree, and then click to select the client group to which the desired client belongs.
4. The Client list appears.

<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>						
	Name	IP Address	Mac Address	Model	Firmware	Profi
	Atrust-033EB2	192.168.7.111	00:1F:D8:03:3E:B2	US120f	ARM Linux 8.43-FAKC	N/A

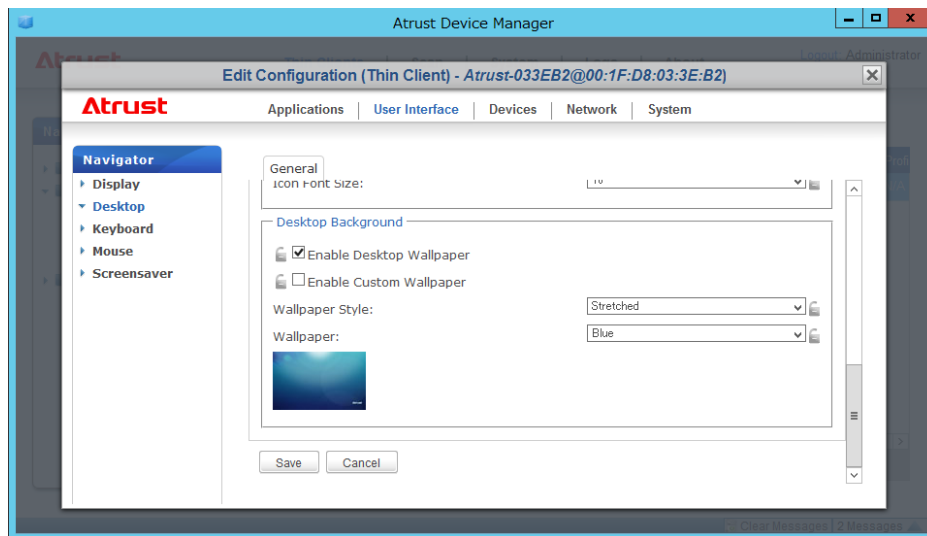
- Click to select the desired clients, and then click **Edit Configuration** on the top of the Client list.

Note To select more than one client, Ctrl-click to select multiple clients.

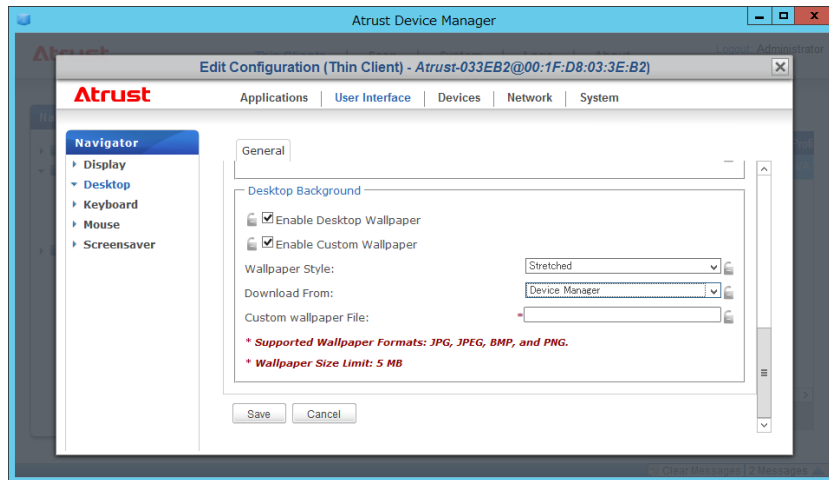
- The Configuration (Thin Client) window appears.



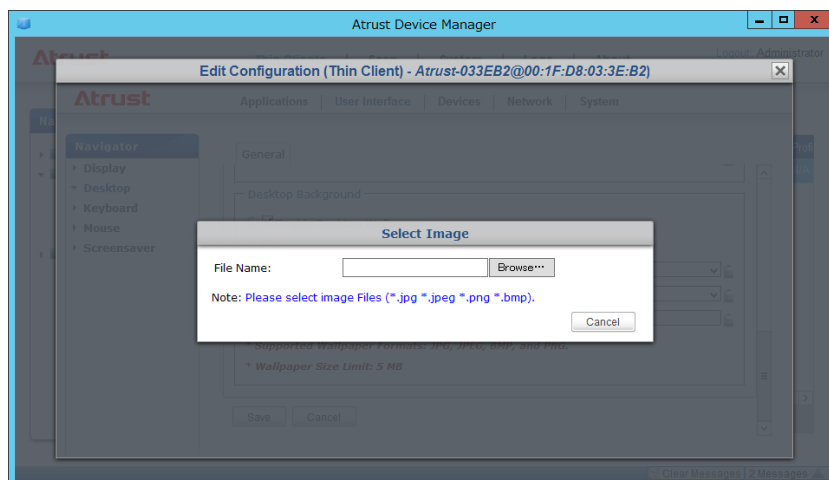
- Click to select **User Interface > Desktop**. Scroll down to show the **Desktop Background** section.



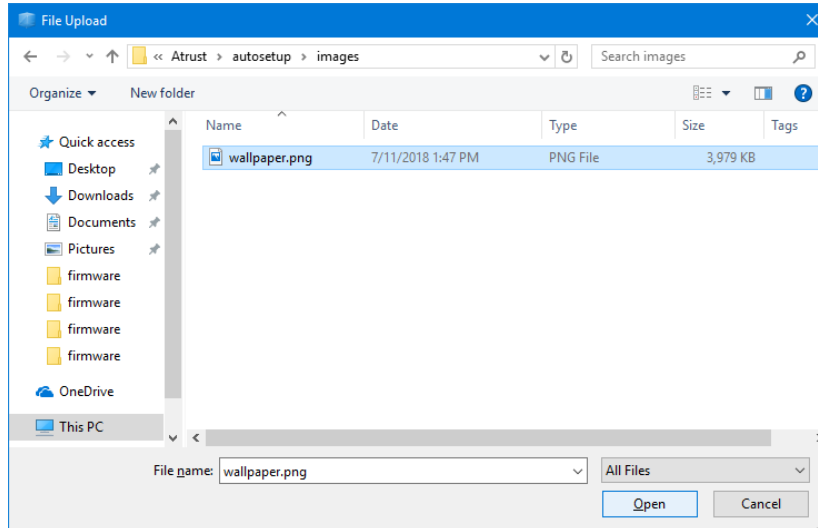
8. Select **Enable Custom Wallpaper**, and select **Device Manager** in Download From.



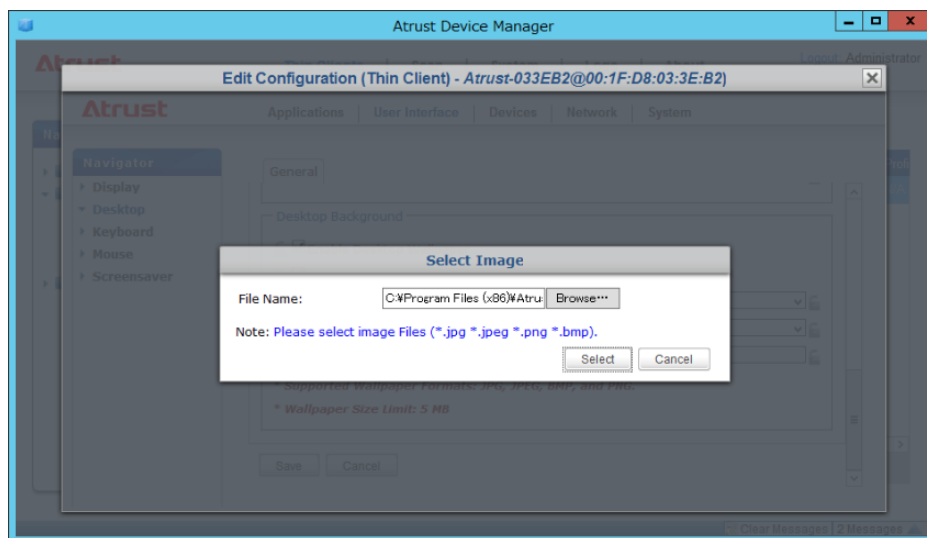
9. Click the Custom wallpaper File field to display the Select Image window.



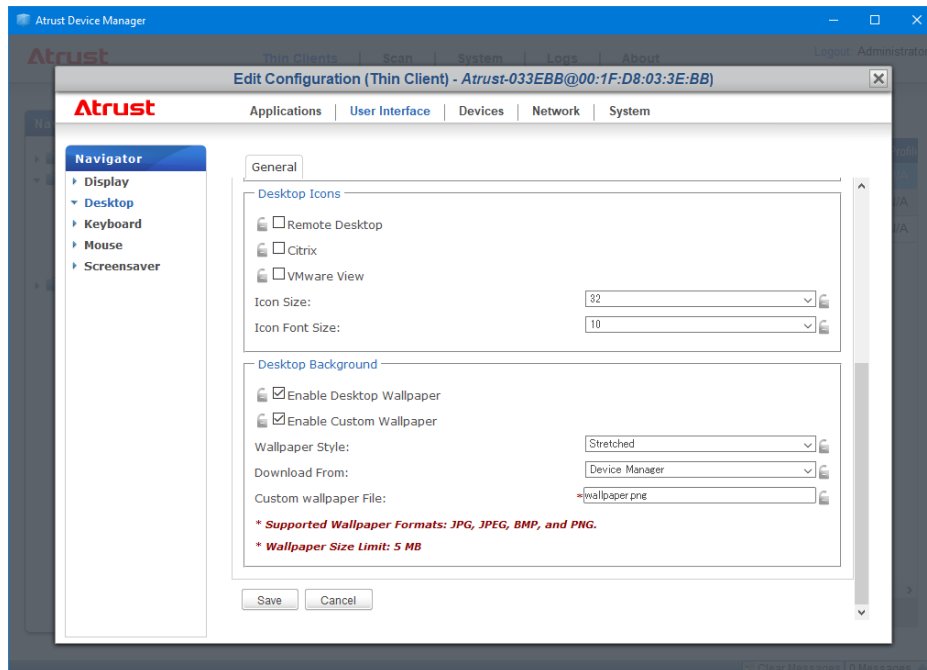
10. Click **Browse**, select the image file prepared in step 2, and then click Open.



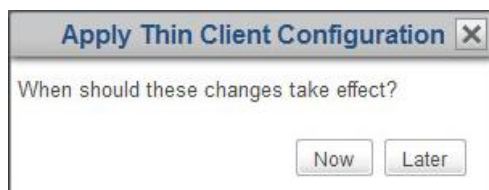
11. Click **Select**.



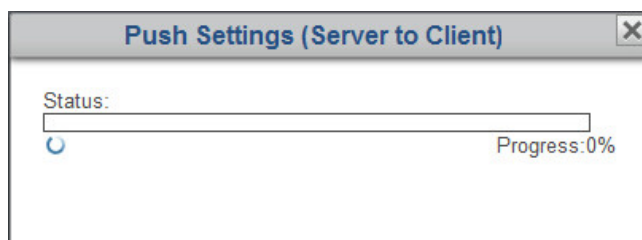
12. Check that the file name of the selected image file is reflected in the field.



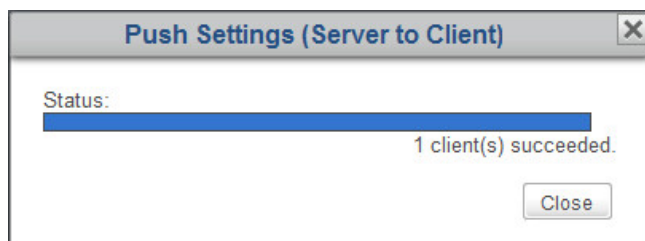
13. Click **Save**.
14. Close the Configuration (Thin Client) window.
15. When the Configuration (Thin Client) window is closed, the Apply Thin Client Configuration window appears.



16. Click **Now**.
17. The Push Settings window appears showing the progress and result of pushing client settings.



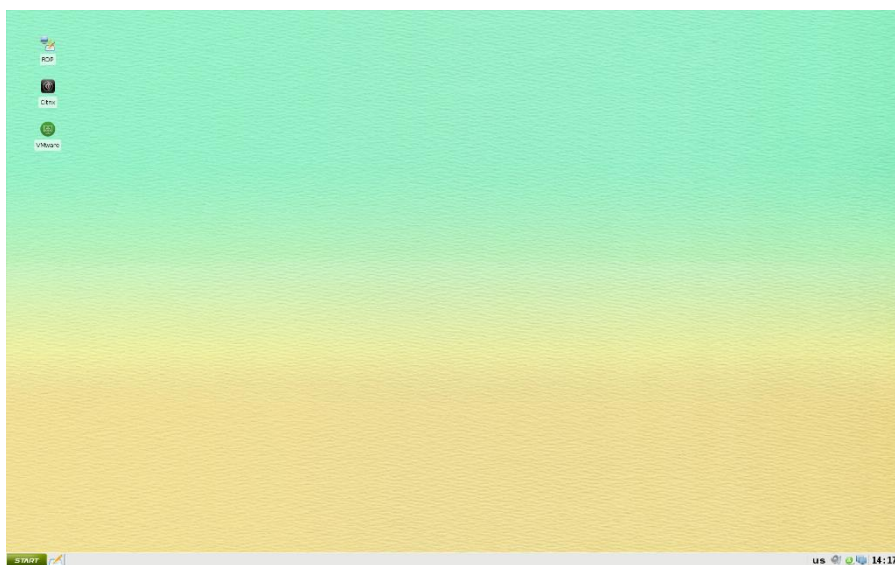
18. After completion, click **Close** to exit.



19. Check the status of the client through the Status icon in front of it. If needed, reboot the client to complete pushing of client settings.

Note For details on client status icons, please refer to "3.4.7 Client Status Icons".

20. Check that the wallpaper has been reflected on the client.



4.6 Configuring Client Settings with ACS

ACS allows you to configure client settings on a local client. Some settings can only be configured with ACS on a local client.

For details on how to configure client settings on a local client by using ACS, please refer to the user's guide of your thin client.

5

Chapter 5 Advanced Uses of ADM

This chapter describes advanced uses of ADM.

5.1 Using ADM as an Auto Setup File Server

Using ADM as an Auto Setup File Server

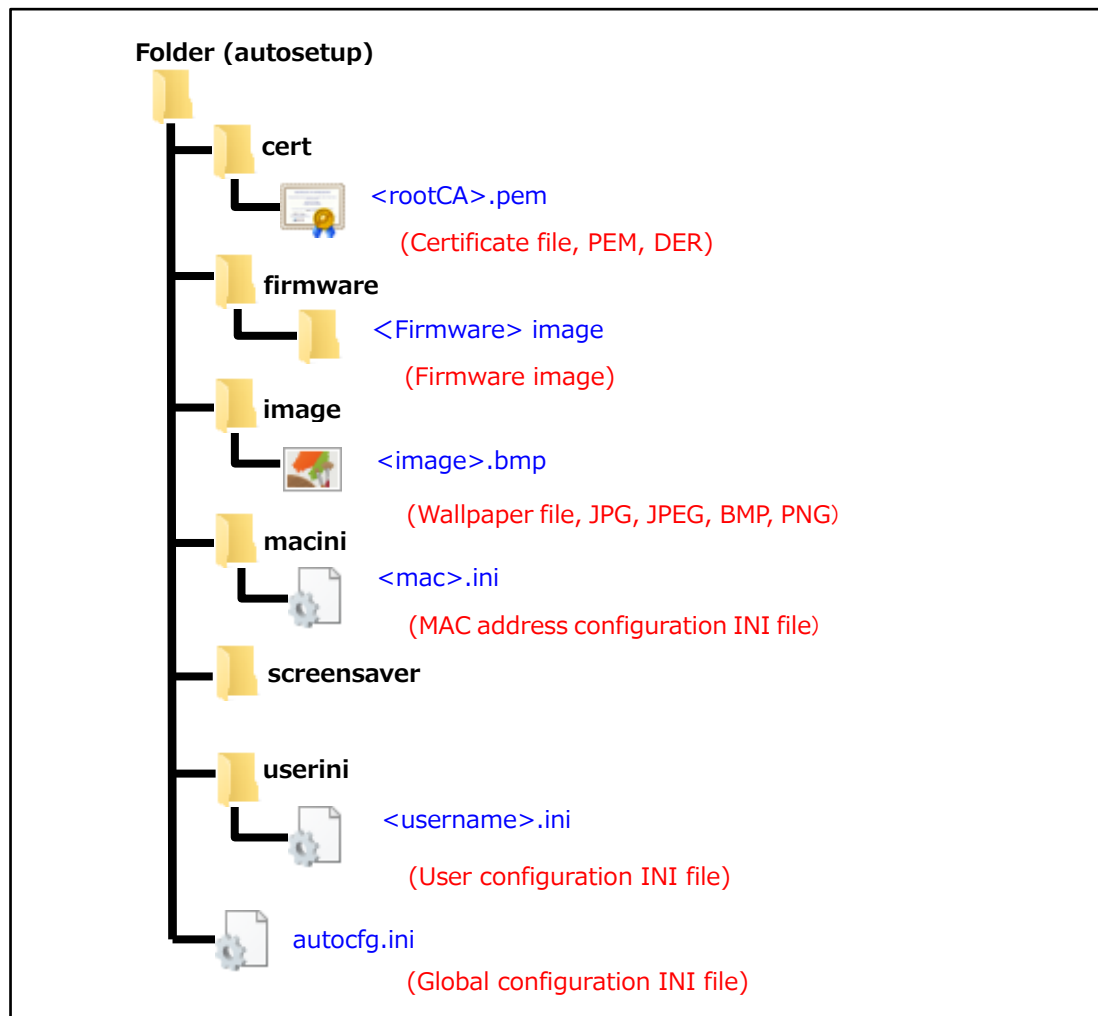
5.1 Using ADM as an Auto Setup File Server

You can use ADM as an auto setup file server.

Important

Auto setup is supported by US120f. This function is not available on US320f and US310e. For details on auto setup, please refer to "3.2 Auto Setup" in the US120f User's Guide.

To use ADM as an auto setup file server, configuration INI files must be stored in the autosetup folder in advance. The following is a configuration example of the autosetup folder.



Note

The autosetup folder and its subfolders are created automatically when ADM is installed. By default, the location of the folder is "C:\Program Files (x86)\Atrust\autosetup\". If you have changed the path when installing ADM, replace it with an appropriate path.

Important To use auto setup, autocfg.ini (global configuration INI file) is essential.

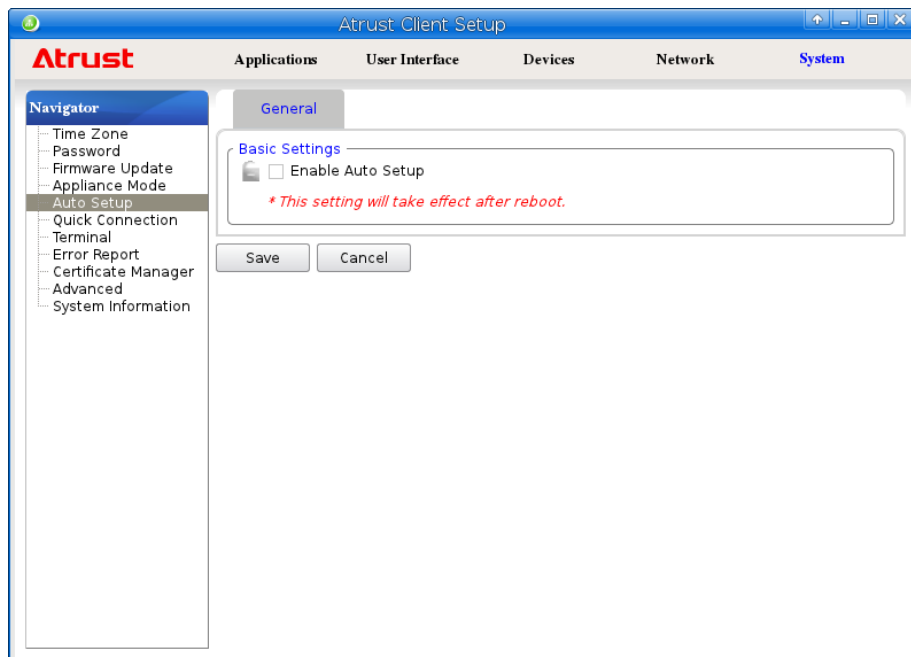
To use ADM as an auto setup file server, please do the following:

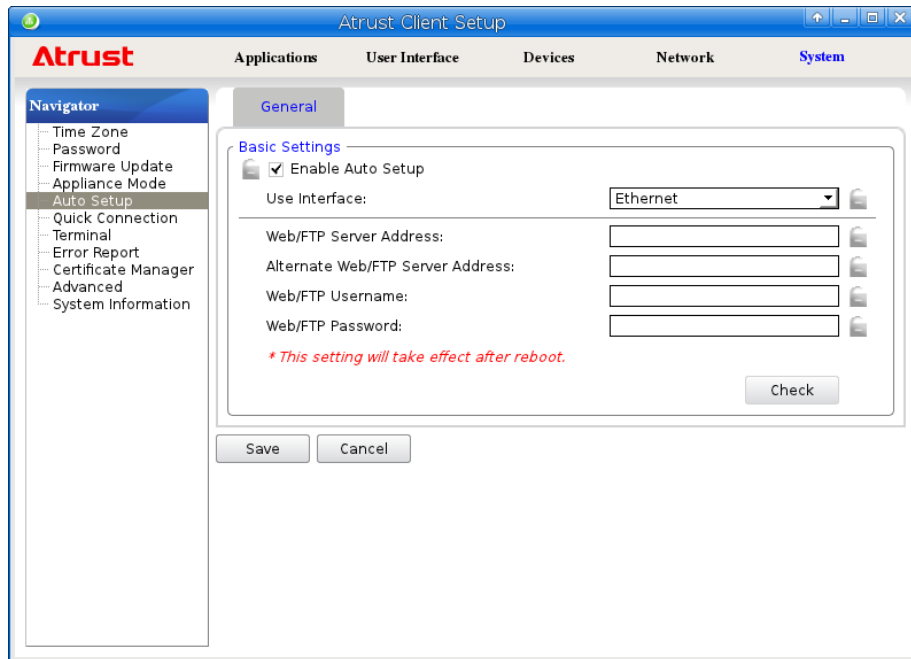
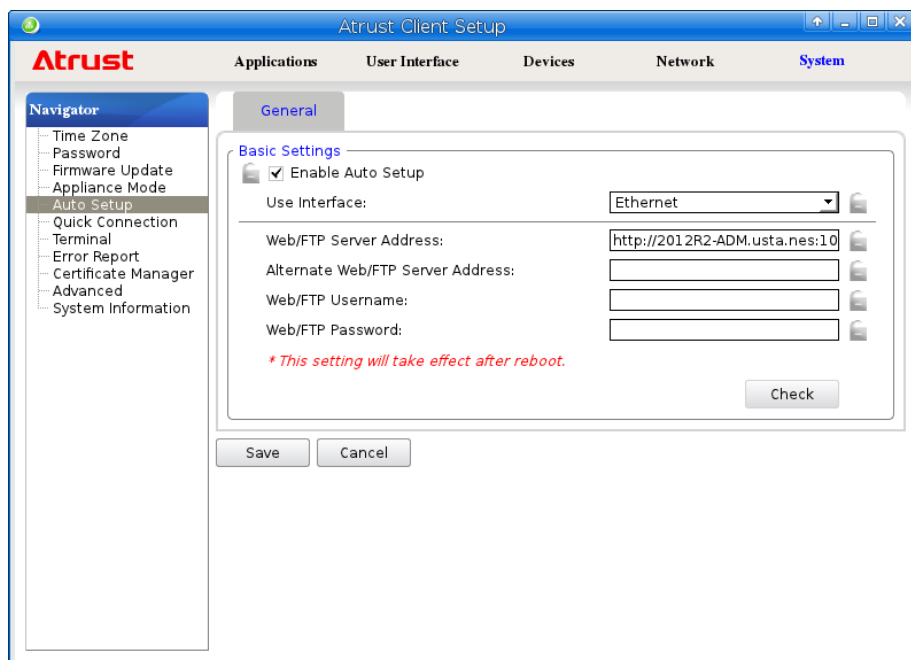
Important Do not use auto setup and pushing of client settings from ADM simultaneously. If client settings from ADM are applied to US120f using auto setup, the settings of auto setup have precedence.

1. Sign in to the ADM server with the Administrator account.
2. Store the files required for auto setup under the autosetup folder.
3. After storing the required files in step 2, start ACS of US120f.

Note You can also configure the settings in steps 3 through 9 by editing the group settings and individual settings of ADM and pushing them to the client. For information on how to edit group configuration, please refer to "4.3 Editing or Adjusting a Group Configuration". For information on how to edit individual configuration, please refer to "4.4 Editing or Adjusting an Individual Configuration".

4. Click to select **System > Auto Setup**.

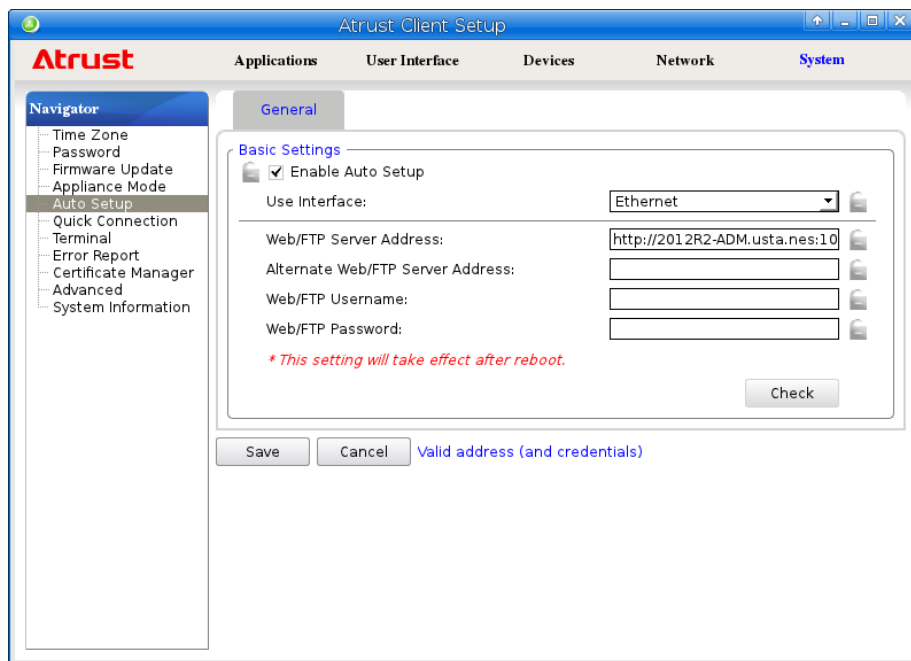


5. Select **Enable auto setup**.6. Click to select **Use Interface**, and type in the server address of ADM in **Web/FTP Server Address**.

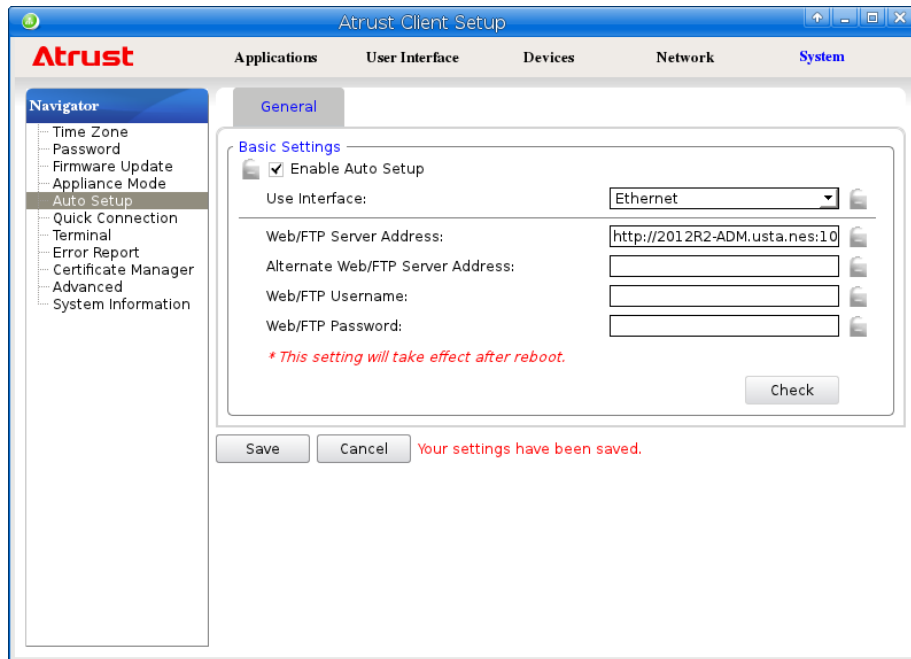
Note

- The format for entering the server address of ADM is "http://<Server FQDN>:10080/autosetup>".
- To use ADM as a file server, leave "Web/FTP User Name" and "Web/FTP Password" blank.

7. Click **Check** to see the values you entered are OK.



8. Click **Save**.



9. Exit ACS, and then reboot US120f.
10. After completion, US120f refers to ADM as an auto setup file server.



Chapter 6 Notes and Restrictions

This chapter describes notes and restrictions on using ADM.

6.1 Synchronizing ADM with ACS Settings

Notes on synchronizing the settings of ADM with those of ACS

6.2 Adding to and Releasing from Management

Notes on adding clients to and releasing them from the management of ADM

6.3 Notes on Taking and Installing Snapshots

Notes on the behavior of Default User Account at Snapshot Installation

6.4 Notes on Updating Firmware and Installing Snapshots

Notes on updating firmware and installing snapshots

6.5 Notes on Accessing the ADM Management Console

Notes on accessing web-based ADM Management Console

6.6 Notes on Using VNC (Remote Shadow)

Notes on using VNC (Remote Shadow)

6.7 Notes on Backup and Restoring ADM Server

Notes on Backup and Restoring ADM Server

6.8 Restrictions

Restrictions on using ADM and known issues

6.1 Synchronizing ADM with ACS Settings

If the administrator changes ACS settings on a thin client without doing so as a remote operation from ADM, the settings of ACS will not be identical to those of ADM. ADM does not update the settings automatically when it communicates with ACS. The administrator needs to synchronize the settings by performing **Pull Settings (from Client to Server)** from ADM Management Console to the thin client where the changes were made.

6.2 Adding to and Releasing from Management

In the case of US310e, when ACS is registered in an ADM Server, the managed status is enabled, and any other ADM Servers become unable to manage the ACS. This specification is intended to prevent access from the malicious ADM servers. When using US320f and US120f, ADM add the terminal which is already registered in another ADM server, and become able to manage the ACS. When these device is registered with another ADM, The client can't be controlled from the ADM server registered prior. To restrict register thin client operation from another ADM, enable **Enable Password Protection**. Please refer to "3.2.12 Configuring Password Protection for Managed Devices" for detail.

When thin client isn't registered as a management target of the ADM server, or thin client unregistered as a management target of the ADM isn't effective stealth mode, it is detected by a malice server, and settings may be changed. Therefore, please be sure to make the thin client running in the production environment to the state registered as a management target of the ADM server. When you do not use an ADM server, thin client makes the stealth mode effective.

For details on stealth mode, please refer to "2.10 Enabling / Disabling Automatic Registration and Stealth Mode" in the US320f User's Guide or "2.1.10 advanced" in the US120f Use's Guide. Stealth Mode in US120f is supported in 8.51-CAKD or later version. To release the managed status, remove the thin client from the ADM server or reset the thin client by selecting **Reset Mode**. Please refer to the User's Guide of the thin client for **Reset Mode**.

To cancel management registration, "remove" the thin client from the ADM server to which it is registered, or execute Reset Mode on the thin client. For details on Reset Mode, refer to the user's guide of the thin client. In US120f, you can also cancel the management registration of ADM without initializing ACS settings by executing Disconnect from ADM. For details on Disconnect from ADM, refer to the user's guide of US120f.

Important

- If thin client that ACS configuration is set in kitting environment is migrated from kitting environment to production environment, it is necessary to be careful. In this case, you need to remove this thin client information from the kitting environment ADM server. If this operation is not performed, production environment ADM server cannot register this thin client. Reset Mode remove ACS configuration not only ACS managed status. Please be careful.
- The production environment ADM server executes "Pull Settings" after detecting thin client. As a result, the thin client ACS settings are synchronized to the ADM server. Thin client ACS settings are overwritten on the settings of the ADM server side when you execute the "Pull Settings". Please be careful.
- If US320f or US120f is used, you can register it on the production ADM server without removing client registration from the ADM server in the kitting environment by using the method described in "Discovering Clients Including Password-Protected Devices".

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 isn't updated. Administrators need to remove the thin client at ADM side.

6.3 Notes on Taking and Installing Snapshots

You can use a snapshot to capture a customized OS image that you can re-use in your organization. Notes on taking and installing snapshots are described below.

Important

- Taking snapshots and installing ones cannot be used for a wireless LAN client.
- Taking snapshots and installing ones are not available on US120f.

6.3.1 Types of Snapshots

When a snapshot is installed, the System Preparation Utility (Sysprep) executes. The System Preparation Utility initializes terminal-specific information such as the SID, making it possible to install that information in multiple terminals as a master image.

Important

In ADM2.08.045 or later, "Backup" has been deleted from types of snapshots.

6.3.2 Behavior of Default User Account at Snapshot Installation

When a snapshot is installed, the Administrator account is re-created. Accordingly the Administrator profile (desktop items such as files, shortcuts, and folders, as well as My Documents, Favorites, etc.) is initialized. Therefore, after installing a snapshot, the Administrator's profile settings from before a snapshot is taken are not reflected.

The profile of the User account is retained the settings of before the snapshot is taken but there are some exceptions. Input language, display language, format, location, user locale, region and language settings such as the system locale are not retained. These settings are initialized. If you want to retain these settings after snapshot installation, you need to use Unattend Files (C:\Windows\Panther\unattend.xml). Unattend.xml is the response file for the Windows setup. It is possible to configure the default settings of Windows.

The following are the steps to keep the changes of regional and language settings and time zone.

1. Sign in with the Administrator account, and disable the UWF.
2. Sign in with the User account.
3. Set regional and language settings and time zone. If you need to set the display language, please install the language pack (the Internet environment is required). Depending on the settings, you will have to sign out or restart. Please make sure that all settings are reflected properly after setting completion.
4. Sign in with the Administrator account.
5. Open the response file (C:\Windows\Panther\unattend.xml) in Notepad, and edit the value of the following elements. The following value is the default value of English OS. Specifies the time zone (For example, Eastern Standard Time, Romance Standard Time) and language code you want to use. Language is ISO-639 language code, and Area is ISO 3166-1 country or region identifier. (For example, en-US, fr-FR or es-ES)

```
<TimeZone>GMT Standard Time</TimeZone>
```

```
<InputLocale>en-US</InputLocale>
```

```
<SystemLocale>en-US</SystemLocale>
```

```
<UILanguage>en-US</UILanguage>
```

```
<UILanguageFallback>en-US</UILanguageFallback>
```

```
<UserLocale>en-US</UserLocale>
```

6. Enable the UWF and take snapshot.

6.3.3 About Joining a Domain

A snapshot cannot be taken for a thin client that is joined to a domain. The snapshot feature uses the System Preparation (Sysprep) tool for imaging. Sysprep will remove all system-specific information such as the security identifier (SID) of computer from the installed Windows image. Sysprep is executed only in case of a member of workgroup and is not executed in case of a member of a domain. If the thin client is joined to a domain, please take a snapshot after you removed the thin client from the domain.

Important US120f cannot be added to a domain environment.

6.4 Notes on Updating Firmware and Installing Snapshots

This section describes notes on updating firmware and installing snapshots

6.4.1 Maintenance of ACS Settings

When the firmware is updated or a snapshot is installed, ACS settings are retained as described below.

ACS settings after updating firmware

The ACS settings of the thin client on which the firmware is distributed are retained.

ACS settings after installing a snapshot (US320f and US310e)

The ACS settings of the thin client from which the snapshot is taken are retained.

6.4.2 Canceling Activation (License Authentication) (US320f and US310e)

Thin client has been activated at the factory. But if, by using 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 the User's Guide for more details about activation.

Important US120f does not require activation.

6.5 Notes on Accessing the ADM Management Console

ADM is a web-based application running on Apache HTTP Server. Use prism to access the site. prism allows you to use web applications as if they were local applications. In addition, prism eliminates the risk of crashing or restarting that might occur when using a browser. You can easily launch ADM through the prism shortcut (ADM shortcut) created on your desktop.

Since the ADM site is configured using HTTPS, if the site is accessed from a web browser, you can access the top page (login screen), but you cannot log in due to access restrictions. Please note that the ADM Management Console cannot be accessed from a web browser.

6.6 Notes on Using VNC (Remote Shadow)

VNC (remote shadow) is useful, but it requires attention to security. If the remote shadow feature is enabled, anyone who knows the password can connect to US320f/US120f/US310e from other VNC client software as well as from ADM. It is therefore important to implement security measures (such as using us310e only within the firewall or disabling VNC when it is not being used) when using this feature.

6.7 Notes on Backup and Restoring ADM Server

A notice about a backup and restoration of the ADM server is indicated here.

6.7.1 Database and Firmware and Package Backup

When you must install ADM server newly because ADM server broke down by some kind of troubles, the following backup files are necessary to restore ADM server.

- Database backup archive file
- firmware file
- snapshot file
- package file

Before importing firmware file and package file to ADM server, please save the file to another computer. Please regularly save for database backup archive file, too. Please also export snapshot from the ADM server and save it to another computer.

Please refer to following sections.

- 3.2.6 Managing Client Snapshots
- 3.2.15 Backing Up the Management Database
- 3.2.16 Managing Database Archive Files

6.7.2 Restoration of ADM Server

It is possible to import the Database backup archive file and firmware file to the new ADM server in order to restore. New ADM Server's IP address and computer name does not have to be same.

Please refer to following sections.

- 3.2.4 Managing Thin Client Firmware Files
- 3.2.5 Managing WES Package Files
- 3.2.6 Managing Client Snapshots
- 3.2.17 Restoring a Database Archive File

6.8 Restrictions

This section describes various restrictions.

6.8.1 Restrictions on ADM

1. When configuring the external management database in the ADM database source settings, you are not allowed to locate the database in an existing ADM server. An operation in which multiple ADM servers reference a single database is not permitted.
2. When specifying Use External Server in Deploy Server for ADM, the URL cannot be an https (SSL) URL.
3. Firmware and packages cannot be registered to a shared folder on the network.
4. When exporting a snapshot of US320f and US310e, make sure that you have at least 20 GB of free space on your disk. This space is required to compress and copy the snapshot image file and ensure stable system operation.
5. Updating firmware to US320f and US310e or installing snapshots from ADM configured on a VMware ESXi virtual machine may cause delay in the network, leading to an image file download failure. In this case, setting flow control of virtual NIC of VMware ESXi to disable may improve the delay. For details on how to set flow control of virtual NIC of VMware ESXi to disable, refer to the following knowledge base: Configuring flow control on VMware ESXi and VMware ESX. (<http://kb.vmware.com/kb/2079125>)
6. When the database of ADM is archived and restored on another ADM, the "Pull Settings" and "Push Settings" features do not operate normally
7. When deleting a client group, the following message appears even if no client is registered in the group.
[Message]
'<Client Group Name>' contains items.
Please select whether to move all items to Ungrouped or delete all of them.
8. When deleting a profile group, the following message appears even if no client is registered in the group.
[Message]
'< Profile Group Name >' contains items.
Please select whether to move all items to Ungrouped or delete all of them.
9. After profile settings including settings requiring a reboot are pushed to a client and the client reboots, the client status icon may remain Reboot needed (🔄). It may take some time until the client status icon is updated.
10. Make sure that ADM build only one in the identical segment. When more than one ADM is built in the identical segment, there is a possibility that unexpected error may occur in ADM.

6.8.2 Restrictions on US320f

1. If image delivery is canceled due to disconnection from the power supply or the network while firmware is being upgraded through ADM or while snapshots are being installed, the operation system cannot be launched. In this case, press Esc while starting up the thin client to launch NEC Thin Client Menu. Select Firmware Update from the menu and locate the file server (ADM) IP address from thin client to recover the firmware. Additionally, you can also recover the device image by using Atrust Recovery USB Disk Creator. For details, refer to each guide.

Note Specify the IP address of the ADM server as the default server path of ADM.

2. When creating a Citrix ICA connection shortcut in ADM or ACS, specifying the SSL/TLS+HTTPS server location for Connection Settings > Network Protocol will cause an error when connecting to a Citrix ICA session.
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 Atrust Client Setup, "RC5 128 bit (login only)", "RC5 40 bit", "RC5 56 bit", and "RC5 128 bit" keys can be used for encryption by specifying an option on Add / Edit Citrix ICA Session. However, if you use XenDesktop 7 or later and use encrypted connection, use only "RC5 128 bit" key. Do not use "RC5 128 bit (login only)", "RC5 40 bit", or "RC5 56 bit" key.
4. If other than Default is specified for Window Size in the option settings for adding/editing a Citrix ICA session of ADM and ACS, the DesktopViewer toolbar is not displayed in the Citrix ICA session. To display the DesktopViewer toolbar, specify Default for Window Size, or connect to the Citrix ICA session by using Citrix Receiver.

6.8.3 Restrictions on US310e

1. If image delivery is canceled due to disconnection from the power supply or the network while firmware is being upgraded through ADM or while snapshots are being installed, the operation system cannot be launched. In this case, press Esc while starting up the thin client to launch NEC Thin Client Menu. Select Firmware Update from the menu and locate the file server (ADM) IP address from thin client to recover the firmware. Additionally, you can also recover the device image by using Atrust Recovery USB Disk Creator. For details, refer to each guide.

Note Specify the IP address of the ADM server as the default server path of ADM.

2. When creating a Citrix ICA connection shortcut in ADM or ACS, specifying the SSL/TLS+HTTPS server location for Connection Settings > Network Protocol will cause an error when connecting to a Citrix ICA session.
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 Atrust Client Setup, "RC5 128 bit (login only)", "RC5 40 bit", "RC5 56 bit", and "RC5 128 bit" keys can be used for encryption by specifying an option on Add / Edit Citrix ICA Session. However, if you use XenDesktop 7 or later and use encrypted connection, use only "RC5 128 bit" key. Do not use "RC5 128 bit (login only)", "RC5 40 bit", or "RC5 56 bit" key.
4. If other than Default is specified for Window Size in the option settings for adding/editing a Citrix ICA session of ADM and ACS, the DesktopViewer toolbar is not displayed in the Citrix ICA session. To display the DesktopViewer toolbar, specify Default for Window Size, or connect to the Citrix ICA session by using Citrix Receiver.

6.8.4 Restrictions on US120f

1. If image delivery is canceled due to disconnection from the power supply or the network while firmware is being upgraded through ADM or while snapshots are being installed, the operation system cannot be launched. In this case, press Esc while starting up the thin client to launch NEC Thin Client Menu. Select Firmware Update from the menu and locate the file server (ADM) IP address from thin client to recover the firmware. Additionally, you can also recover the device image. For details, refer to the user's guide of US120f.

**Atrust Device Manager 2.09.001
User's Guide**

Third edition, September 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.