

Atrust Device Manager 2.08.041 User's Guide

Contents

Chapter 1 Overview.....	3
1.1 Introduction	4
1.2 New Features	5
1.3 Features	6
1.4 System Requirements	7
1.4.1 Supported Endpoint Devices	7
1.4.2 Supported Platforms.....	7
1.4.3 Hardware Requirements.....	7
1.4.4 Software Requirements.....	7
1.4.5 Background Service and Used Ports of Atrust Device Manager	8
1.4.6 Configuring the network environment	9
Chapter 2 Installing and Upgrading Atrust Device Manager	11
2.1 Installing Atrust Device Manager	12
2.2 Installing Java Software	17
2.3 Initial Setup	18
2.4 Upgrading Atrust Device Manager	20
2.5 Uninstalling Atrust Device Manager.....	21
Chapter 3 Using Atrust Device Manager	22
3.1 Atrust Device Manager	23
3.1.1 Interface Overview	23
3.1.2 Available Tasks at a Glance	24
3.2 Establishing a Basic Administration Environment	25
3.2.1 System Tab Overview.....	25
3.2.2 Available Tasks at a Glance	26
3.2.3 Managing Accounts for Administration	27
3.2.4 Managing Thin Client Firmware Files.....	29
3.2.5 Managing Zero Client Image Files.....	32
3.2.6 Managing WES Package Files.....	33
3.2.7 Managing Client Snapshots	36
3.2.8 Managing Certificates of Remote Computers.....	39
3.2.9 Configuring Remote Deployment Settings.....	39
3.2.10 Selecting the Service IP of Atrust Device Manager	41
3.2.11 Configuring Auto-Logout for Atrust Device Manager	42
3.2.12 Configuring the Database Source of Atrust Device Manager.....	43
3.2.13 Selecting the Interface Language of Atrust Device Manager.....	44
3.2.14 Backing Up the Management Database	44
3.2.15 Managing Database Archive Files	45
3.2.16 Restoring a Database Archive File.....	46
3.2.17 Managing P2T License Files	46
3.2.18 Scheduling Automatically Performed Tasks	47
3.3 Adding Clients into a Managed Group	50
3.3.1 Scan Tab Overview.....	50
3.3.2 Available Tasks at a Glance	50
3.3.3 Client Detection and Management.....	51
3.3.4 Discovering Clients in the Whole Range of a Local Network	52
3.3.5 Discovering Clients in a Specified Range of IP Addresses	53
3.3.6 Creating and Managing an IP Range List.....	54
3.3.7 Discovering Clients using a Predefined IP Range List.....	55
3.4 Managing All Your Clients	57
3.4.1 Thin Clients Tab Overview	57
3.4.2 Available Tasks at a Glance	58
3.4.3 Getting Your Zero Client Ready for Use	59
3.4.4 Creating Client Groups.....	60
3.4.5 Managing Client Groups	61
3.4.6 Moving Clients to Another Group.....	62
3.4.7 Deleting Clients from a Group	63
3.4.8 Understanding Client Status Icons	64

3.4.9 Client Settings.....	65
3.4.10 Creating Setting Profile Groups	67
3.4.11 Managing Setting Profile Groups.....	68
3.4.12 Creating Client Setting Profiles	69
3.4.13 Managing Client Setting Profiles.....	72
3.4.14 Using Individualized Client Settings	75
3.4.15 Using Hybrid Client Settings	77
3.4.16 Pushing Settings to Clients through Your Local Network	79
3.4.17 Pulling Client Settings through Your Local Network.....	83
3.4.18 Pushing Certificates of Remote Computers to Clients	86
3.4.19 Sending Messages to Clients	87
3.4.20 Editing or Viewing the Basic Information about a Client	88
3.4.21 Rebooting Clients through Your Local Network	89
3.4.22 Shutting Down Clients through Your Local Network.....	92
3.4.23 Waking Clients through Your Local Network.....	95
3.4.24 Updating Client Firmware.....	98
3.4.25 Installing Software Packages.....	100
3.4.26 Taking Client Snapshots	102
3.4.27 Restoring Client Snapshots	103
3.4.28 Assisting a Client User Remotely	104
3.4.29 Exporting Client Data.....	106
3.4.30 Digging Out Profiles, Clients, or Event Logs with Quick Search.....	107
3.4.31 Digging Out Clients with Filters.....	108
3.4.32 Managing Your Filters	110
3.5 Viewing and Managing Event Logs.....	111
3.5.1 Logs Tab Overview	111
3.5.2 Available Tasks at a Glance	111
3.5.3 Viewing Event Logs.....	112
3.5.4 Exporting Event Logs	113
3.5.5 Emptying Event Logs.....	114
3.6 Viewing Software Information	115
3.6.1 About Tab Overview	115
3.6.2 Available Tasks at a Glance	115
3.6.3 Viewing Information on Atrust Device Manager	116
3.6.4 Viewing Atrust Contact Information	116
3.6.5 Viewing Atrust Software License Agreement.....	116
Chapter 4 Configuring Client Settings.....	117
4.1 Desktop Virtualization and Client Configuration	118
4.2 Client Settings at a Glance.....	119
4.3 Editing or Adjusting a Group Configuration	120
4.4 Editing or Adjusting an Individual Configuration.....	122
4.5 Configuring Client Settings with Atrust Client Setup	124
Chapter 5 Notes and Restrictions.....	125
5.1 Synchronizing ADM with ACS Settings	126
5.2 Adding to and Releasing from Management.....	126
5.3 Notes on Taking and Installing Snapshots	127
5.3.1 Types of Snapshots.....	127
5.3.2 Behavior of Default User Account at Snapshot Installation	127
5.3.3 About Joining a Domain.....	127
5.3.4 Limitation of the Number of Snapshots That Can Be Taken	128
5.4 Retaining ACS Settings When Updating Firmware and Installing a Snapshot.....	129
5.5 Deactivation (License Activation) After Firmware Update or Snapshot Installation	129
5.6 Notes on Accessing the ADM Management Console.....	129
5.7 Notes on Using VNC (Remote Shadow).....	130
5.8 Notes on Backup and Restoring ADM Server	131
5.8.1 Database and Firmware and Package Backup	131
5.8.2 Restoration of ADM Server	131
5.9 Restrictions	132

Chapter 1 Overview

This chapter provides an overview of the Atrust Device Manager and the system requirements.

1.1 Introduction

A brief introduction to Atrust Device Manager

1.2 New Features

New features and enhanced functions in this product release

1.3 Features

The key features of Atrust Device Manager

1.4 System Requirements

The system requirements for the installation and operation of Atrust Device Manager

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 Atrust Device Manager 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



WARNING

- It is necessary to upgrade the US310e firmware to 1.20-INTL to use the new features. If you are using an old version of US310e firmware, upgrade it.

This product release provides the following new and enhanced functions:

Global setting of the web browser

The global setting of the web browser can be enabled and disabled in the client settings.

Desktop icon for remote desktop connection (Span mode)

A remote desktop connection (Span mode) desktop icon has been added to the client settings.

Snapshot backup

A backup type snapshot is now available in addition to the conventional deployment type snapshot.

Change of Administrator account password when taking snapshots

The built-in Administrator account password can now be changed when taking a deployment-type snapshot.

Application of firmware updates to client groups

Firmware updates can now be applied to client groups.

The following feature is no longer available as of this product release:

Setting of Atrust Client Setup user password

This feature is no longer available. It is now only possible to set an Atrust Client Setup access password in the client settings.

This product release includes the following modifications:

- The remote shutdown password policy has been modified.
- The ADM administrator password and ACS access user password policies have been modified.
- The problem that some user account profile settings are initialized when a snapshot is taken has been corrected.
- The irregularity with some of the VMware View connection snapshot settings has been corrected.
- The irregularity with some of the Webfeed type remote desktop connection shortcut settings has been corrected.

1.3 Features

The key features of Atrust Device Manager 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. US310e does not support the management of zero clients because it is not the zero clients.

1.4 System Requirements

The system requirements for the installation and operation of Atrust Device Manager are as follows:

1.4.1 Supported Endpoint Devices

Atrust Device Manager supports the following Atrust client family:

Model:

- US310e

Firmware:

- 1.10-INTL
- 1.20-INTL



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 (32-bit only)
- Windows 8 / 8.1 (32-bit only)
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2



WARNING

- The server on which you install Atrust Device Manager (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
- 10/100 Mb Ethernet network adapter / network interface card

1.4.4 Software Requirements

- Java software or Java Runtime Environment (for the Shadow feature, see page 104.)

1.4.5 Background Service and Used Ports of Atrust Device Manager

Background Service and Used Ports of Atrust Device Manager			
Service Name	Description	Protocol	Port
Atrust - Apache2.2	Atrust Apache HTTP Server Used for Web based User Interface of Atrust Device Manager and Web-based firmware update.	TCP	10443 10080
Atrust - Multicast	Atrust Multicast Service Used for service of one-to-many firmware update.	TCP	10081
Atrust - NBD	Atrust NBD Service Used to provide Network Block Device for zero clients to download zero images.	TCP	10010 to 10030
Atrust - PgSQL	Atrust PgSQL Database Server Used as database of Atrust Device Manager.	TCP	5432 (local only)
Atrust - PXE	Atrust PXE Service Used to allow network-based booting for zero clients.	UDP	4011 67
Atrust - TFTP	Atrust TFTP Service Used to allow zero clients to fetch kernel and boot loader during a PXE boot.	UDP	69
Atrust Device Manager	Atrust Device Manager Agent Used to allow the management of client settings and the communication with built-in Atrust Client Setup on clients	TCP UDP	10005 10007 10006



NOTE

- The name you can find on Windows Services management console.



WARNING

- ADM (Atrust Device Manager) automatically installs and configures everything you need for ADM use with respect to HTTP server, database, and the Windows Firewall.
- ADM (Atrust Device Manager) does not support changing the default port numbers.

1.4.6 Configuring the network environment

Installing a DHCP server

To update the firmware or take a snapshot of a thin client, or install a thin client, by using Atrust Device Manager, you need to install a DHCP server. Without a DHCP server installed, these features cannot be used.

The thin client needs to establish a network link at UEFI bootup to obtain the firmware update and snapshot image files from the server. The information for the network link is provided by the DHCP server.

Wake on LAN

Wake on LAN messages cannot be sent to a thin client that does not belong to the same segment as Atrust Device Manager. Wake on LAN broadcasts a magic packet on layer 2, so Wake on LAN messages 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.

VPN

Atrust Device Manager 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

- Atrust Device Manager 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).



WARNING

- Note that no Atrust Device Manager 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 firmware, taking snapshots, and installing thin clients 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 Atrust Device Manager

This chapter gives detailed instructions on how to install and upgrade your Atrust Device Manager.

2.1 Installing Atrust Device Manager

The installation of Atrust Device Manager

2.2 Installing Java Software

The installation of Java Software or Java Runtime Environment

2.3 Initial Setup

The initial setup of Atrust Device Manager

2.4 Upgrading Atrust Device Manager

The upgrade of Atrust Device Manager

2.5 Uninstalling Atrust Device Manager

The uninstallation of Atrust Device Manager

2.1 Installing Atrust Device Manager

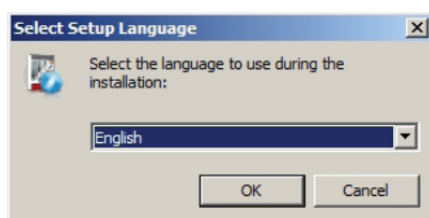
To install Atrust Device Manager on your computer, please follow the steps below:



NOTE

- Before proceeding, ensure that:
 - ✓ Your operating system is supported (see "1.4 System Requirements" on page 7)
 - ✓ Your computer meets system requirements (see "1.4.4 Software Requirements" on page 7)
- To install a newer version of Atrust Device Manager, it's recommended to install it directly without uninstalling the current Atrust Device Manager. For more information on how to upgrade your Atrust Device Manager, please refer to section "2.4 Upgrading Atrust Device Manager" on page 20.
- Setting up a static IP address on your computer.

1. Get a copy of the installation program of Atrust Device Manager 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.



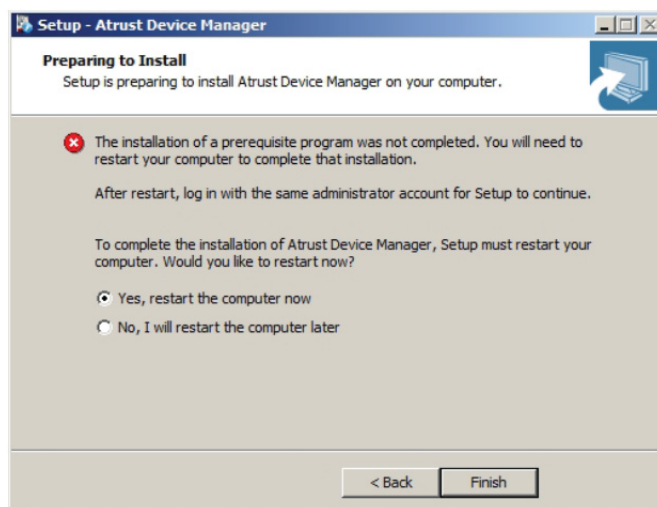
4. The Setup Wizard appears. Click **Next** to continue.



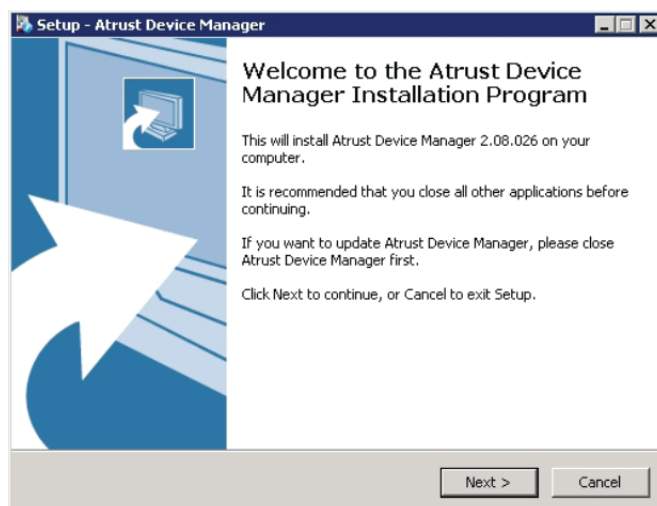
NOTE

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

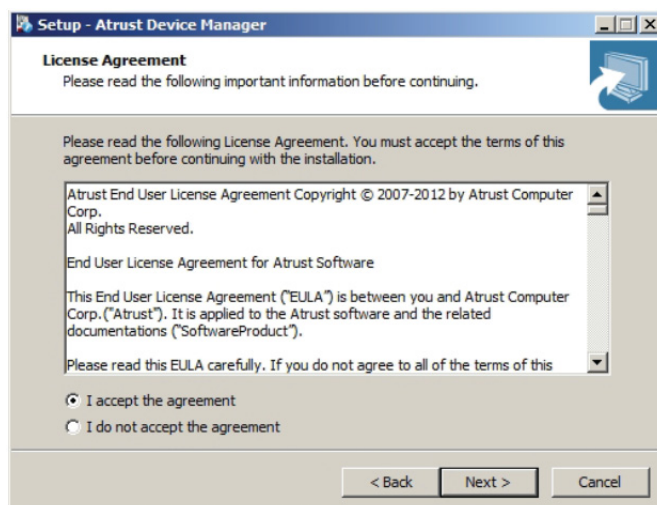
5. A message appears prompting you to restart for the installation of a prerequisite program. Select **Yes, restart the computer now**, and then click **Finish**.



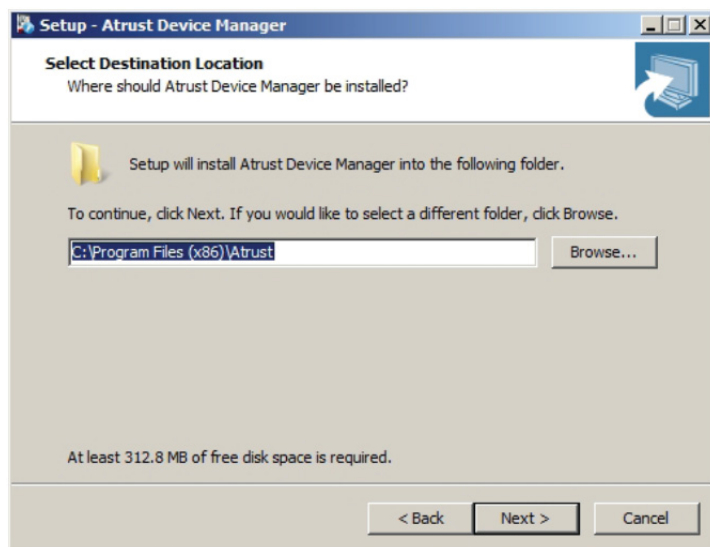
6. After restart, the Setup Wizard appears again. Click **Next** to continue.



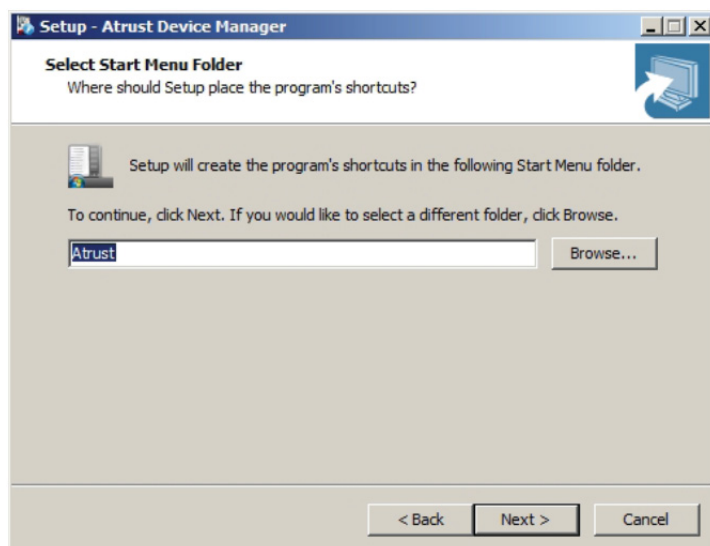
7. The License Agreement page appears. Read this agreement, select **I accept the agreement**, and then click **Next** to continue.



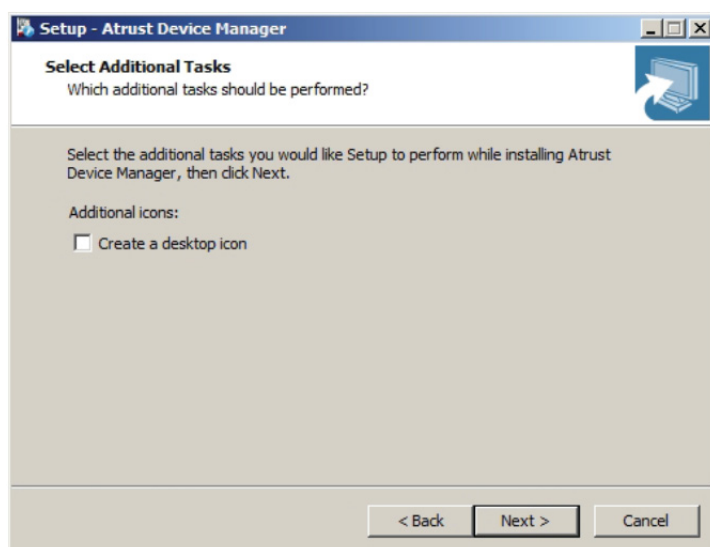
8. Use the default installation directory or click **Browse** to locate the desired one, and then click **Next** to continue.



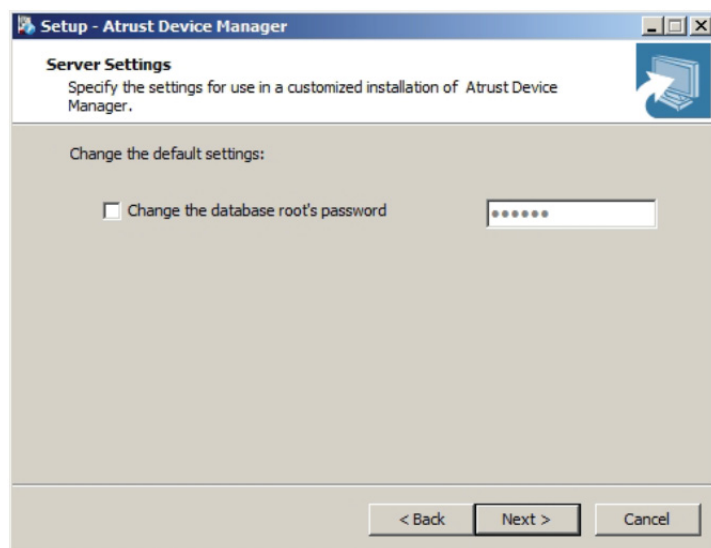
9. Use the default Start menu folder or type to create a new folder for the shortcuts of programs. Or, click **Browse** to choose an existing folder. Click **Next** to continue.



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



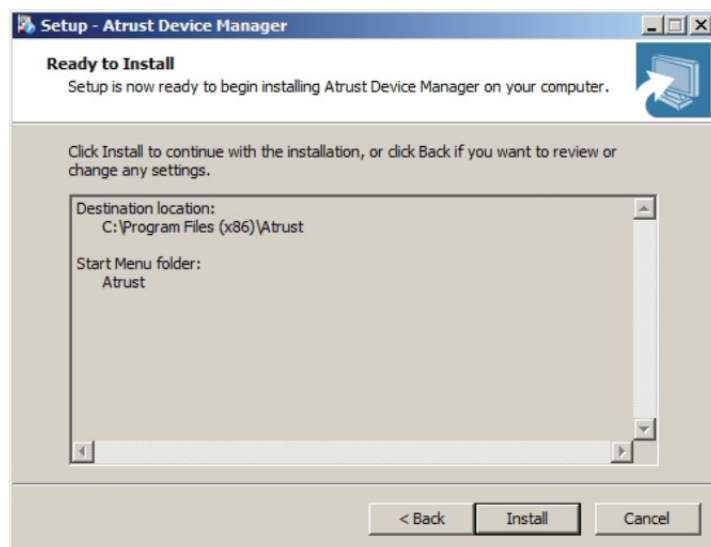
11. Change the default database password for the superuser or use the default. After completion, click **Next** to continue.



NOTE

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

12. Click **Install** to start installing Atrust Device Manager on your computer.



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



2.2 Installing Java Software

To access full functionality of Atrust Device Manager, you need to install the Java software, which is free and downloadable from Java's official website at java.com. The Java software or Java Runtime Environment is required for the Shadow feature of Atrust Device Manager, enabling you to remotely assist a client user.



NOTE

- For more details, please refer to section "3.4.28 Assisting a Client User Remotely" on page 104.

It is recommended to install 32-bit Java for Atrust Device Manager. In case that the computer where you install Atrust Device Manager also needs 64-bit Java for other purposes, you could install both 32-bit and 64-bit Java.



NOTE

- For more information, please visit Java's website at java.com.
- For Java **Version 7 Update 51** or **the later**, you may need to add your computer to the (Security) Exception Site list. Go to **Control Panel**, click **Java > Security > Edit Site List > Add**, type **<https://localhost:10443>**, and then click **OK** to apply.
- If you fail to download the Installer from Java's website at java.com, refer to java's SE site.

2.3 Initial Setup

When launching Atrust Device Manager for the first time, you need to complete the initial setup. Follow the instructions below to complete the required configuration:

1. Launch Atrust Device Manager 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.



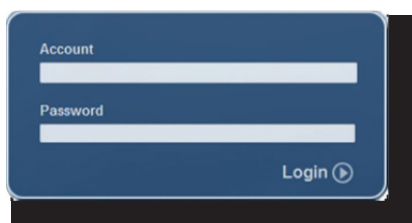
The screenshot shows the 'Atrust Device Manager Setup Wizard' window. It has two main sections: 'Choose service IP address' and 'Create default administrator account'. In the first section, the 'IP Address' is set to '192.168.11.109'. In the second section, there are three input fields for 'Account', 'New Password', and 'Confirm Password', each with a red asterisk indicating a required field. A 'Save' button is located at the bottom right of the window.



NOTE

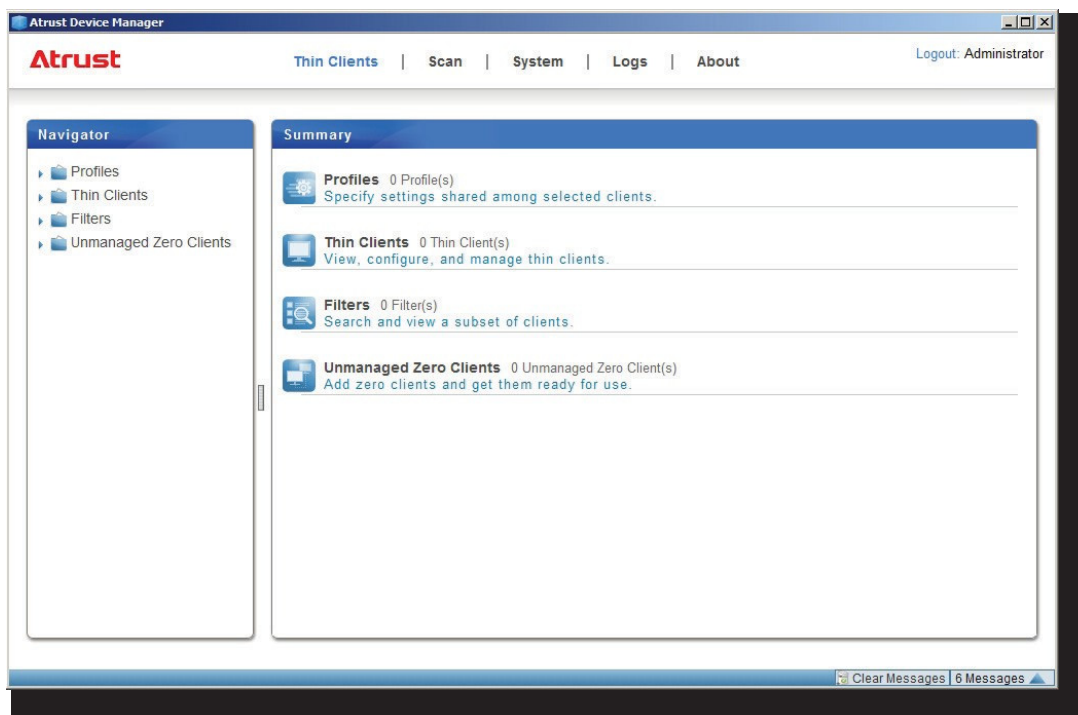
- The unconnected LAN port may appear in the list of available IP addresses with the address value **0.0.0.0**.
- It is strongly recommended to use a fixed IP address as the service IP of Atrust Device Manager. The change of the service IP may make all the managed clients become unmanageable.

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



The screenshot shows the 'Login' screen of Atrust Device Manager. It features two input fields labeled 'Account' and 'Password'. Below these fields is a 'Login' button with a right-pointing arrow.

4. The management interface of Atrust Device Manager appears.



NOTE

- In next chapter, we will describe the functionality and use of Atrust Device Manager in details.

2.4 Upgrading Atrust Device Manager

To upgrade your Atrust Device Manager to a newer version, you can just install the new program without uninstalling the old one. For information on how to install Atrust Device Manager, please refer to section "2.1 Installing Atrust Device Manager" on page 12.



NOTE

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



WARNING

- Before upgrading your Atrust Device Manager, ensure that you've logged out and closed the Atrust Device Manager console.

2.5 Uninstalling Atrust Device Manager

To uninstall your Atrust Device Manager on a computer, please do the following:



NOTE

- To **upgrade** your Atrust Device Manager, it's recommended **not** to uninstall the current Atrust Device Manager. For more information, please refer to section "2.4 Upgrading Atrust Device Manager" on page 20.
- Ensure that you have backed up important data on Atrust Device Manager before proceeding.



WARNING

- Before uninstalling your Atrust Device Manager, ensure that you've logged out and closed the Atrust Device Manager console.

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

Chapter 3 Using Atrust Device Manager

This chapter provides instructions on how to manage clients with Atrust Device Manager.

3.1 Atrust Device Manager

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

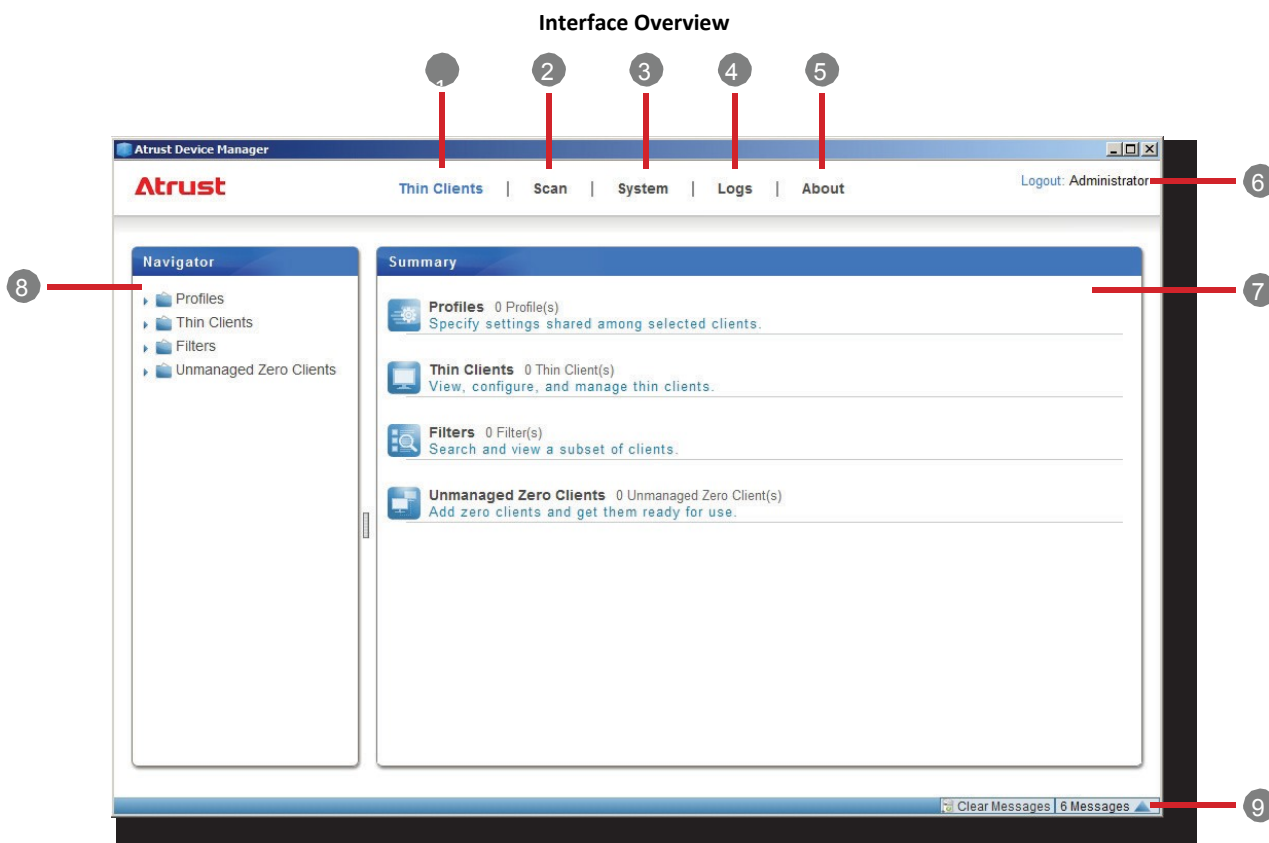
3.1 Atrust Device Manager

Atrust Device Manager 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 Atrust Device Manager, please do the following:

1. Launch Atrust Device Manager on your computer.
2. Type your credentials, and then press **Enter** or click **Login**. The Atrust Device Manager 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 Atrust Device Manager.
6	Logout button	Click to log out from Atrust Device Manager.
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

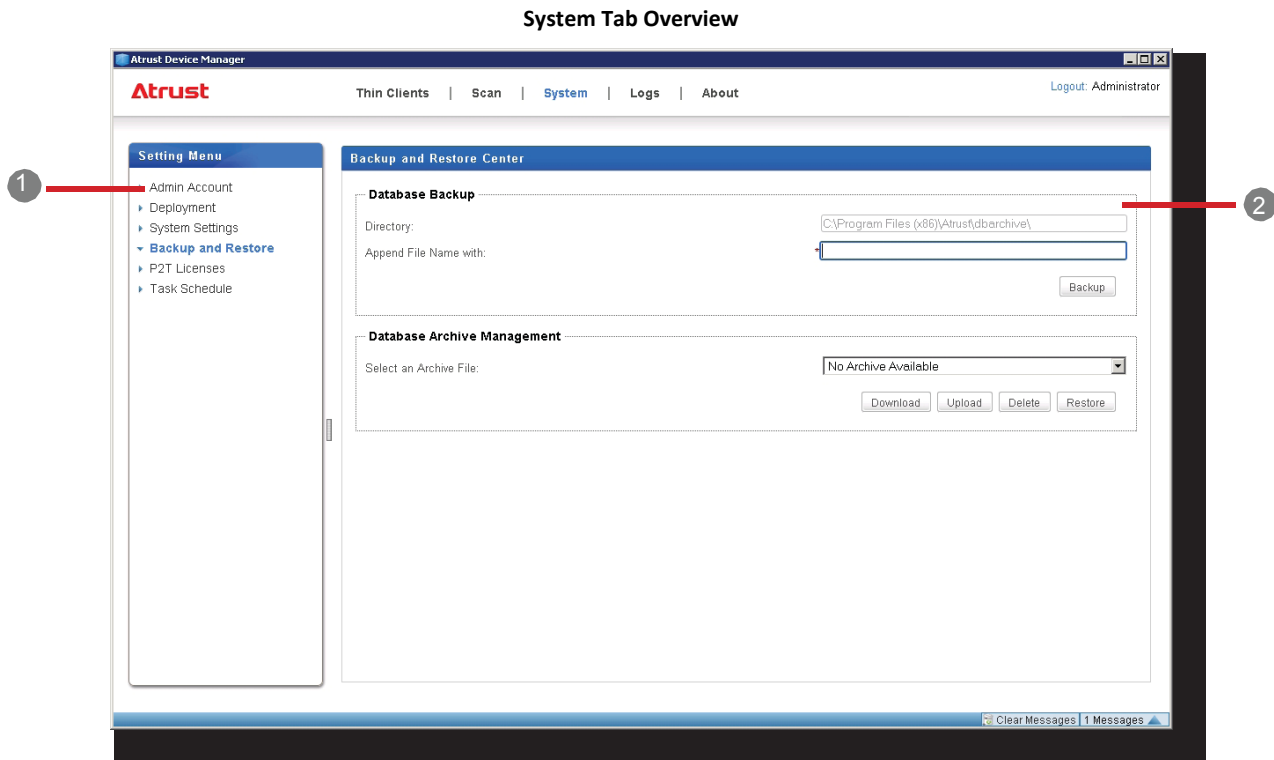
The following table shows functionality provided in each tab. For more details, please refer to the corresponding section as shown below:

Tab	Function List	Section	Page
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 	3.2 Establishing a Basic Administration Environment	25
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 	3.3 Adding Clients into a Managed Group	50
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 	3.4 Managing All Your Clients	57
Logs	<ul style="list-style-type: none"> • Viewing event logs • Exporting event logs 	3.5 Viewing and Managing Event Logs	111
About	<ul style="list-style-type: none"> • Viewing information on Atrust Device Manager • Viewing Atrust contact information 	3.6 Viewing Software Information	115

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 Atrust Device Manager.



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	Page
1	Creating accounts for administration	3.2.3	27
2	Deleting an account	3.2.3	28
3	Editing an account	3.2.3	28
4	Importing thin client firmware files	3.2.4	29
5	Deleting thin client firmware files	3.2.4	30
6	Scanning thin client firmware files	3.2.4	31
7	Importing zero client image files	3.2.5	32
8	Deleting zero client image files	3.2.5	–
9	Importing WES package files	3.2.6	33
10	Deleting WES package files	3.2.6	34
11	Scanning WES package files	3.2.6	35
12	Exporting client snapshots	3.2.7	36
13	Importing client snapshots	3.2.7	37
14	Deleting client snapshots	3.2.7	37
15	Scanning client snapshots	3.2.7	38
16	Importing certificates of remote computers	3.2.8	39
17	Deleting certificates of remote computers	3.2.8	–
18	Configuring remote deployment settings	3.2.9	39
19	Selecting the service IP address of Atrust Device Manager	3.2.10	41
20	Configuring auto-logout for Atrust Device Manager	3.2.11	42
21	Configuring the database source of Atrust Device Manager	3.2.12	43
22	Selecting the interface language of Atrust Device Manager	3.2.13	44
23	Backing up the management database	3.2.14	44
24	Downloading a database archive file	3.2.15	45
25	Uploading a database archive file	3.2.15	45
26	Deleting a database archive file	3.2.15	45
27	Restoring a database archive file	3.2.16	46
28	Importing P2T license files	3.2.17	46
29	Scheduling automatically performed tasks	3.2.18	47

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		2014-05-15 01:07:49	Admin



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 Atrust Device Manager; 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		2014-05-15 01:07:49	Admin
Francis	Francis Crick		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 Atrust Device Manager. Before proceeding, you need to import firmware files of appropriate versions for Atrust Device Manager.



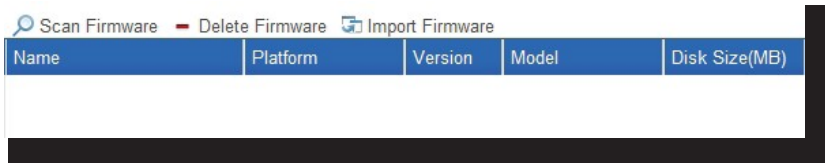
NOTE

- For instructions on how to update firmware for clients remotely, please see section "3.4.24 Updating Client Firmware" on page 98.
- To upgrade your zero clients, what you need is an image file for zero clients rather than a firmware file for thin clients. For information on zero client image files, please refer to section "3.2.5 Managing Zero Client Image Files" on page 32.

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.



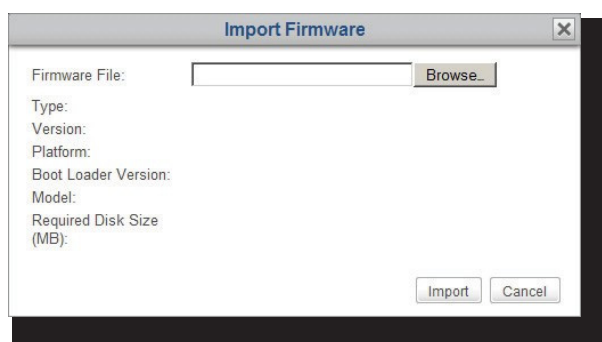
Name	Platform	Version	Model	Disk Size(MB)
------	----------	---------	-------	---------------



NOTE

- If you never imported firmware files into Atrust Device Manager, 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.



Import Firmware

Firmware File: Browse...

Type:

Version:

Platform:

Boot Loader Version:

Model:

Required Disk Size (MB):

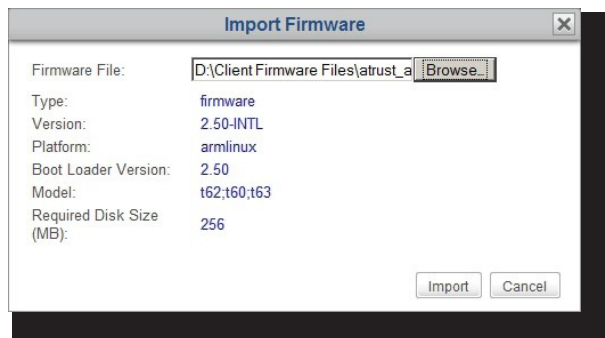
Import Cancel

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

**NOTE**

- Atrust Device Manager 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.

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



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

Scan Firmware Delete Firmware Import Firmware				
Name	Platform	Version	Model	Disk Size(MB)
ARM LINUX 2.50-INTL	ARM Linux	2.50	t60, t62, t63	256

Deleting Thin Client Firmware Files

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

- On **System** tab, click **Deployment > Firmware**.
- The Firmware list appears in Management area.
- 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.

- The Delete Firmware window appears prompting you for confirmation.
- Click **Delete** to confirm.
- 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 Atrust Device Manager 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 Atrust Device Manager to use remote firmware files on another computer for client management, please refer to section "3.2.9 Configuring Remote Deployment Settings" on page 39.

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



NOTE

- The default installation directory of Atrust Device Manager 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 Zero Client Image Files

**WARNING**

- This feature is not supported. A zero client is an endpoint device without any operating system pre-installed. US310e is not the zero clients.

3.2.6 Managing WES Package Files

With WES (Windows Embedded Standard) 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 for Atrust Device Manager.



NOTE

- The Windows Embedded Standard 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 "3.4.25 Installing Software Packages" on page 100.

Importing WES Package Files

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



NOTE

- For information about availability of a newer or up-to-date version of package file (.zip format), please contact your dealer.

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	Size(MB)	Req. Spaces(MB)	Publisher



NOTE

- If you never imported WES package files into Atrust Device Manager, 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.

The 'Import Package' dialog box contains the following fields and buttons:

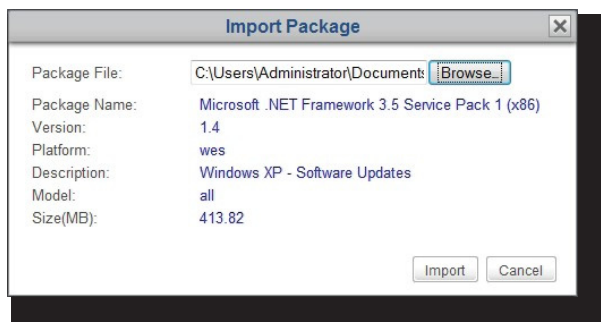
- Package File:** A text input field with a 'Browse...' button next to it.
- Package Name:** A text input field.
- Version:** A text input field.
- Platform:** A text input field.
- Description:** A text input field.
- Model:** A text input field.
- Size(MB):** A text input field.
- Buttons:** 'Import' and 'Cancel' buttons at the bottom right.

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

**NOTE**

- Atrust Device Manager 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	Size(MB)	Req. Spaces(MB)	Publisher
Microsoft .NET Framework 3.5	Application	1.4	1.11-INTL	WES	413.82	708	Atrust

Deleting WES Packages

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

- On **System** tab, click **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 Atrust Device Manager 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 Atrust Device Manager to use remote package files on another computer for client management, please refer to section "3.2.9 Configuring Remote Deployment Settings" on page 39.

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



NOTE

- The default installation directory of Atrust Device Manager 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.

3.2.7 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.



NOTE

- For instructions on how to take a system snapshot for clients, please refer to section "3.4.26 Taking Client Snapshots" on page 102.

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 between 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 Atrust Device Manager 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

- Atrust Device Manager 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 Atrust Device Manager 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 Atrust Device Manager to use remote snapshots on another computer for client management, please refer to section "3.2.9 Configuring Remote Deployment Settings" on page 39.

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



NOTE

- The default installation directory of Atrust Device Manager is C:\Program Files (x86)\Atrust. All snapshots taken or imported through Atrust Device Manager 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.

3.2.8 Managing Certificates of Remote Computers



3.2.9 Configuring Remote Deployment Settings

You can deploy, maintain, and upgrade your thin clients from a remote computer with Atrust Device Manager. All required files (firmware, snapshot, or package files) can come from the same computer where your Atrust Device Manager 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 Atrust Device Manager is installed	Default
Using remote updates and snapshots	Configure settings to get all needed files from another computer	



NOTE

- In Atrust Device Manager, 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:

Username:

Password:

Save

Snapshot

Server Type: Use External Server

Snapshot URL:

Username:

Password:

Save

WES Packages

Server Type: Use External Server

WES Packages URL:

Username:

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: Use External Server

Firmware URL:

Username:

Password:

Save

Snapshot

Server Type: Use External Server

Snapshot URL:

Username:

Password:

Save

WES Packages

Server Type: Use External Server

WES Packages URL:

Username:

Password:

Save

3.2.10 Selecting the Service IP of Atrust Device Manager

To select the service IP address of your Atrust Device Manager, please do the following:

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

Atrust Device Manager

Service IP Address:

3. Click **Save** to apply.



NOTE

- It is strongly recommended to use a fixed IP address as the service IP of Atrust Device Manager. The change of the service IP may make all the managed clients become unmanageable. In case that the IP address of the computer where Atrust Device Manager is installed is changed, ensure that you make the Service IP setting here consistent with the new IP address.



NOTE

- In case that the service IP changes, your Atrust Device Manager will prompt you to select a new service IP when you log in to the management console.

3.2.11 Configuring Auto-Logout for Atrust Device Manager

Atrust Device Manager 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 Atrust Device Manager, 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.

Auto Logout

Auto Logout After:

3. Click **Save** to apply.

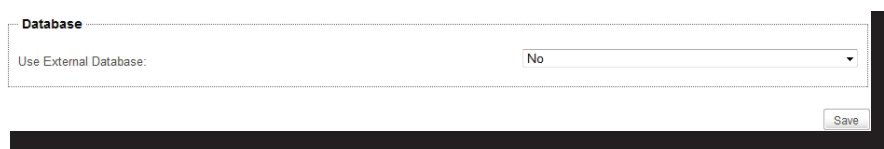
3.2.12 Configuring the Database Source of Atrust Device Manager

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

Using Local Management Database

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

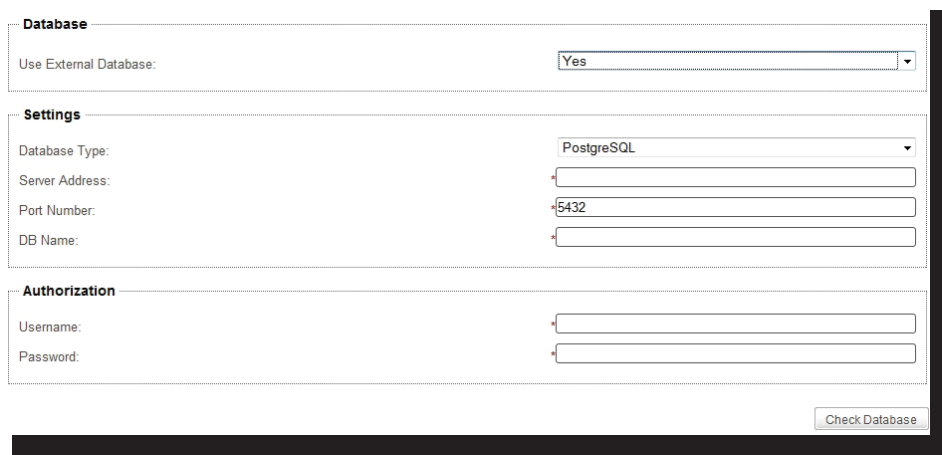
1. On **System** tab, click **System Settings > External Database**.
2. The External Database pane appears in Management area.
3. Click the drop-down menu to select **No**.



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.




NOTE

- Four database management systems are supported: PostgreSQL, MySQL, MsSQL (Microsoft SQL Server), and Oracle (Oracle Database).
- 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.

3.2.13 Selecting the Interface Language of Atrust Device Manager

To select the interface language of your Atrust Device Manager, 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.

3.2.14 Backing Up the Management Database

To back up the management database of Atrust Device Manager, please do the following:

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



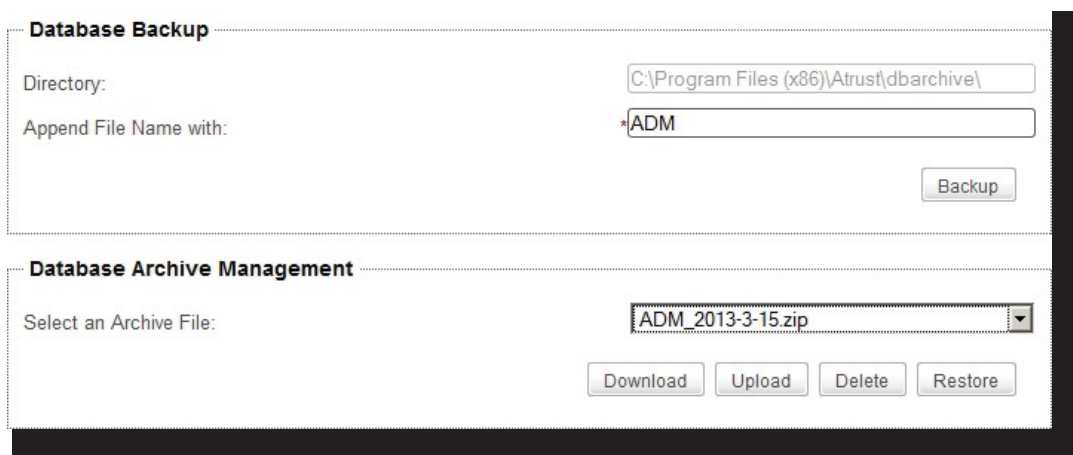
The screenshot shows the 'Database Backup' section of the Atrust Device Manager interface. It contains two text input fields: 'Directory:' with the value 'C:\Program Files (x86)\Atrust\dbarchive\' and 'Append File Name with:' with the value '*ADM'. A 'Backup' button is located at the bottom right of the section.



TIP

- 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.



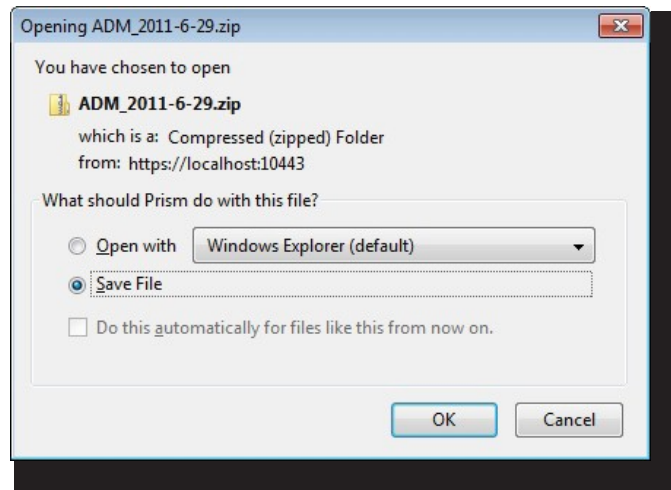
The screenshot shows two sections of the Atrust Device Manager interface. The top section is 'Database Backup', which is identical to the one in the previous block. The bottom section is 'Database Archive Management'. It features a 'Select an Archive File:' label and a dropdown menu showing 'ADM_2013-3-15.zip'. Below the dropdown are four buttons: 'Download', 'Upload', 'Delete', and 'Restore'.

3.2.15 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. Select **Save File**, and then click **OK** to confirm.



4. In the opened window, navigate to the desired location, and then click **Save** to store the file.

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.

3.2.16 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.

Database Archive Management

Select an Archive File: ADM_2013-3-15.zip

3. Click **Restore** to return the management database of Atrust Device Manager to the desired state.

3.2.17 Managing P2T License Files

**WARNING**

- This feature is not supported.

3.2.18 Scheduling Automatically Performed Tasks

Atrust Device Manager 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.



NOTE

- The Task list might be empty, if you 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: 2014-4-23 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.

Add Task Schedule

☒ Enable Task Schedule

Schedule

Details

Perform:

Daily

Execute every

1

 day(s).

Start Date:

2014-04-24

Select

Start Time:

11

 :

55

Comment:

End Sessions and Refresh Endpoints before Afternoon Opening Time

Previous:


Next:

Previous Result:

Save

Cancel

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

 **NOTE**

- One **task** consists of **one or more actions**.

Add Task Schedule

☒ Enable Task Schedule

Schedule

Details

Add

Edit

Delete

Module Name	Action	Comment	Order	
-------------	--------	---------	-------	--

Comment:

End Sessions and Refresh Endpoints before Afternoon Opening Time

Previous:

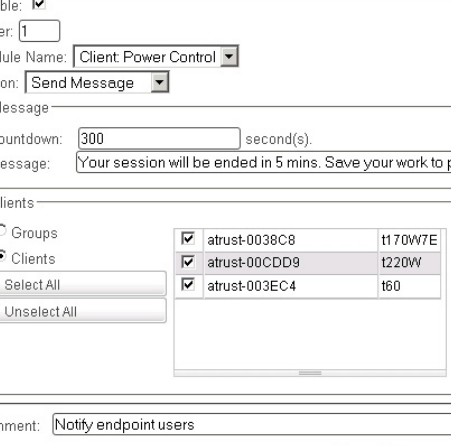
Next:

Previous Result:

Save

Cancel

- 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:

Module Name:

Action:

Message

Countdown: second(s).

Message:

Clients

☐ Groups

☒ Clients

<input checked="" type="checkbox"/>	atrust-0038C8	t170W7E
<input checked="" type="checkbox"/>	atrust-00CDD9	t220W
<input checked="" type="checkbox"/>	atrust-003EC4	t60

Comment:

The screenshot shows a standard Windows-style dialog box titled "Add". It features a close button (X) in the top right corner. The dialog contains the following elements:

- Enable:** A checkbox that is currently checked.
- Order:** A text input field containing the number "4".
- Module Name:** A dropdown menu with "Task: Wait" selected.
- Wait:** A text input field containing "10", followed by the text "minute(s)." indicating the unit of time.
- Comment:** A larger text input field containing the text "Wait for 10 mins".
- Buttons:** "OK" and "Cancel" buttons located at the bottom right of the dialog.

Enable: ☒

Order:

Module Name:

Action:

Clients

☐ Groups

☒ Clients

<input checked="" type="checkbox"/>	atrust-0038C8	t170WV7E
<input checked="" type="checkbox"/>	atrust-00CDD9	t220WV
<input checked="" type="checkbox"/>	atrust-003EC4	t60

Comment:

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	Order
	Power Control	Send Message	Notify endpoint users	1
	Wait	10 min.	Wait for 10 mins	2
	Power Control	Shutdown	Shut down endpoints	3
	Wait	10 min.	Wait for 10 mins	4
	Power Control	Wake On LAN	Wake endpoints remotely	5

Comment:

End Sessions and Refresh Endpoints before Afternoon Opening Time

Previous:

Next:

Previous Result:

Save

Cancel

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

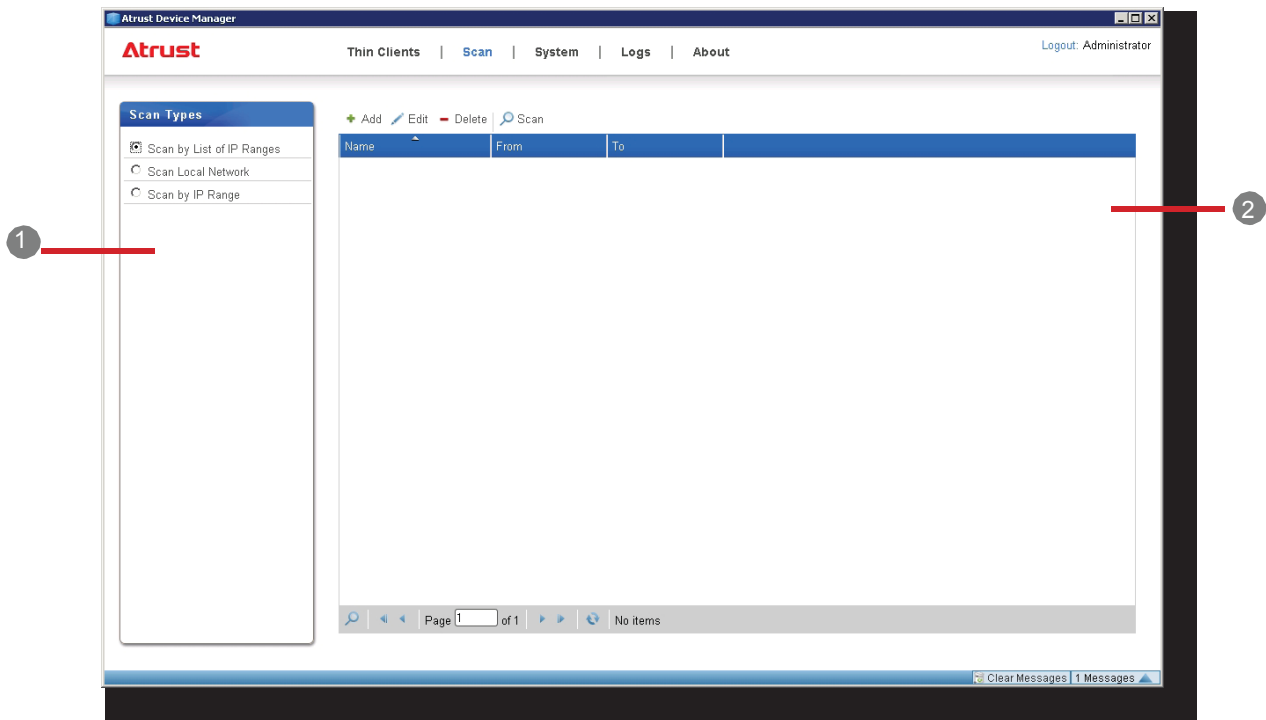
+ Add ✎ Edit - Delete 🔍 View Log					
	Schedule	Comment	Next Schedule	Prev Schedule	Status
✔	Daily	End Sessions and Refresh Endpoints before Afternoon Opening Time	2014-04-24 11:55		

3.3 Adding Clients into a Managed Group

3.3.1 Scan Tab Overview

Scan tab enables you to discover unmanaged clients over your local network, including clients that are not managed by the current Atrust Device Manager instance. To access the functionality of Scan tab, click the tab on Atrust Device Manager.

Scan Tab Overview



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	Page
1	Discovering clients in the whole range of a local network	3.3.4	52
2	Discovering clients in a specified range of IP addresses	3.3.5	53
3	Discovering clients using predefined IP range lists	3.3.6	54
		3.3.7	55

3.3.3 Client Detection and Management

Your client is not managed by any Atrust Device Manager by factory default. To manage your clients with Atrust Device Manager, you need to first detect unmanaged clients over your local network, and then add them into a managed group under your Atrust Device Manager.



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:

Type	Model	Prerequisites	Method	Section	Page
Thin Client	US310e	<ul style="list-style-type: none">Clients are connected to the local networkClients are powered up	Manual Scan	3.3.4	52
				3.3.5	53
				3.3.6	54



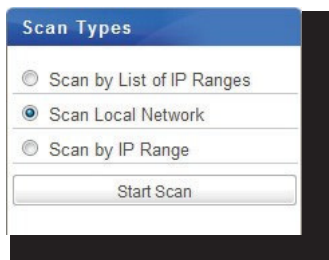
NOTE

- If the computer where an Atrust Device Manager is installed connects to a local network, then the Atrust Device Manager is connected to the local network.
- After adding clients into a managed group under your Atrust Device Manager, 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" on page 57.

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 Atrust Device Manager, please do the following:

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



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

The interface shows the 'Scan Types' dialog on the left with 'Scan Local Network' selected. On the right, a table lists discovered clients. Above the table is a 'Put in group' dropdown menu set to '05 Conference Room', and buttons for 'Unselect All' and 'Select All'.

Name	IP	Mac Address	Model	Firmware	Managed
atrust-001C16	192.168.50.155	00:1F:D8:00:1C:16	t50	ARM Linux 1.75-INTL	No
atrust-002132	192.168.50.192	00:1F:D8:00:21:32	t50	ARM Linux 1.75-INTL	No
atrust-00385C	192.168.50.129	00:1F:D8:00:38:5C	t170W7E	WES7 1.16-INTL	No
atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.51-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 "3.4.4 Creating Client Groups" on page 60.
- 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 Atrust Device Manager.



NOTE

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

3.3.5 Discovering Clients in a Specified Range of IP Addresses

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

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

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

Name	IP	Mac Address	Model	Firmware
atrust-0008BA	192.168.11.72	00:1F:D8:00:08:BA	t160W	WES 1.03-INTL
atrust-001C64	192.168.11.101	00:1F:D8:00:1C:64	t50	Atrust Linux 1.30-INTL
atrust-001FA0	192.168.11.71	00:1F:D8:00:1F:A0	t50	Atrust Linux 1.31-INTL

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 "3.4.4 Creating Client Groups" on page 60.
- 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 Atrust Device Manager.



NOTE

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

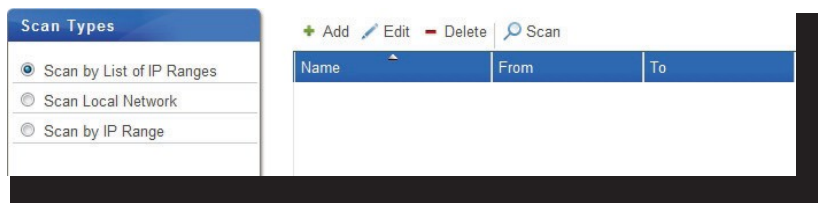
3.3.6 Creating and Managing an IP Range List

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

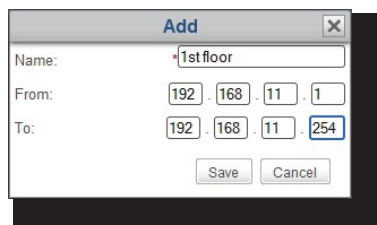
Creating an IP Range List

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

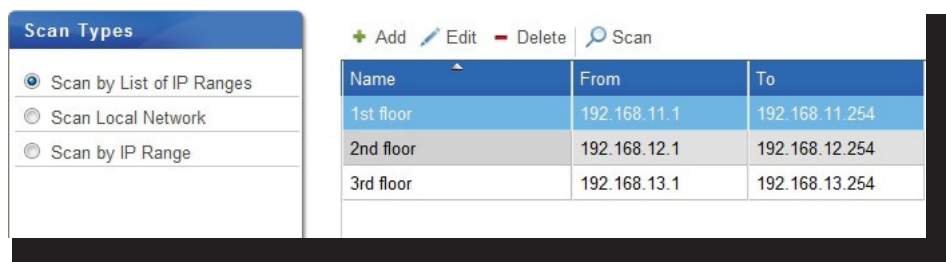
To discover unmanaged clients using a predefined IP Range list and add the desired client(s) into a managed group under Atrust Device Manager, please do the following:



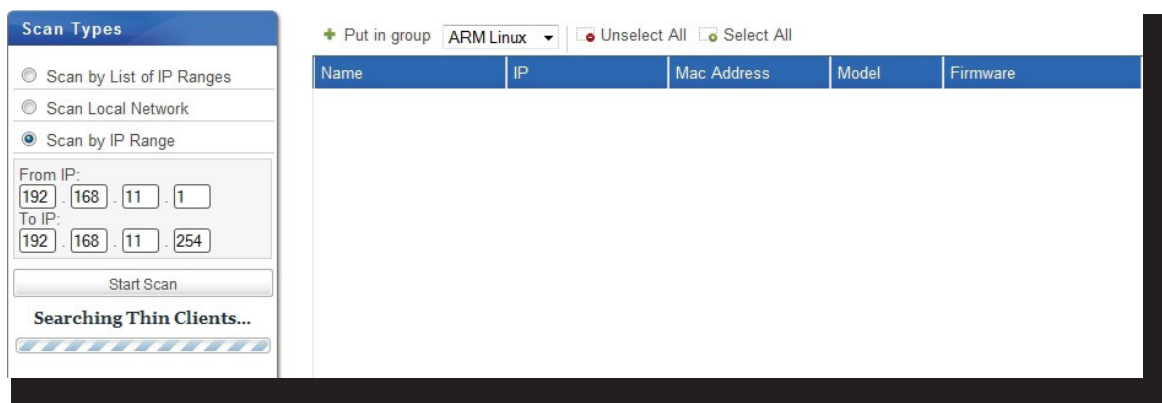
NOTE

- If you have not created any IP Range list, please refer to "3.3.6 Creating and Managing an IP Range List" on page 54 for instructions.

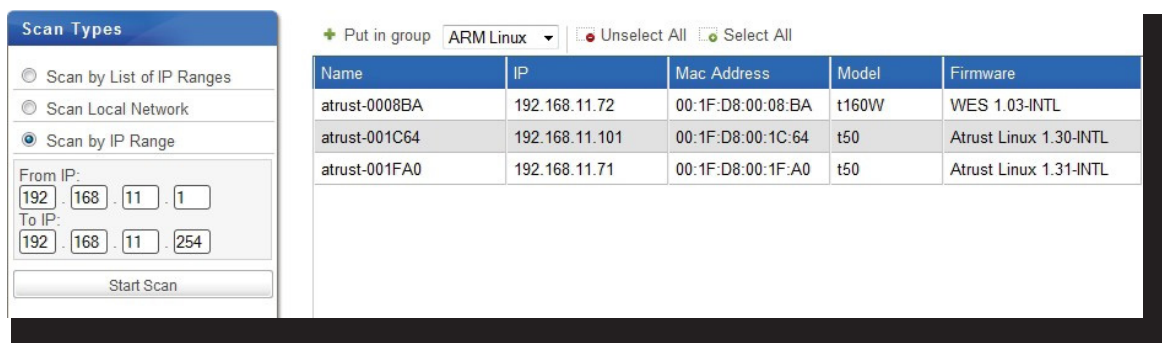
- On **Scan** tab, select **Scan by List of IP Ranges**.
- The IP Range list appears.
- Click to select the desired IP range, and then click **Scan** to look for unmanaged clients within the range.



- While searching for thin clients, the selected IP range is shown on the right.



- On completion, the discovered clients are listed in Management area.



6. 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 "3.4.4 Creating Client Groups" on page 60.
- To select multiple clients, just click to select each individual client. You can also use **Select All** and **Unselect All** above the Client list to select/unselect clients.

7. On completion, the client(s) is managed by your Atrust Device Manager.

**NOTE**

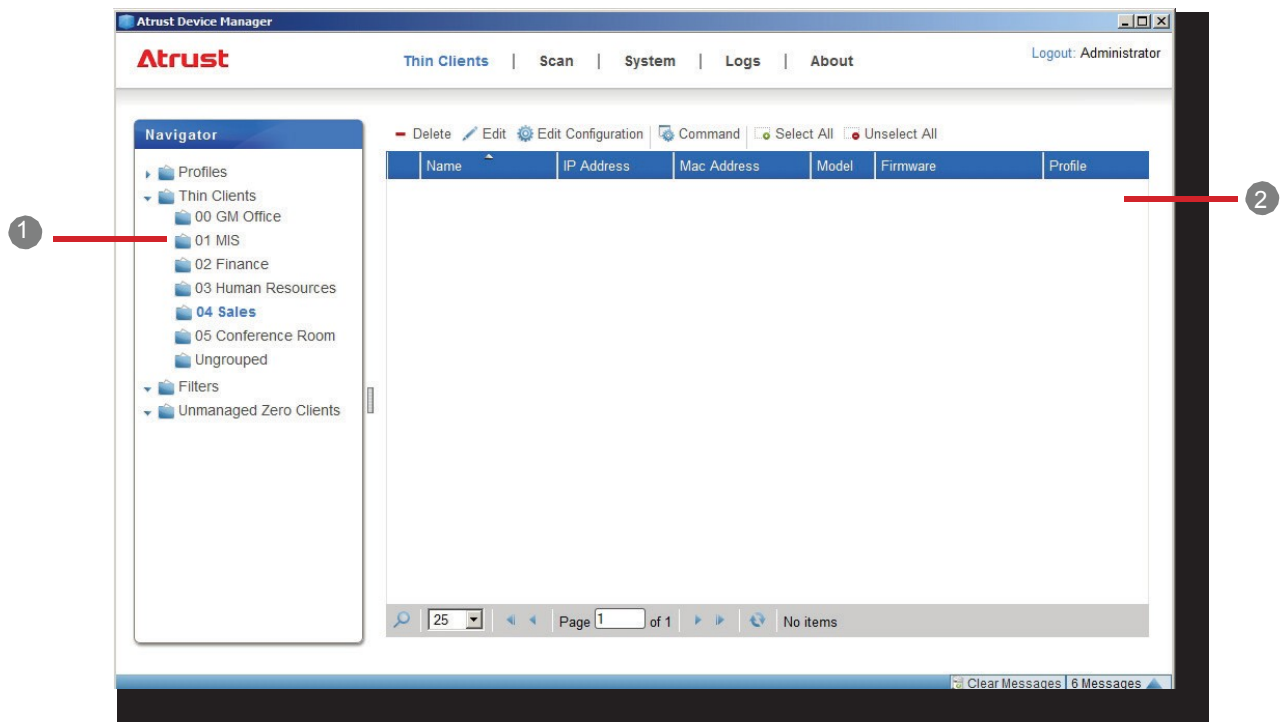
- Whichever group you add a client to (including **Ungrouped**), once **Put in group** is executed successfully, the client will be managed by your Atrust Device Manager.

3.4 Managing All Your Clients

3.4.1 Thin Clients Tab Overview

Thin **C**lients tab helps you to manage all your clients. To access the functionality of **Thin Clients** tab, click the tab on Atrust Device Manager.

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	Page
1	Getting your zero client ready for use	3.4.3	59
2	Creating client groups	3.4.4	60
3	Managing client groups	3.4.5	61
4	Managing clients in a group	3.4.6 3.4.7	62 63
5	Creating setting profile groups	3.4.10	67
6	Managing setting profile groups	3.4.11	68
7	Creating client setting profiles	3.4.12	69
8	Managing client setting profiles	3.4.13	72
9	Using individualized client settings	3.4.14	75
10	Using hybrid client settings	3.4.15	77
11	Pushing settings to clients through your local network	3.4.16	79
12	Pulling settings from clients through your local network	3.4.17	83
13	Pushing certificates of remote computers to clients	3.4.18	86
14	Sending messages to clients	3.4.19	87
15	Editing or viewing basic information about a client	3.4.20	88
16	Rebooting clients through your local network	3.4.21	89
17	Shutting down clients through your local network	3.4.22	92
18	Waking clients through your local network	3.4.23	95
19	Updating client firmware	3.4.24	98
20	Installing software packages	3.4.25	100
21	Taking client snapshots	3.4.26	102
22	Restoring client snapshots	3.4.27	103
23	Assisting a client user remotely	3.4.28	104
24	Monitoring a client remotely	3.4.28	104
25	Controlling a client remotely	3.4.28	104
26	Exporting client data	3.4.29	106
27	Digging out profiles or managed clients with Quick Search	3.4.30	107
28	Digging out managed clients with filters	3.4.31	108
29	Managing your client filters	3.4.32	110

3.4.3 Getting Your Zero Client Ready for Use

**WARNING**

- This feature is not supported. A zero client is an endpoint device without any operating system pre-installed. US310e does not support the management of zero clients because it is not the zero clients.

3.4.4 Creating Client Groups

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

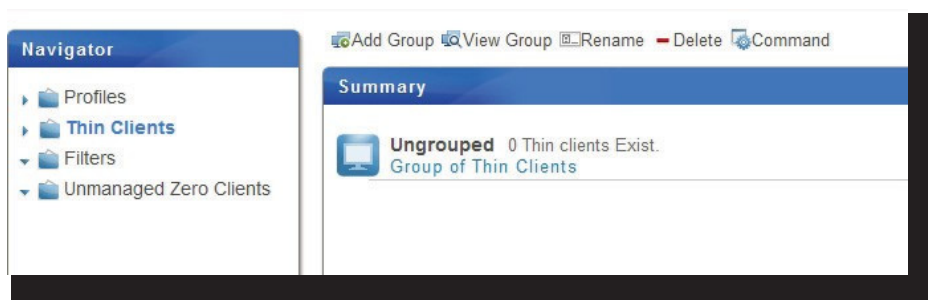


NOTE

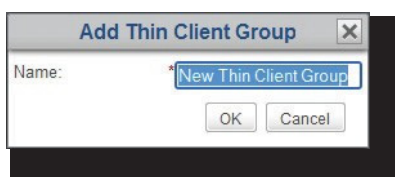
- The default client group is **Ungrouped**. You can change a client's group if needed.

To create a client group, please do the following:

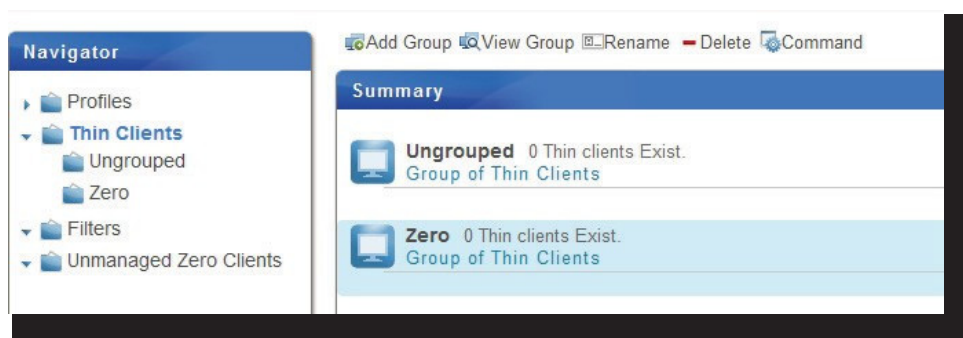
1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. Click **Add Group** on the top of the Management area.



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.



3.4.5 Managing Client Groups

Renaming a Client Group

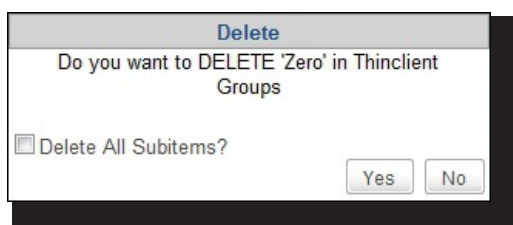
To rename a client group, please do the following:

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.



- To keep all clients in this group, leave **Delete All Subitems** cleared, and then click **Yes** 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 **Yes** to confirm. All clients in this group will be removed from your Atrust Device Manager.



NOTE

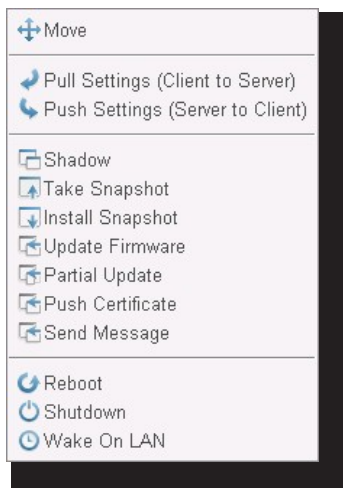
- Removing a client from your Atrust Device Manager will release the client from the management of Atrust Device Manager.

4. The client group is deleted.

3.4.6 Moving Clients to Another Group

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

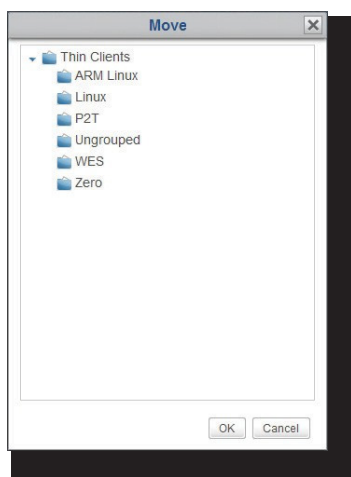
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. Click to select the desired client, and then click **Command** on the top of the Client list to open the Command menu.



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.

3.4.7 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 Atrust Device Manager will release the client from the management of Atrust Device Manager.

3.4.8 Understanding 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.

Name	IP Address	Mac Address	Model	Firmware	
t200W-00084E	192.168.11.117	00:1F:D8:00:08:4E	t200W	WES 1.13-INTL	
t200W-000AB2	192.168.11.109	00:1F:D8:00:0A:B2	t200W	WES 1.13-INTL	
t210W-001BFE	192.168.11.139	00:1F:D8:00:1B:FE	t210W	WES 1.13-INTL	



NOTE

- With filters, you can access and manage a specific set of clients quickly on Atrust Device Manager. For more information on filters, please refer to section "3.4.31 Digging Out Clients with Filters" on page 108.

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 Atrust Device Manager and you need to push the change to the client.
Pushed		Indicates that Atrust Device Manager has pushed a configuration change to the client.
Unknown		Indicates that the managed client is now added and managed by another instance of Atrust Device Manager.



NOTE

- A tooltip pops up if you hover your mouse pointer over an icon.

3.4.9 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" on page 117.

Remote and Local Management of Client Settings

You can configure your client settings locally or remotely. With Atrust Device Manager, you can configure client settings remotely through your local network. With Atrust Client Setup, client settings can be configured locally on a specific client.



NOTE

- The Atrust Client Setup 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 Atrust Client Setup console. For a detailed list of client settings that are only locally available, please refer to section "4.2 Client Settings at a Glance" on page 119.

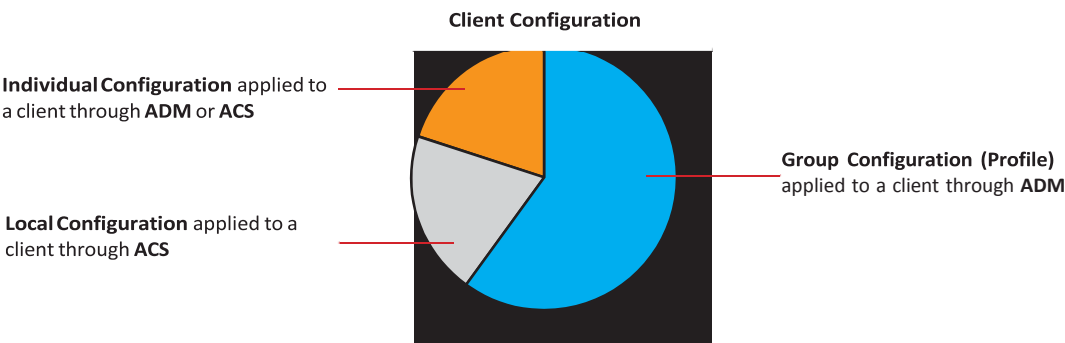
Group Configuration and Individual Configuration

Atrust Device Manager 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 Atrust Client Setup, 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	Page
Local	Local configuration	Atrust Client Setup (ACS)	4.2	119
			4.5	124
	Individual configuration	Atrust Client Setup (ACS)	4.2	119
			4.5	124
Remote	Group configuration	Atrust Device Manager (ADM)	3.4.12	69
	Individual configuration	Atrust Device Manager (ADM)	3.4.14	75

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

Locking the Setting Values

Atrust Device Manager also allows you to lock a setting value. When a setting value is locked, the gray lock icon of the setting value will become the secured blue (🔒) or orange (🔒) lock icon. You are not allowed to lock a setting value with Atrust Client Setup when you manage client settings locally on a client.

In Atrust Device Manager, a blue lock icon indicates that the current value of the corresponding setting item comes from a group configuration; an orange lock icon then indicates that the value or data comes from an individual configuration.

3.4.10 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.

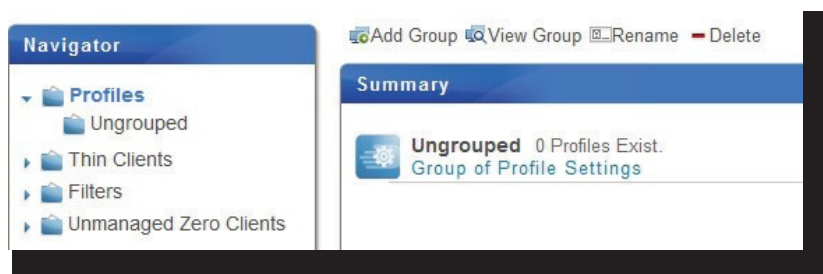


NOTE

- 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:

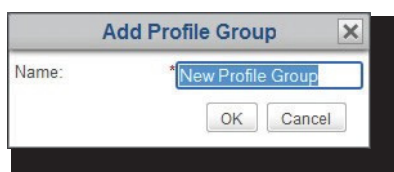
1. On **Thin Clients** tab, click **Profiles**.
2. The Profile Group list appears.



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.

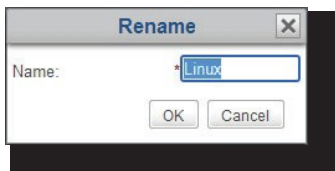


3.4.11 Managing Setting Profile Groups

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.

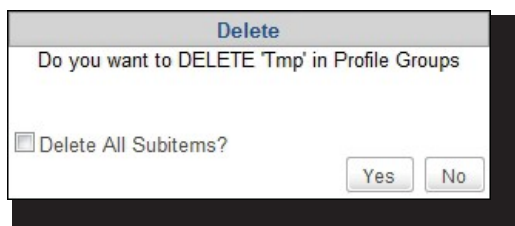


4. Type in the new name for the profile group, and then click **OK** to confirm.

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.



- To keep all setting profiles in this group, leave **Delete All Subitems** cleared, and then click **Yes** to confirm. All setting profiles in this group will be moved to **Ungrouped** (the system default).
- To delete all setting profiles in this group as well, select **Delete All Subitems**, and then click **Yes** to confirm. All setting profiles in this group will be removed.



NOTE

- 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.

3.4.12 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 "3.4.9 Client Settings" on page 65.

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:

- 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 "3.4.10 Creating Setting Profile Groups" on page 67.

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



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

Add

Name:

Description:

Platform:

Model:

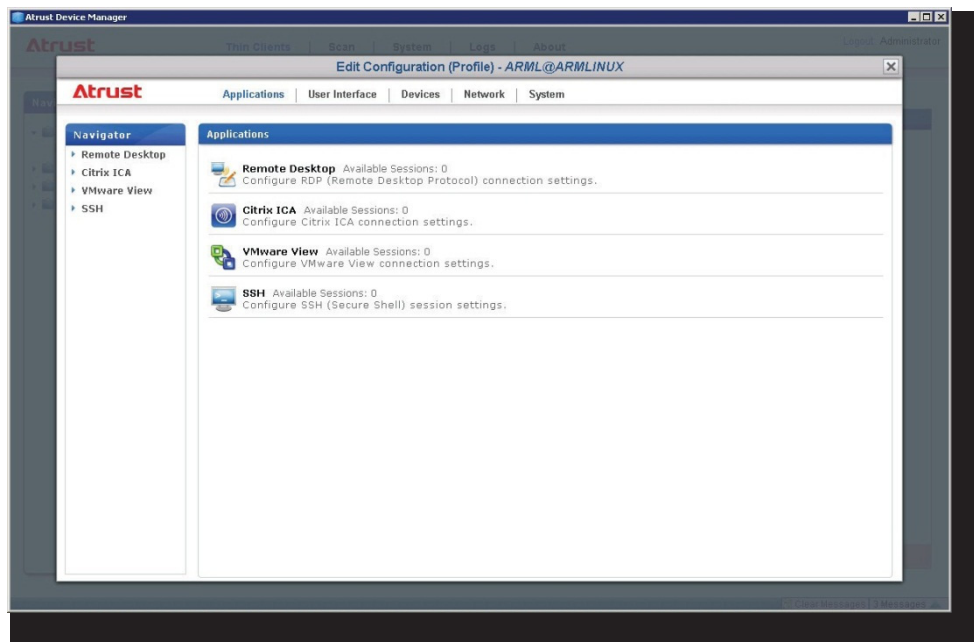


NOTE

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

- 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.



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



NOTE

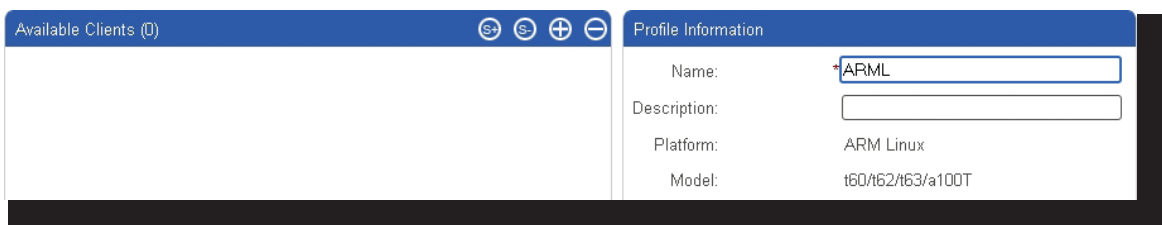
- The Edit Configuration window for the profile (group configuration) is just like a remote version of Atrust Client Setup on a client. You can simply edit client settings for this setting profile through this window. For detailed instructions on how to configure client settings, please refer to "Chapter 4 Configuring Client Settings" on page 117.


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

STEP 2: Specify the applicable scope of the setting profile

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

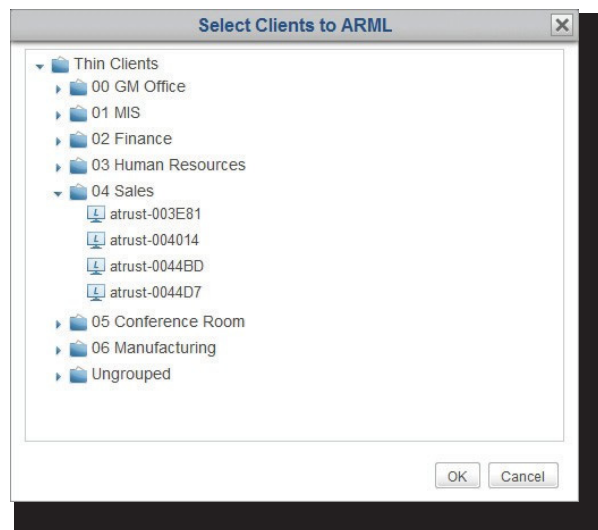
- Click to select the newly created profile, and then click **Edit** on the top of the Profile list to specify the applicable scope of the profile.
- Both the Profile Information and Available Clients panes appear in Management area.



- 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.

- 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.



NOTE

- 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 "3.4.4 Creating Client Groups" on page 60 and "3.3.3 Client Detection and Management" on page 51 separately.
- 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 "3.4.16 Pushing Settings to Clients through Your Local Network" on page 79.

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.



NOTE

- Only a well-defined setting profile is actually used for remote configuration of multiple clients. If the applicable scope of a setting profile is not specified, the profile (group configuration) does not affect any client.
- From now on, we will call a client configuration set up by applying a shared setting profile a **group configuration**.

3.4.13 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	Num. of TCs
A-t60	ARMLINUX	t60/t62/t63	Policy A wt. t60	0
B-t60	ARMLINUX	t60/t62/t63	Policy B wt. t60	0
C-t60	ARMLINUX	t60/t62/t63	Policy C wt. t60	1
D-t60	ARMLINUX	t60/t62/t63	Policy D wt. t60	0

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.
 - 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.



NOTE

- For detailed instructions on the adjustment of client settings or profile information, please refer to section "3.4.12 Creating Client Setting Profiles" on page 69.

5. To adjust the applicable scope of this profile, use to make desired changes, and then click **Save** to apply.

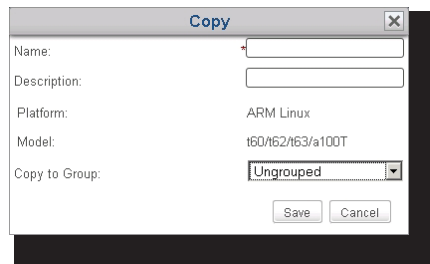
Button	Description
	Click to select all clients in the client list.
	Click to unselect all clients in the client list.
	Click to add new clients.
	Click to remove the selected clients.

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.
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.


**NOTE**

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

5. Provide the required data, and then click **Save** to confirm.
6. The Edit Configuration window for the profile (group configuration) appears.


**NOTE**

- The following steps are similar to those for creating a new setting profile. More information, including both screenshots and notes, can be found in section "3.4.12 Creating Client Setting Profiles" on page 69.

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**

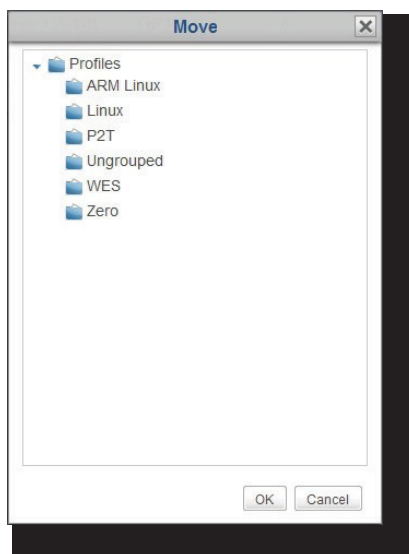
- If you create a new profile by copying a well-defined setting profile, only the part of client settings is copied. The applicable scope of the original profile is not included.

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

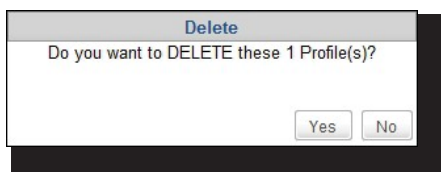


5. Click to select the desired profile group, and then click **OK** to confirm.
6. The selected setting profile is moved to the desired profile group.

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.

3.4.14 Using Individualized Client Settings

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

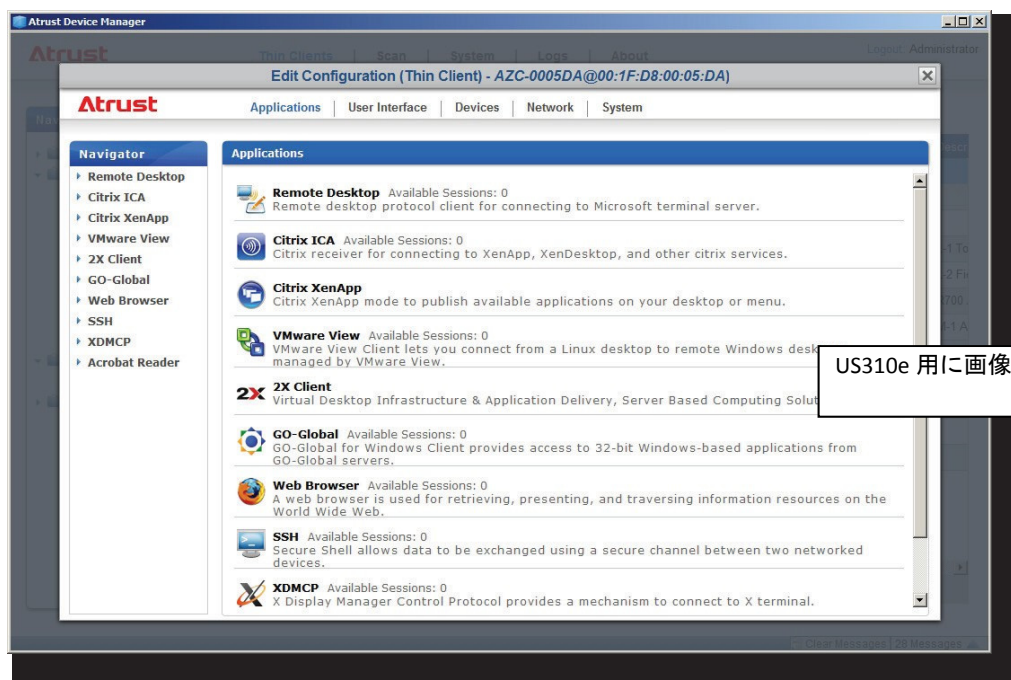


NOTE

- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 65.
- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 83.

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.

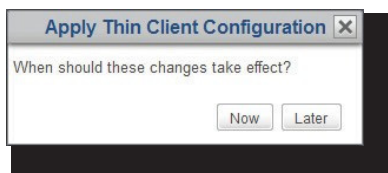


5. Use this window to edit the individual configuration.

**NOTE**

- The Edit Configuration window is just like a remote version of Atrust Client Setup. 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 "3.4.15 Using Hybrid Client Settings" on page 77 for more details). For detailed instructions on how to configure specific client settings, please refer to "Chapter 4 Configuring Client Settings" on page 117.

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 using the **Pushing Settings** feature.

3.4.15 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 "3.4.9 Client Settings" on page 65.

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.
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.



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 "3.4.12 Creating Client Setting Profiles" on page 69.

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 Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 83.

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 "3.4.14 Using Individualized Client Settings" on page 75.

3.4.16 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 Atrust Device Manager. You can then configure client settings remotely through your local network.



NOTE

- Some settings can only be configured locally on clients. See section "3.4.9 Client Settings" on page 65 and "Chapter 4 Configuring Client Settings" on page 117 for more details.

Pushing Settings to a Client

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



NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to **pull client settings from all managed clients** for Atrust Device Manager **before** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 83.

- 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.
- The Client list appears.

<div> Delete Edit Edit Configuration Command Select All Unselect All </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

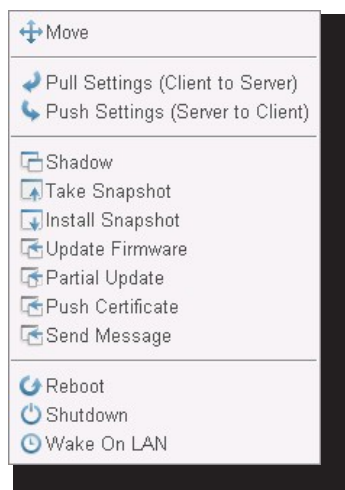
- Click to select the desired client, and then click **Command** on the top of the Client list.



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 "3.4.8 Understanding Client Status Icons" on page 64.

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

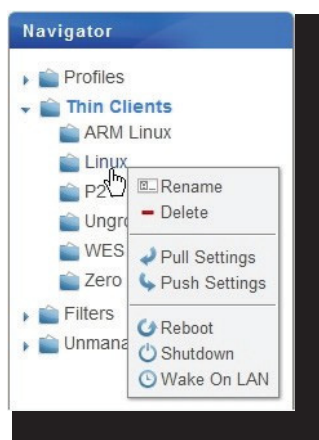
To push settings to a client group, please do the following:



NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to **pull client settings from all managed clients** for Atrust Device Manager **before** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 83.

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**.



3. The Pushing Settings window appears showing the progress and result of pushing 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 "3.4.8 Understanding Client Status Icons" on page 64.

4. After completion, click **Close** to exit.
5. 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

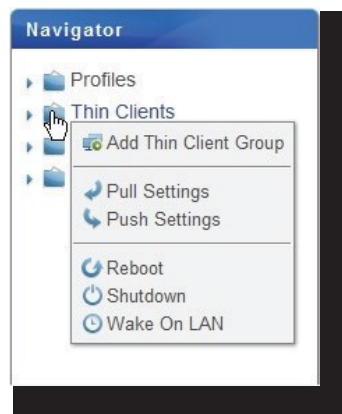
To push settings to all client groups, please do the following:



NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to **pull client settings from all managed clients** for Atrust Device Manager **before** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 83.

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



2. Click to select **Push Settings**.
3. The Push Settings window appears showing the progress and result of pushing settings.



NOTE

- Ensure that all 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 "3.4.8 Understanding Client Status Icons" on page 64.

4. After completion, click **Close** to exit.
5. Check the status of clients through the Status icon in front of clients. If needed, restart clients to complete the configuration changes on clients.

3.4.17 Pulling Client Settings through Your Local Network

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



NOTE

- Some settings can only be configured locally on clients. These settings cannot be retrieved from clients and stored in Atrust Device Manager. See section "3.4.9 Client Settings" on page 65 and "Chapter 4 Configuring Client Settings" on page 117 for more details.

Pull Settings from a Client

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

- 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.
- The Client list appears.

	Delete		Edit		Edit Configuration		Command		Select All		Unselect All
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description				
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A					
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A					

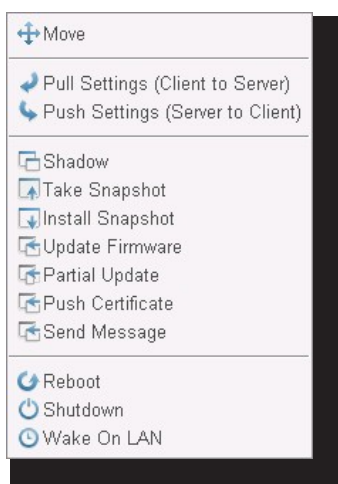
- Click to select the desired client, and then click **Command** on the top of the Client list.



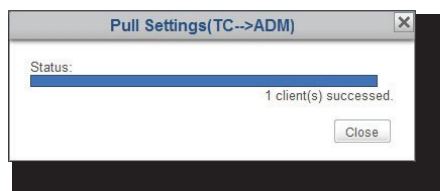
NOTE

- 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 pull settings from 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 "3.4.8 Understanding Client Status Icons" on page 64.

- 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.

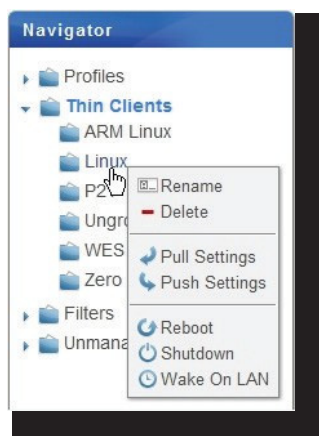


9. After completion, click **Close** to exit.

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**.



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



NOTE

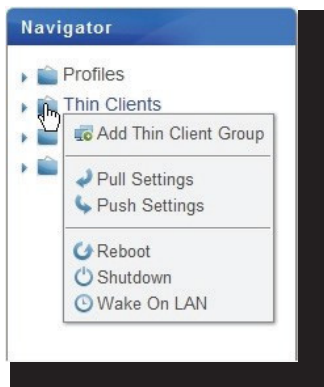
- Ensure that clients in the selected group are all powered up. Otherwise you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 64.

4. 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.



2. Click to select **Pull Settings**.
3. The Pull Settings window appears showing the progress and result of retrieving settings.



NOTE

- Ensure that all clients are powered up. Otherwise, you may fail to pull settings from 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 "3.4.8 Understanding Client Status Icons" on page 64.

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

3.4.18 Pushing Certificates of Remote Computers to Clients

**WARNING**

- This feature is not supported.

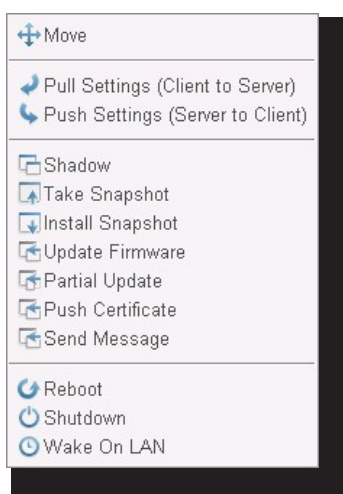
3.4.19 Sending Messages to Clients

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.

<div> Delete Edit Edit Configuration Command Select All Unselect All Export </div>								
Name	IP Address	Mac Address	Model	Firmware	Profile	Description	Asset ID	
atrust-0038C8	192.168.0.117	00:1F:D8:00:38:C8	t170W7E	WES7 1.57-INTL	N/A			
atrust-003EC4	192.168.0.101	00:1F:D8:00:3E:C4	t60	ARM Linux 2.62-PREI	N/A			
atrust-00CDD9	192.168.0.109	00:1F:D8:00:CD:D9	t220W	WES8 0.18-INTL	N/A			

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 Context:

OK

Cancel

7. Type in the data, and then click **OK** to confirm.
8. The message will be sent to the desired client(s).

3.4.20 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

	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-003E81	192.168.50.111	00:1F:D8:00:3E:81	t60	ARM Linux 2.52-INTL	N/A	
	atrust-004014	192.168.50.180	00:1F:D8:00:40:14	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	

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-003E81)

Name:
 Description:
 Profile:
 Asset ID:

IP Address:
 MAC Address:
 Serial Number:
 Model Name:
 Last Boot Time:
 Firmware:

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

- 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.



NOTE

- 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.

3.4.21 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.

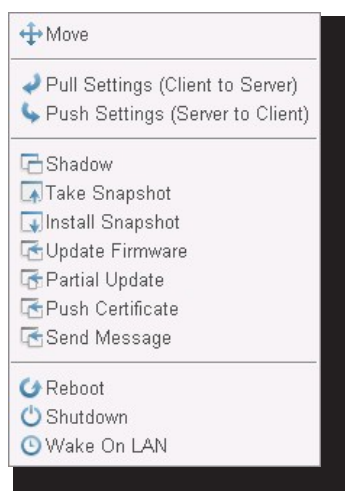
Rebooting a Client through Your Local Network

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 </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-003E81	192.168.50.111	00:1F:D8:00:3E:81	t60	ARM Linux 2.52-INTL	N/A	
	atrust-004014	192.168.50.180	00:1F:D8:00:40:14	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

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



4. Click to select **Reboot**.



NOTE

- To select more than one client, Ctrl-click to select the desired clients.



WARNING

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

5. 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.

6. After completion, the Status icon will indicate the client is on-line again.

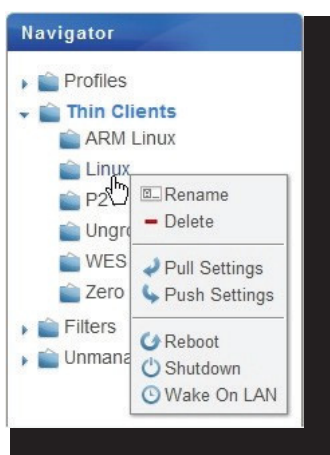
**NOTE**

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

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**.

**WARNING**

- 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.

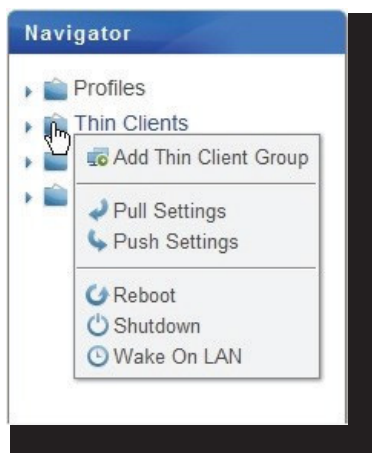
**NOTE**

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

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**.



WARNING

- Ensure that no important tasks are performed on clients.

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 "3.4.8 Understanding Client Status Icons" on page 64.

3.4.22 Shutting Down Clients through Your Local Network

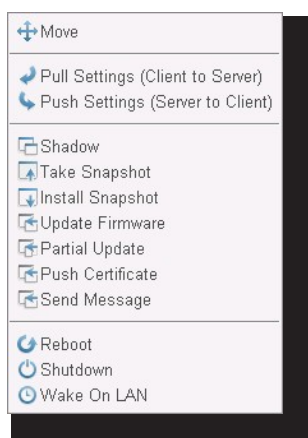
Shutting Down a Client through Your Local Network

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 </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

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



4. Click to select **Shutdown**.



NOTE

- To select more than one client, Ctrl-click to select the desired clients.



WARNING

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

5. 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.
6. After completion, the Status icon will indicate the client is off-line.



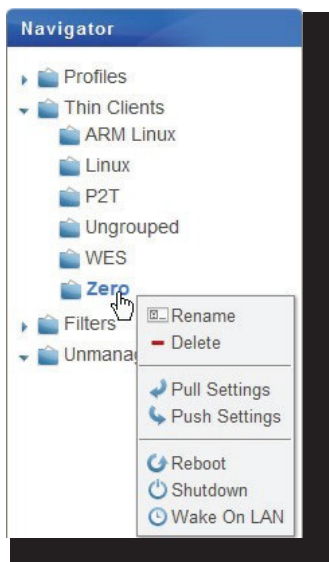
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

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.



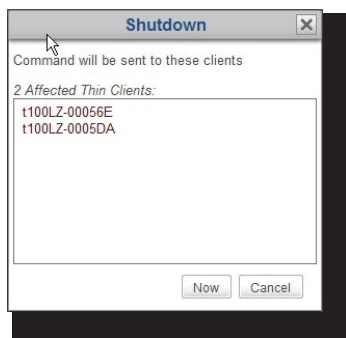
3. Click to select **Shutdown**.



WARNING

- 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.



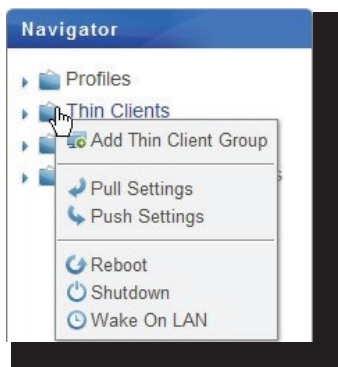
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

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.



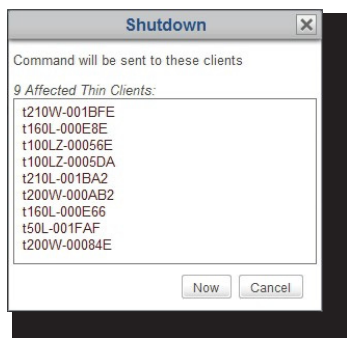
2. Click to select **Shutdown**.



WARNING

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

3. The Shutdown window appears prompting for confirmation.



4. 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.
5. 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 "3.4.8 Understanding Client Status Icons" on page 64.

3.4.23 Waking Clients through Your Local Network

The Wake on LAN feature enables you to wake multiple clients through your local network if clients are connected to power outlets and the local network.

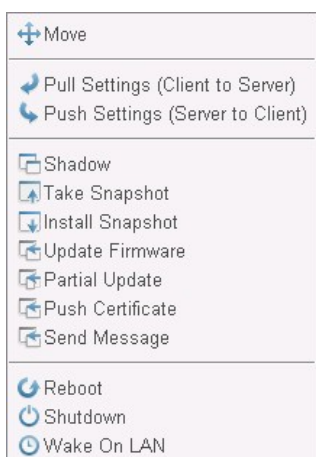
Waking a Client through Your Local Network

To wake 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 </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

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.

4. Click to select **Wake On LAN**.
5. The selected client is powered up.
6. After completion, the Status icon will indicate the client is on-line.



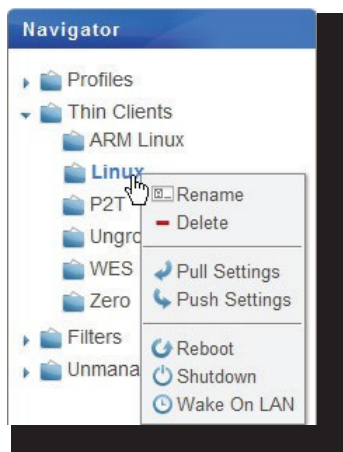
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

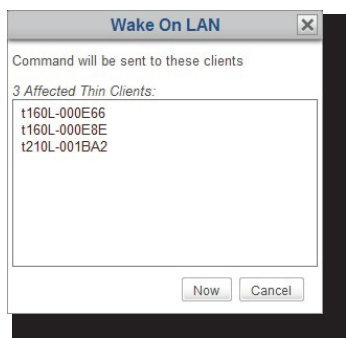
Waking a Client Group through Your Local Network

To wake 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 appears prompting for confirmation.



5. Click **Now** to confirm.
6. Each client in this group is powered up.
7. After completion, the Status icons will indicate clients of this group are on-line.



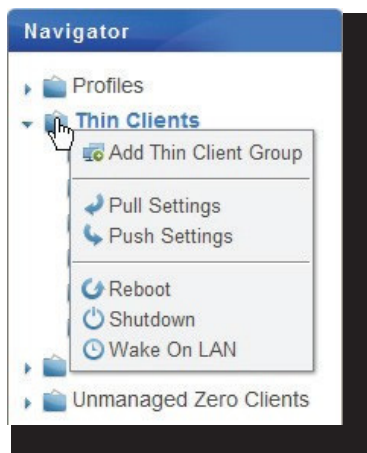
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

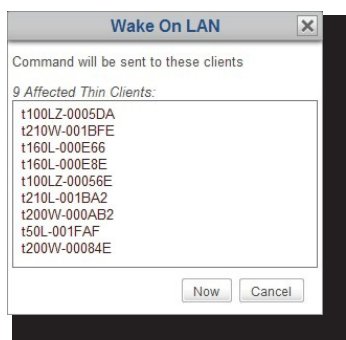
Waking All Client Groups through Your Local Network

To wake 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. After completion, the Status icons will indicate all managed clients are on-line.



NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 64.

3.4.24 Updating Client Firmware

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



NOTE

- Updating client firmware will NOT erase any client configuration.

- 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.
- The Client list appears.

<div> Delete Edit Edit Configuration Command Select All Unselect All </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t160L-000E66	192.168.11.59	00:1F:D8:00:0E:66	t160L	Atrust Linux 1.29-INTL	t160L Pro	
	t160L-000E8E	192.168.11.63	00:1F:D8:00:0E:8E	t160L	Atrust Linux 1.25-INTL	t160L Light	
	t210L-001BA2	192.168.11.136	00:1F:D8:00:1B:A2	t210L	Atrust Linux 1.29-INTL	t210L Pro	

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



NOTE

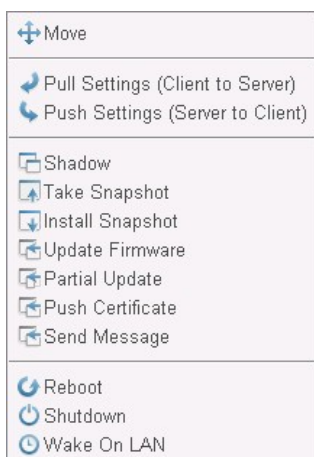
- To select more than one client, Ctrl-click to select the desired clients.



WARNING

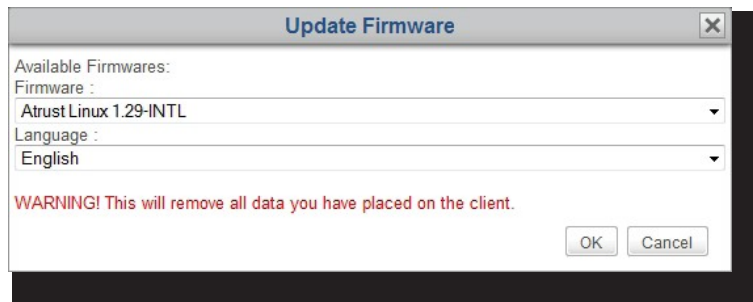
- Ensure that no important tasks are performed on the selected clients.

- The Command menu appears.



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

3.4.25 Installing Software Packages

To install a software package for your 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.

<div> Delete Edit Edit Configuration Command Select All Unselect All </div>							
	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t200W-00084E	192.168.11.109	00:1F:D8:00:08:4E	t200W	WES 1.13-INTL	t200W Pro	
	t200W-000AB2	192.168.11.72	00:1F:D8:00:0A:B2	t200W	WES 1.13-INTL	t200W Shadow	
	t210W-001BFE	192.168.11.139	00:1F:D8:00:1B:FE	t210W	WES 1.13-INTL	t210W Light	

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



NOTE

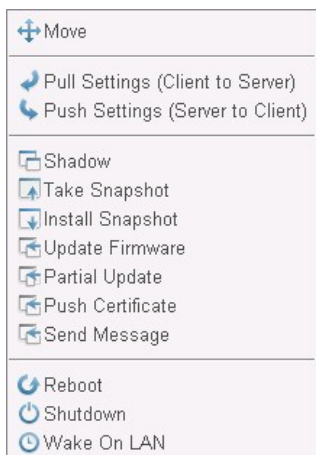
- To select more than one client, Ctrl-click to select the desired clients.



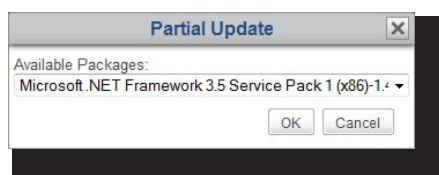
WARNING

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

4. The Command menu appears.



5. Click to select **Partial Update**.
6. The Partial Update window appears prompting you to select the software package.



7. Click the drop-down menu to select the desired software package, and then click **OK** to confirm.
8. 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.
9. After completion, the desired software package is installed on the selected client.

**TIP**

- To check remotely if the installation is completed, select the client, and then click **Edit** to view the basic information about a client. For more details, refer to section "3.4.20 Editing or Viewing the Basic Information about a Client" on page 88.

3.4.26 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.

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

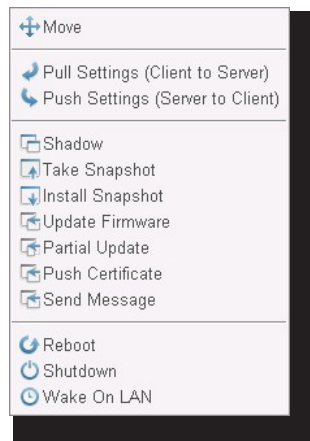
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click to select the client group to which the desired client belongs.
2. The Client list appears.
3. Click to select the desired client, and then click **Command** on the top of the Client list.



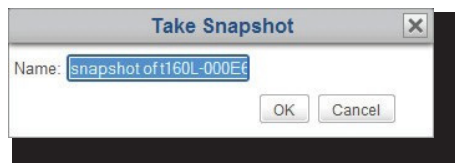
NOTE

- 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.
8. 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.
9. After completion, the system snapshot is added to the Snapshot list.



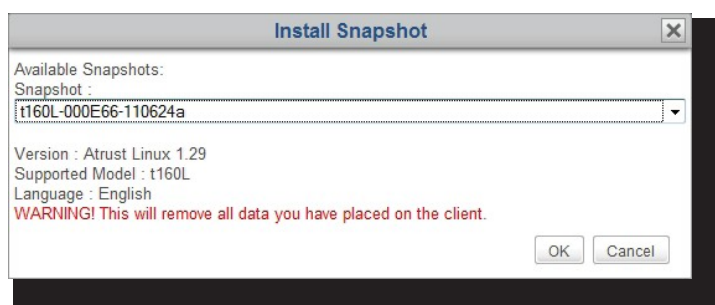
NOTE

- To access the Snapshot list, click **System** tab, and then click **Deployment > Snapshot**.
- Refer to section "3.2.7 Managing Client Snapshots" on page 36 for instructions on how to manage your snapshots.

3.4.27 Restoring Client Snapshots

To restore a system copy of 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 **Command** on the top of the Client list.
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. 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.
9. After completion, the client is restored to the desired state.

3.4.28 Assisting a Client User Remotely

The **Shadow** feature enables you to remotely assist client users in resolving problems or configuring local settings. You can remotely monitor and control a client just like a local client user.

**NOTE**

- Ensure that you have installed the Java software or Java Runtime Environment. It is required to execute the **Shadow** feature.

To remotely assist a client user, please do the following:

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

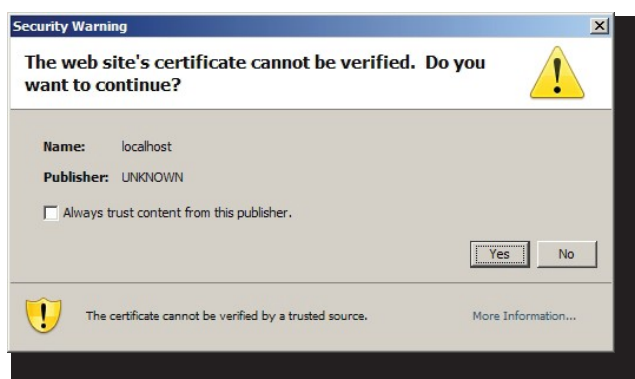
**NOTE**

- It is not allowed to select multiple clients while executing the **Shadow** feature. However, you could do it one by one for multiple clients.

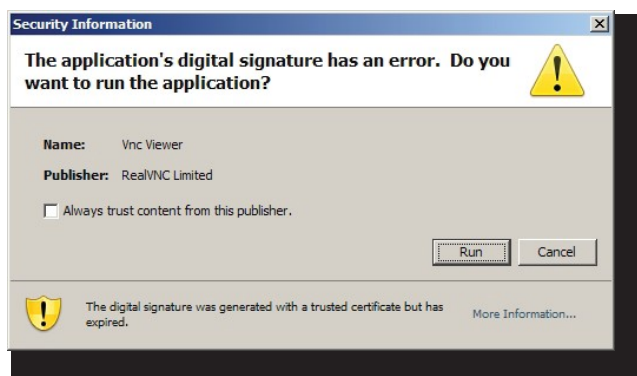
4. The Command menu appears.
5. Click to select **Shadow**.
6. The Java software is launched displaying an animated picture on the screen as below.



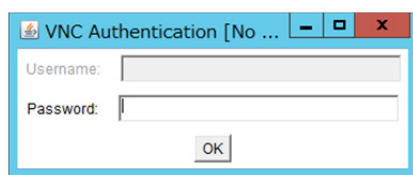
7. A warning message appears with the certificate information. Click **Yes** to continue.



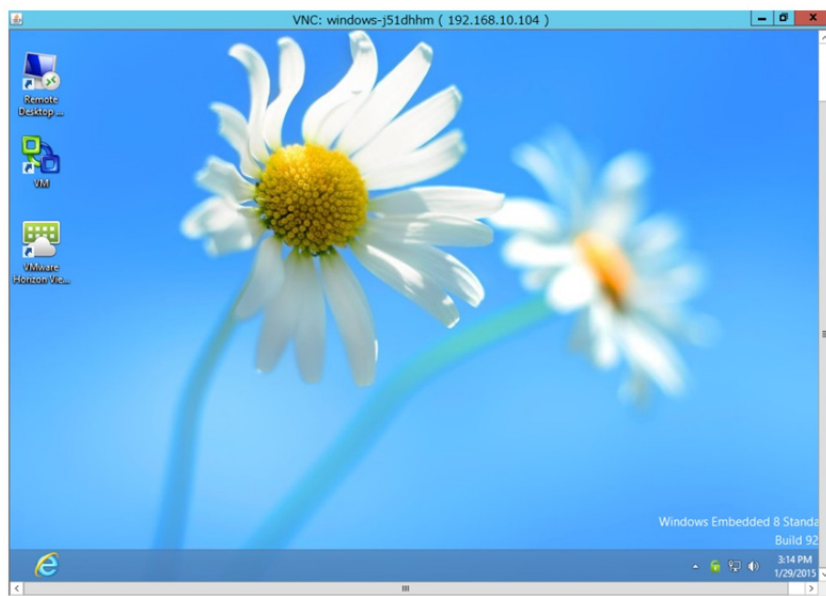
8. Another warning message appears with the information about the application digital signature. Click **Run** to continue.



9. The VNC Authentication window may appear prompting you for the Shadow password.



10. Type in your Shadow password, and then click **OK** to confirm.
11. A window pops up with the desktop screen of the selected client.



12. Now you can remotely monitor and control the client to assist the client user.

**NOTE**

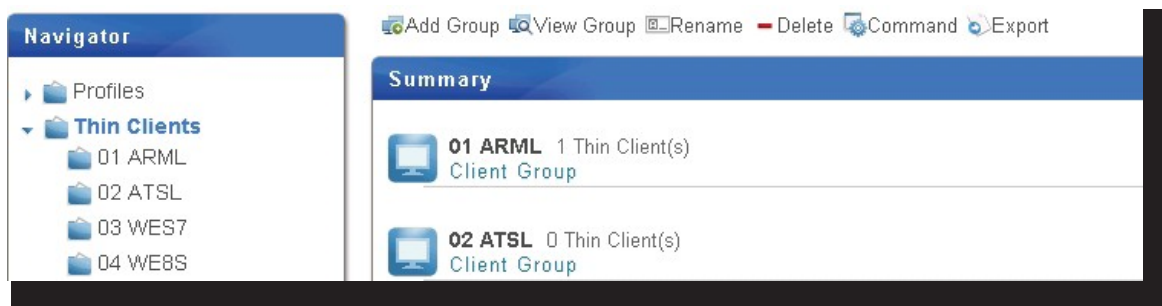
- The user of the client could also control the system with the local keyboard and mouse.

3.4.29 Exporting Client Data

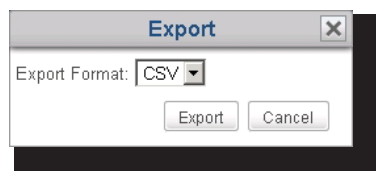
The **Export** feature available on the top of the Client Group list or the Client list allows you export an inventory of managed clients.

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

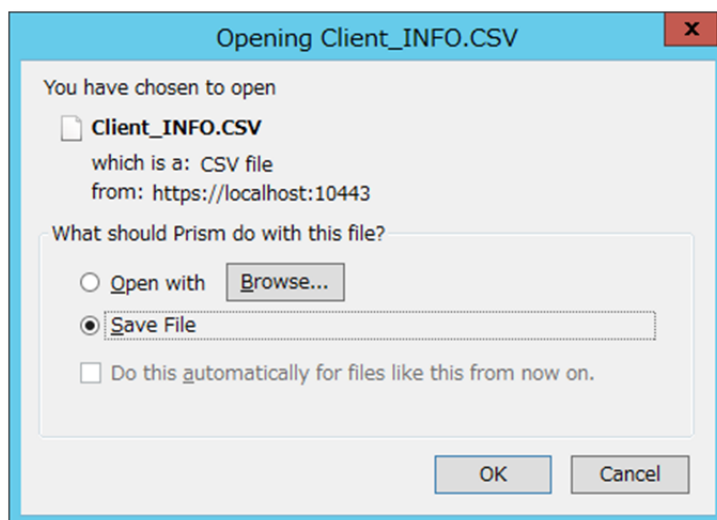
1. On **Thin Clients** tab, click to select the desired group in the Navigation area.
2. Click **Export** on the top of the Client Group list or the Client list.



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 save or open the generated file. Click to select the desired option, and then click **OK** to confirm.



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


At the bottom of each Profile, Client, Zero Client, or Log list, you can access Quick Search to help you dig out the profiles, clients, or event logs.

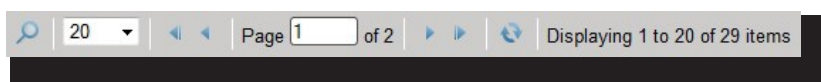


NOTE

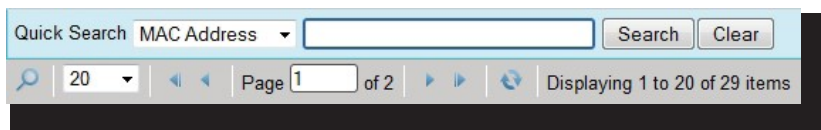
- Event logs will be introduced on section "3.5.1 Logs Tab Overview" on page 111.
- You can also use filters to find out the desired clients within the managed clients. For details, please refer to section "3.4.31 Digging Out Clients with Filters" on page 108.

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

1. Open the Profile, Client, Zero Client, or Log List.
 - On **Thin Clients** tab, click **Profiles** or **Thin Clients**, and then click the group to which the Profile or Client list belongs to open the Profile or Client list.
 - On Atrust Device Manager, click on **Logs** tab to open the Log list.
2. The Profile, Client, Zero Client or Log list appears in Management area.
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.



NOTE

- You can also use Quick Search to dig out clients within managed clients and unmanaged zero clients. For details, please refer to "3.4.30 Digging Out Profiles, Clients, or Event Logs with Quick Search" on page 107.

3.4.31 Digging Out Clients with Filters

Atrust Device Manager 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.



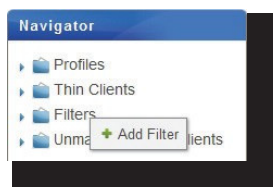
NOTE

- You can also use Quick Search to dig out clients within managed clients and unmanaged zero clients. For details, please refer to "3.4.30 Digging Out Profiles, Clients, or Event Logs with Quick Search" on page 107.

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

Filter Name: *

Field Name	Operator	Value	Action
Name	equals		Add

Available Filter Conditions

Preview Save Cancel

Filter Preview

Name	Group
Filter Preview	

5. Type in the desired name for this filter.

- 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 "3.4.20 Editing or Viewing the Basic Information about a Client" on page 88 for detailed instructions.

- Click **Add** to add a condition to a filter.
- Repeat steps 5 through 7 to add a new condition.
- Click **Preview** to view the result of a filter. The result is displayed in the Filter Preview pane.
- 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:

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

The screenshot shows the Atrust Device Manager web interface. The top navigation bar includes 'Thin Clients', 'Scan', 'System', 'Logs', and 'About'. The 'Thin Clients' tab is active, and the 'Filters' section in the left sidebar is expanded. The main area displays a table of clients filtered by IP address (192.168.11.x).

Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
t200W-00084E	192.168.11.109	00:1F:D8:00:08:4E	t200W	WES 1.13-INTL	t200W Shadow	
t200W-000AB2	192.168.11.77	00:1F:D8:00:0A:B2	t200W	WES 1.12-INTL	t200W Pro	
t210L-001BA2	192.168.11.136	00:1F:D8:00:1B:A2	t210L	Atrust Linux 1.29-INTL	t210L Pro	
t210W-001BFE	192.168.11.139	00:1F:D8:00:1B:FE	t210W	WES 1.13-INTL	t210W Light	
t50L-001FAF	192.168.11.125	00:1F:D8:00:1F:AF	t50	Atrust Linux 1.35-INTL	t50L Pro	

The interface also shows a 'Navigator' sidebar with categories like Profiles, Thin Clients, and Filters. The bottom status bar indicates 'Page 1 of 1' and 'Displaying 1 to 5 of 5 items'.

3.4.32 Managing Your Filters

Deleting a Filter

To delete a filter, please do the following:

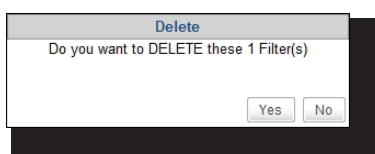
1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.
3. Click to select the desired filter, and then click **Delete** on the top of the Filter list.



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:

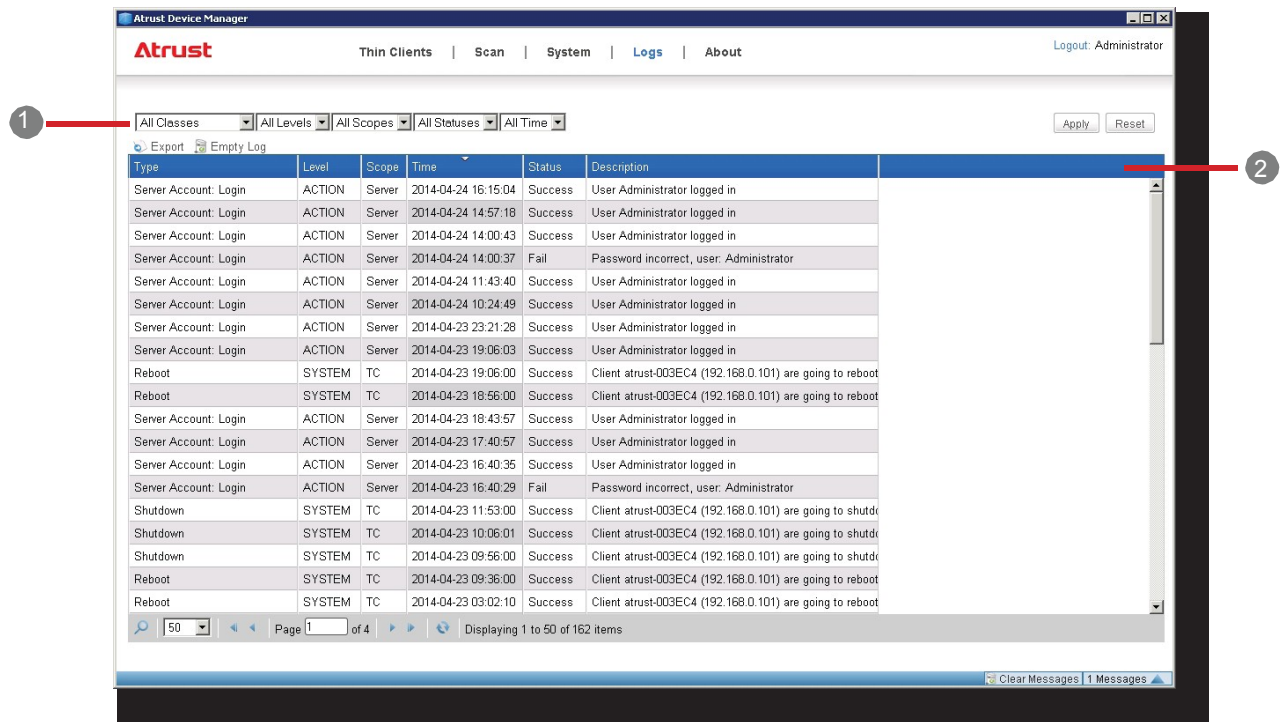
1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.
3. Click to select the desired filter, and then click **Edit** on the top of the Filter list.
4. The Filter Condition List and Filter Preview panes appear in Management area.
5. Adjust conditions 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 Atrust Device Manager.

Logs Tab Overview



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.

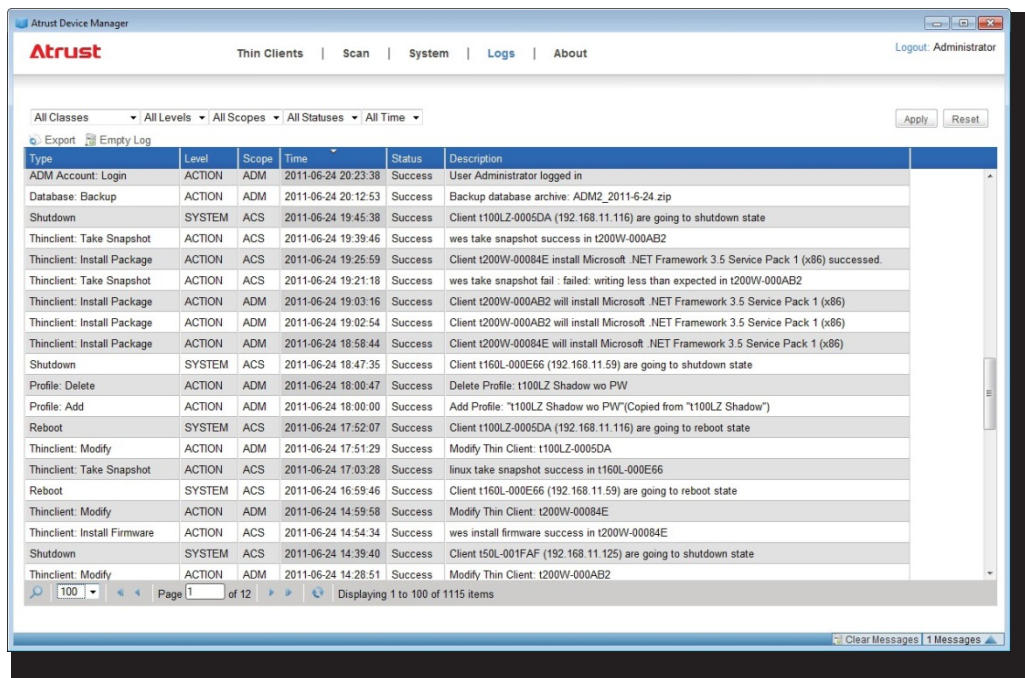
3.5.2 Available Tasks at a Glance

No.	Available Task	Section	Page
1	Viewing your event logs	3.5.3	112
2	Exporting your event logs	3.5.4	113
3	Emptying your event logs	3.5.5	114

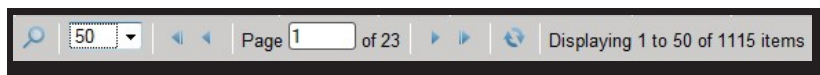
3.5.3 Viewing Event Logs

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

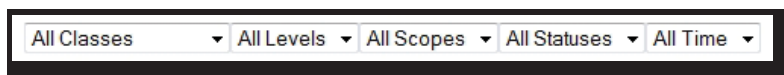
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.



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



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



3.5.4 Exporting Event Logs

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

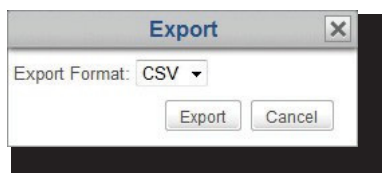
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.
 - To export log entries within a specific scope, click the drop-down menus to define the scope, and then click **Apply** to confirm.
 - To export all log entries, ensure that, on drop-down menus, the selected options do not limit the scope of the Log list.



NOTE

- 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 between opening or saving the exported file.
7. Click to select **Save File**, and then click **OK**.
8. In the opened window, locate the desired directory to save the file.

3.5.5 Emptying Event Logs

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



NOTE

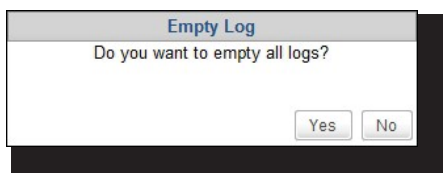
- You cannot partially delete log entries.



WARNING

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

1. On Atrust Device Manager, 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 Atrust Device Manager.



NOTE

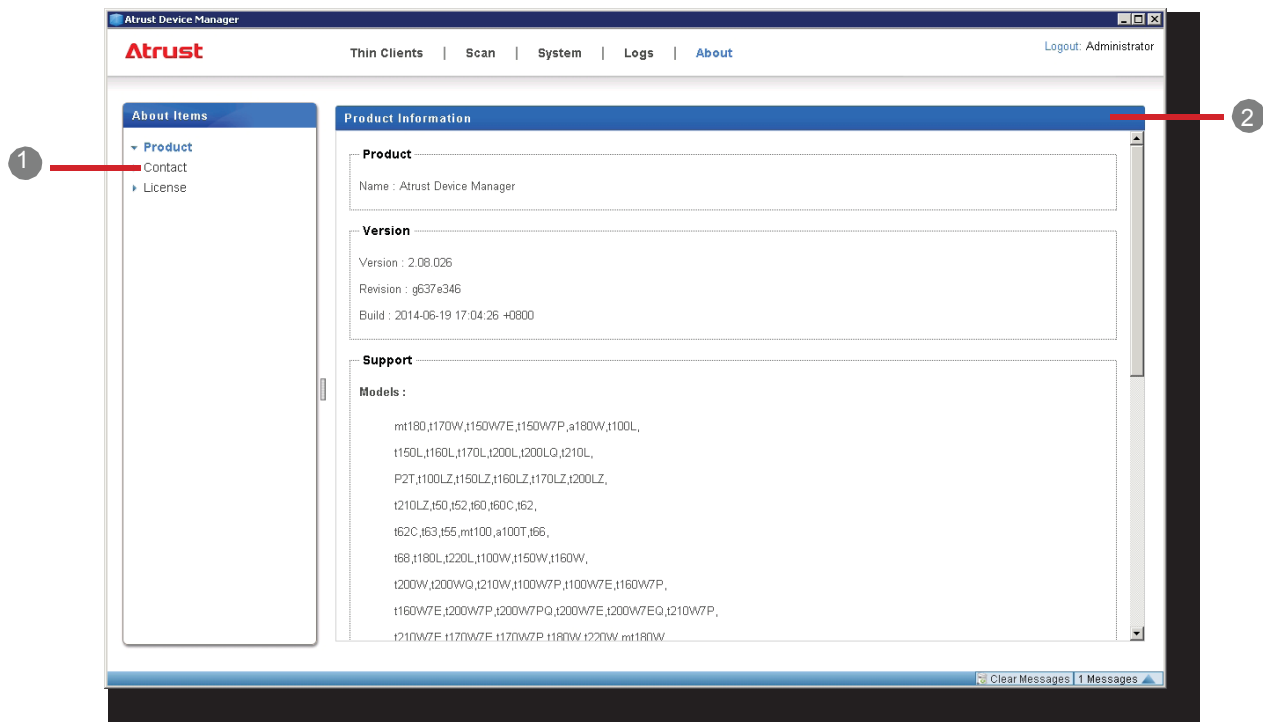
- A new log entry about emptying log will be added to the Log list.

3.6 Viewing Software Information

3.6.1 About Tab Overview

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

About Tab Overview



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	Page
1	Viewing information on Atrust Device Manager	3.6.3	116
2	Viewing Atrust contact information	3.6.4	116
3	Viewing Atrust Software License Agreement	3.6.5	116

3.6.3 Viewing Information on Atrust Device Manager

To view information on Atrust Device Manager, please do the following:

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

3.6.4 Viewing Atrust Contact Information

To view Atrust 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 Atrust Software License Agreement

To view Atrust Software License Agreement, please do the following:

1. On **About** tab, click **License** in Navigation area.
2. Atrust 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 Atrust Device Manager and Atrust Client Setup

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 Configuring Client Settings with Atrust Client Setup

How to configure client settings with Atrust Client Setup

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.



NOTE

- The available **tabs** and **setting items** may vary, depending on: the **client model**, **firmware version**, and the used **operating system**.
- Some setting items are **only available locally on client devices**. You can adjust those settings through Atrust Client Setup. In the table below, settings that are only available locally on clients are marked with an asterisk (*).

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for Remote Desktop sessions.
	Citrix ICA		Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create shortcuts on the local desktop and START menu for ICA sessions.
	VMware View		Click to configure VMware View connection settings and create shortcuts on the local desktop and START menu for View sessions.
	Web Browser		Click to configure general (for web-based clients only) or specific browser session settings. A desktop shortcut is created for specific browser sessions launched with the desired initial web page.
User Interface	Desktop		Configure desktop icons.
Devices	USB Storage		Click to configure settings for USB storage devices.
	Audio		Click to configure settings for audio devices.
System	Password		Configure administration privileges and remote assistance settings.
	Firmware Update *		Click to update firmware through the network. This feature is only applicable when this client is managed by the Atrust Device Manager console.
	Snapshot *		Click to take a snapshot (system copy at a specific point of time) for your client device, which you can use for mass deployment, system backup, and recovery.
	Appliance Mode		Click to enable/disable the Appliance mode to allow/disallow the automatic Remote Desktop session. In Appliance mode, the client starts up with the desired Remote Desktop session and shuts down when the user logs off the session.
	UWF		Click to configure UWF (Unified Write Filter) settings. As a sector-based write filter, UWF will intercept all write attempts to a protected volume and redirect those attempts to a RAM cache. All system changes only affect the session where the changes are made. After restart, all changes are discarded.

4.3 Editing or Adjusting a Group Configuration

On Atrust Device Manager, 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.

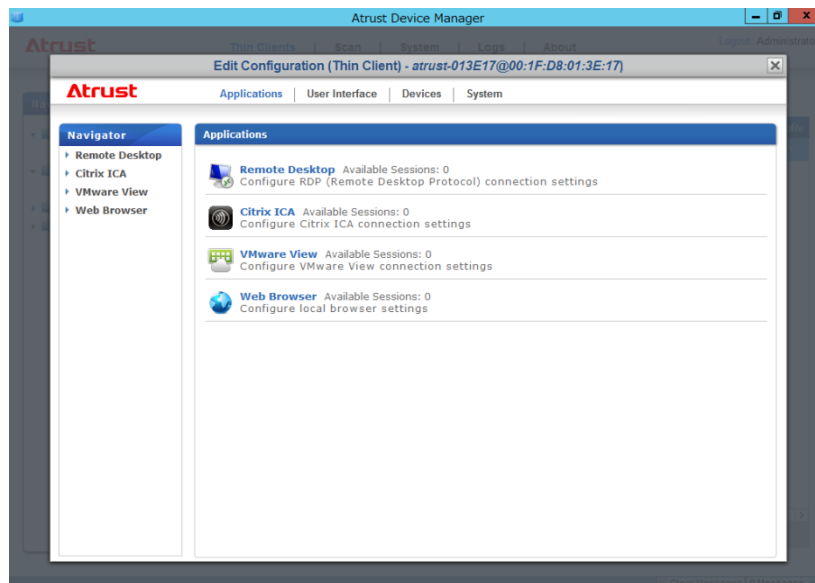



NOTE

- In this section, we will focus on the editing or adjusting of a profile (group configuration) in greater detail. For general instructions on how to create a profile (group configuration) or on how to open the Edit Configuration window for profile, please refer to section "3.4.12 Creating Client Setting Profiles" on page 69.
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 65.
- 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, please refer to section "4.4 Editing or Adjusting an Individual Configuration" on page 122.

To configure a setting in the Edit Configuration window (for a group configuration), please do the following:


1. In the Edit Configuration window for a profile, click the tab to which the desired setting belongs.



2. Click on the icon of the desired setting.
3. Click **Add** to add an entry for that setting if necessary.
4. On the detailed setting page(s), click on the gray lock icon  located close to a setting item to activate the item.



NOTE

- The lock icon will become orange  when you click to activate the item.
- When a lock icon becomes orange, the corresponding setting value is locked on clients and cannot be changed locally through Atrust Client Setup.

5. Choose or type in the desired setting values.

6. After the editing of setting values is completed, click **Save** at the bottom of that setting page to save the changes.
7. Repeat steps 1 through 6 to edit other settings.

**NOTE**

- Other values of invalid setting items will not be applied to clients.
- You need to push settings to target group of clients for the changes to take effect.

4.4 Editing or Adjusting an Individual Configuration

On Atrust Device Manager, 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 "3.4.14 Using Individualized Client Settings" on page 75.

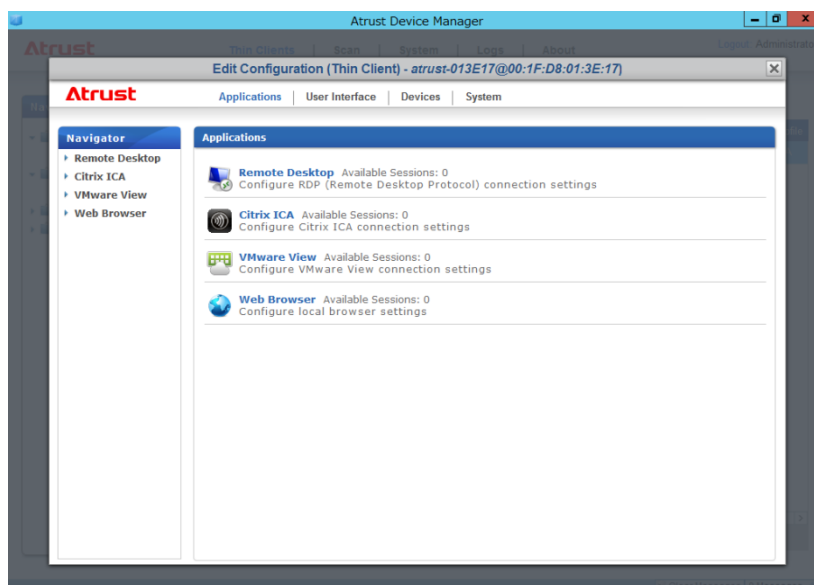


NOTE

- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 65.
- 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.

To configure a setting in the Edit Configuration window (for a client), please do the following:




1. In the Edit Configuration window for a client, click the tab to which the desired setting belongs.



2. Click on the icon of the desired setting.
3. Click **Add** to add up an entry for that setting if necessary.

4. On the detailed setting page(s), choose or type in the desired setting values.

**NOTE**

- Click on the gray lock  icon located close to a setting item to lock its value. The gray lock will become orange  and secured. When a lock icon becomes orange and secured, the corresponding setting value is locked on the client and cannot be changed locally through Atrust Client Setup.
- 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.
- If you apply a group configuration to a client, all related settings will also be shown in the Edit Configuration window for that client.

5. After the editing of setting values is completed, click **Save** at the bottom of that setting page to save the changes.
6. Repeat steps 1 through 5 to edit other settings.

**NOTE**

- You need to push settings to that client for the changes to take effect.

4.5 Configuring Client Settings with Atrust Client Setup

Atrust Client Setup allows you to configure client settings locally on clients. Additionally, some settings are only available locally on clients and therefore can only be configured through Atrust Client Setup.



NOTE

- For the list of client settings only locally accessible on clients, please refer to section "4.2 Client Settings at a Glance" on page 119.
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 65.

For more information on how to configure client settings locally on clients with Atrust Client Setup, please refer to the User's Manual for a specific thin client model.

Chapter 5 Notes and Restrictions

This chapter describes notes and restrictions on using Atrust Device Manager.

5.1 Synchronizing ADM with ACS Settings

Notes on synchronizing the settings of Atrust Device Manager (ADM) with those of Atrust Client Setup (ACS)

5.2 Adding to and Releasing from Management

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

5.3 Notes on Taking and Installing Snapshots

Notes on the behavior of Default User Account at Snapshot Installation

5.4 Retaining ACS Settings When Updating Firmware and Installing a Snapshot

Notes on retaining ACS settings after firmware update and snapshot installation

5.5 Deactivation (License Activation) After Firmware Update or Snapshot Installation

Notes on deactivation (License Activation) After Firmware Update or Snapshot Installation

5.6 Notes on Accessing the ADM Management Console

Notes on accessing web-based ADM Management Console

5.7 Notes on Using VNC (Remote Shadow)

Notes on using VNC (Remote Shadow)

5.8 Notes on Backup and Restoring ADM Server

Notes on Backup and Restoring ADM Server

5.9 Restrictions

Restrictions on using ADM and known issues

5.1 Synchronizing ADM with ACS Settings

If the administrator changes Atrust Client Setup (ACS) settings on a thin client without doing so as a remote operation from Atrust Device Manager (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.

5.2 Adding to and Releasing from Management

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

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**.



WARNING

- 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.



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.

5.3 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.

5.3.1 Types of Snapshots

Snapshots are divided into deployment type and backup type snapshots. When a deployment type 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. This System Preparation Utility (Sysprep) does not execute in the case of backup type snapshots. A backup type snapshot can be used when a problem has occurred to back up the status before investigating the cause of the problem. A backup type snapshot can only be installed in the terminal where that snapshot was taken. If you install a backup type snapshot in another terminal, that terminal can no longer be used, even if an SID has been assigned, and the license is deactivated.

5.3.2 Behavior of Default User Account at Snapshot Installation

When a deployment type 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.

5.3.3 About Joining a Domain

A deployment type 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.

5.3.4 Limitation of the Number of Snapshots That Can Be Taken

When creating a master image for client deployment task, a deployment type snapshot can be taken multiple times. "Windows rearm count" is consumed once when taking a snapshot once. Please be careful that "Windows rearm count" is not zero. If the Rearm count is 0, a fatal error occurs while trying to run Sysprep. Rearm count is 4 at the time of factory shipment.

To confirm the limitation of the number of snapshots that can be taken, enter the following command from the command prompt in administrator account.

```
slmgr -dlv
```

5.4 Retaining ACS Settings When Updating Firmware and Installing a Snapshot

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

The ACS settings of the thin client from which the snapshot is taken are retained.

5.5 Deactivation (License Activation) After Firmware Update or Snapshot Installation

Thin client has been activated at the factory. But if, by using Atrust Device Manager (ADM) or Atrust Device USB Disk Creator, thin client firmware is updated or snapshot is installed, activation (license activation) is also needed. Please be careful. Please refer to the User's Guide for more details about activation.

5.6 Notes on Accessing the ADM Management Console

Atrust Device Manager (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 (Atrust Device Manager 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.



NOTE

- The self-signed certificate of Atrust Computer Corporation is bound to the ADM site by default. If you want to replace the certificate with a trusted signed certificate in pfx or PKCS#12 format, you will need to convert the certificate by using OpenSSL.

5.7 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 US310e from other VNC client software as well as from Atrust Device Manager. 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.



NOTE

- ADM uses the java plug-in of the web browser for the remote shadow feature. When not using the remote shadow feature, if you want to disable the java plug-in for security reasons, clear the **Enable Java content in the browser** check box on the **Security** tab of **Java Control Panel**.
* In this case, the remote shadow feature can no longer be used.

5.8 Notes on Backup and Restoring ADM Server

A notice about a backup and restoration of the ADM server is indicated here.

5.8.1 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.

- 3.2.7 Managing Client Snapshots
- 3.2.14 Backing Up the Management Database
- 3.2.15 Managing Database Archive Files

5.8.2 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
- 3.2.6 Managing WES Packaging Files
- 3.2.7 Managing Client Snapshots
- 3.2.16 Restoring a Database Archive File

5.9 Restrictions

- 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.
- 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.
- When specifying **Use External Server** in **Deploy Server** for ADM, the URL cannot be an https (SSL) URL.
- 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.
- If other than the default setting is configured for **Window Size** in the option settings for adding or editing Citrix ICA sessions of ADM or ACS, the **Desktop Viewer** toolbar is not displayed. To display the **Desktop Viewer** toolbar, either configure the default setting for **Window Size** or connect to the Citrix ICA session using Citrix Receiver.
- Firmware and packages cannot be registered to a shared folder on the network.
- 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.
- Since a DNS name cannot be used as the server path of ADM, specify the IP address.

- If you select and import a snapshot file by using the **Browse** button, do not click the **Cancel** button. Because data is created when you select the snapshot file, the created data remains in the database even if you cancel the operation. Be sure to complete the import process without canceling it midway and then delete the snapshot. Otherwise, you can no longer register a snapshot file with the same description.
- When exporting a US310e snapshot, 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.
- When the following switching hubs are used, the network may slow down when updating the firmware and installing a snapshot. If the network slows down, the image file may not be downloaded, causing an MD5 checksum error.
 - I-O DATA ETG4-SH8N
 - Logitec LAN-GSW08P/P
 - Logitec LAN-GSW16P/M
- The type of snapshot taken in ADM (2.8.035) may be displayed as a backup type after ADM is upgraded to ADM (2.8.041). The snapshot is actually installed as a deployment type even though it is indicated as a backup type. Use the following procedure to update to the correct display:
 1. Move the target snapshot folder from the following folder in the ADM server to another folder:
C:\Program Files (x86)\Atrust\snapshot
 2. Execute **Scan Snapshot** by selecting **System > Deployment > Snapshot** and confirm that the target snapshot is cleared from the list.
 3. Return the snapshot folder you moved to the folder in step 1 to the original folder.

4. Execute **Scan Snapshot** by selecting **System > Deployment > Snapshot** and confirm that the type of the target snapshot has been updated from backup to deployment.

**Atrust Device Manager
User's Guide**

First edition, September 2015

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

©NEC Corporation 2015

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