Atrust

Atrust Device Manager

Remote Client Management Software
for Atrust t-Series Clients

User's Manual

Version 2.01

Copyright and Trademark Statements

Limitation of Liability

While reasonable efforts have been made to ensure the accuracy of this manual, the manufacturer and distributor assume no liability resulting from errors or omissions in this manual , or from the use of the information contained herein.

Trademark statements

Microsoft and Windows are trademarks of the Microsoft group of companies.

Citrix, ICA, and XenApp are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries.

VMware and VMware View are trademarks or registered trademarks of the VMware, Inc.

GraphOn and GO-Global are registered trademarks and the GO logo is a trademark of GraphOn Corporation.

The Firefox logo is a registered trademark of Mozilla Foundation or Mozilla Corporation.

Adobe and Adobe Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Other product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

About This User's Manual

This manual provides the basic information on how to manage Atrust t-series zero/thin clients with the Atrust Device Manager software.

Manual Structure and Subjects

Chapter	Subject
1	Provides an overview of the Atrust Device Manager software.
2	Gives detailed instructions on how to install and upgrade Atrust Device Manager.
3	Provides instructions on how to manage clients with Atrust Device Manager.
4	Provides basic instructions on client configuration.

Notes, Tips, and Warnings

Throughout this manual, the notes, tips, and warnings in the following formats are used to provide important information, useful advice, and prevent injuries to you, damage to your devices, or loss of data on your system.

NOTE

- A note provides important information for a specific situation.

TIP

- A tip gives a piece of useful advice to perform a task more efficiently.

WARNING

- A warning provides crucial information that must be followed to prevent injuries to you, damage to your devices, or loss of data on your system.

Style Conventions

The following styles are used throughout this manual while referring to operational items on input devices, hardware panels, or application interfaces.

Item	Style	Example
keys on the keyboard	bold	**F11**, **N**, **B**, **S**
application windows, menus, or entry lists	first letter capitalized	Add window, Firmware list, Client list, Command menu
buttons or tabs on a window, toolbars, taskbar, or menu	bold	**OK**, **Next**, **Start**, **System** tab
options on a window, screen, list, or menu	bold	**I accept the agreement**, **Scan by IP Range**, **Update Firmware**, **Push Settings**
selecting a series of options	bold	**Start** > **All Programs** > **Atrust** > **Atrust Device Manager**

Table of Contents

Copyright and Trademark Statements **i**

Limitation of Liability i
Trademark statements i

About This User's Manual **ii**

Manual Structure and Subjects ii
Notes, Tips, and Warnings ii
Style Conventions ii

1 Overview 1

1.1 Introduction 3

1.2 Features 3

1.3 Supported Platforms 4

1.4 Supported Endpoint Devices 4

1.5 Minimum System Requirements 4

2 Installing and Upgrading Atrust Device Manager 5

2.1 Installing Atrust Device Manager 7

2.2 Installing Java Software 10

2.3 Initial Setup 10

2.4 Upgrading Atrust Device Manager 11

2.5 Uninstalling Atrust Device Manager 12

3 Using Atrust Device Manager 13

3.1 Atrust Device Manager 15

3.1.1 Interface Overview 15
3.1.2 Available Tasks at a Glance 16

3.2 Establishing a Basic Administration environment 17

3.2.1 System Tab Overview 17
3.2.2 Available Tasks at a Glance 18
3.2.3 Managing Administrator accounts 19
3.2.4 Managing Thin Client Firmware Files 20
3.2.5 Managing Zero Client Image Files 23
3.2.6 Managing WES Package Files 25
3.2.7 Managing Client Snapshots 27
3.2.8 Configuring Remote Deployment Settings 29
3.2.9 Selecting the Service IP of Atrust Device Manager 31
3.2.10 Configuring the Database Source of Atrust Device Manager 32
3.2.11 Selecting the Interface Language of Atrust Device Manager 33
3.2.12 Backing Up the Management Database 33
3.2.13 Managing Database Archive Files 34
3.2.14 Restoring a Management Database 35
3.2.15 Managing Client Certificate Authority Files 35
3.2.16 Managing P2T License Files 36

3.3 Adding Clients into a Managed Group 38

3.3.1 Scan Tab Overview 38
3.3.2 Available Tasks at a Glance 38
3.3.3 Client Detection and Management 39
3.3.4 Discovering Clients in the Whole Range of a Local Network 40

3.3.5 Discovering Clients in a Specified Range of IP addresses 41
3.3.6 Creating and Managing an IP Range List 42
3.3.7 Discovering Clients using a Predefined IP Range List 43

3.4 Managing All Your Clients 45

3.4.1 Thin Clients Tab Overview 45
3.4.2 Available Tasks at a Glance 46
3.4.3 Getting Your Zero Client Ready for Use 47
3.4.4 Creating Client Groups 48
3.4.5 Managing Client Groups 49
3.4.6 Moving Clients to Another Group 50
3.4.7 Deleting Clients from a Group 51
3.4.8 Understanding Client Status Icons 51
3.4.9 Client Settings 52
3.4.10 Creating Setting Profile Groups 53
3.4.11 Managing Setting Profile Groups 54
3.4.12 Creating Client Setting Profiles 55
3.4.13 Managing Client Setting Profiles 58
3.4.14 Using Individualized Client Settings 61
3.4.15 Using Hybrid Client Settings 63
3.4.16 Pushing Settings to Clients through Your Local Network 64
3.4.17 Pulling Client Settings through Your Local Network 67
3.4.18 Editing or Viewing the Basic Information about a Client 70
3.4.19 Rebooting Clients through Your Local Network 71
3.4.20 Shutting Down Clients through Your Local Network 73
3.4.21 Waking Clients through Your Local Network 77
3.4.22 Updating Client Firmware 80
3.4.23 Installing Software Packages 81
3.4.24 Taking Client Snapshots 82
3.4.25 Restoring Client Snapshots 84
3.4.26 Assisting a Client User Remotely 84
3.4.27 Digging Out Profiles, Clients, or Event Logs with Quick Search 87
3.4.28 Digging Out Clients with Filters 87
3.4.29 Managing Your Filters 89

3.5 Viewing and Managing Event Logs 91

3.5.1 Logs Tab Overview 91
3.5.2 Available Tasks at a Glance 91
3.5.3 Viewing Event Logs 92
3.5.4 Exporting Event Logs 92
3.5.5 Emptying Event Logs 93

3.6 Viewing Software Information 94

3.6.1 About Tab Overview 94
3.6.2 Available Tasks at a Glance 94
3.6.3 Viewing Information on Atrust Device Manager 95
3.6.4 Viewing Atrust Contact Information 95
3.6.5 Viewing Atrust Software License Agreement 95

4 Configuring Client Settings 97

4.1 Desktop Virtualization and Client Configuration 99

4.2 Client Settings at a Glance 99

4.3 Editing or Adjusting a Group Configuration 101

4.4 Editing or Adjusting an Individual Configuration 102

4.5 Configuring Client Settings with Atrust Client Setup 104

4.5.1 Atrust Client Setup for Linux-based Clients 104
4.5.2 Atrust Client Setup for WES-based Clients 105

1

Overview

This chapter provides an overview of the Atrust Device Manager software.

1.1 Introduction

Aturst Device Manager as a remote endpoint device management software 3

1.2 Features

The key features of Atrust Device Manager 3

1.3 Supported Platforms

Operating systems supported by Atrust Device Manager 4

1.4 Supported Endpoint Devices

Client devices supported by Atrust Device Manager 4

1.5 Minimum System Requirements

The minimum system requirements for the installation and operation of Atrust Device Manager 4

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 station 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:

- centralized management of work environments
- drastically reduced endpoint software/hardware issues
- application/desktop access across different platforms
- simplified system maintenance
- improved system security
- more scalability with low-cost endpoint devices

But still you need a powerful software for managing a large number of endpoint devices in a desktop virtualization infrastructure. The Atrust Device Manager software is designed to fill the 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 Features

The key features of Atrust Device Manager are:

- helping the management of zero clients

> **NOTE**
>
> - A zero client is an endpoint device without any operating system pre-installed. The client can only obtain its operating system when it's managed by the Atrust Device Manager software. A managed zero client downloads its operating system from its governing Atrust Device Manager when it is turned on over the network. Both the network connectivity and the governing Atrust Device Manager are prerequisites for its operation.

- pushing custom settings to a large number of clients
- updating firmware and installing software packages for clients
- taking client snapshots for quick system backup and recovery
- rebooting, powering off, and waking clients through the local network
- helping users to troubleshoot problems remotely
- identifying clients and managing IT assets with automatically-captured client information

1.3 Supported Platforms

Atrust Device Manager supports the following operating systems:

- Windows 7/Vista/XP
- Windows Server 2003/2008/2008 R2

1.4 Supported Endpoint Devices

Atrust Device Manager supports the following Atrust client family:

- t50
- t100 series (t100L/t100LZ/t100W)
- t160 series (t160L/t160LZ/t160W)
- t200 series (t200L/t200LZ/t200W/t200WQ)
- t210 series (t210L/t210W)
- t216 series (t216L/t216W)

NOTE

- For more information on available models and detailed specifications, please visit our website at www.atrustcorp.com.

1.5 Minimum System Requirements

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

- Pentium 4, 1.0 GHz processor or the equivalent
- 512 MB of free system memory
- 300 MB of free disk space (2 GB is recommended)
- 10/100 Mb Ethernet network adapter
- Java software or Java Runtime Environment (for the **Shadow** feature, see page 84)

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 7

2.2 Installing Java Software

The installation of Java Software or Java Runtime Environment 10

2.3 Initial Setup

The initial setup of Atrust Device Manager 10

2.4 Upgrading Atrust Device Manager

The upgrade of Atrust Device Manager 11

2.5 Uninstalling Atrust Device Manager

The uninstallation of Atrust Device Manager 12

2.1 Installing Atrust Device Manager

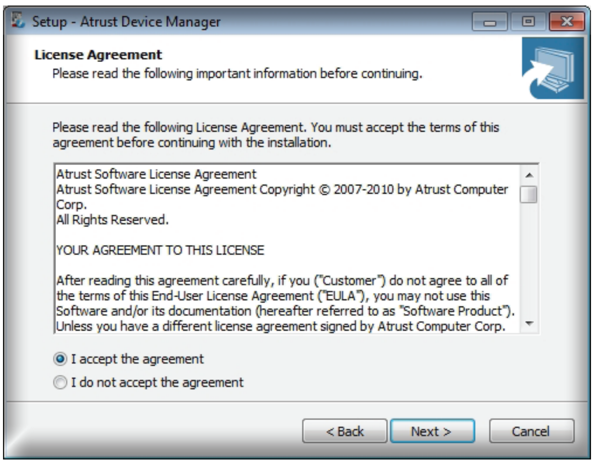
To install Atrust Device Manager on your computer, please follow the steps below:

NOTE

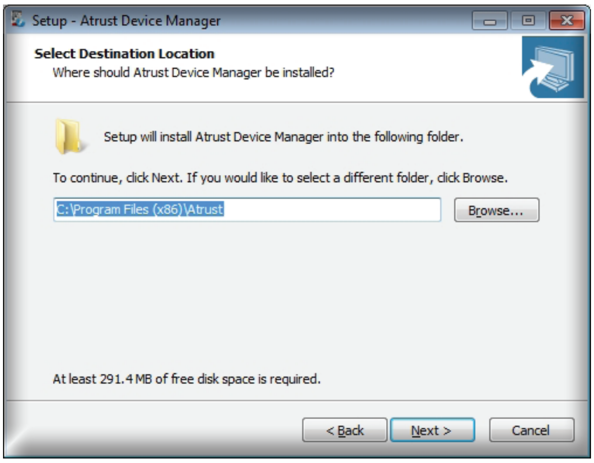
- Ensure that Atrust Device Manager can be installed on your computer before proceeding. For information on system requirements for the installation and operation of Atrust Device Manager, please refer to section "1.5 Minimum System Requirements" on page 4.
- To install a newer version of Atrust Device 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 11.

1. Insert the accompanying Documentation and Utility DVD into your DVD drive.
2. Double click the DVD drive to open the DVD folder, and then click **Utility** > **ADM** to locate the installation program for Atrust Device Manager.
3. Double click **adm-setup-1.xx-enus.exe** to launch the installation program.
4. The Setup Wizard appears.

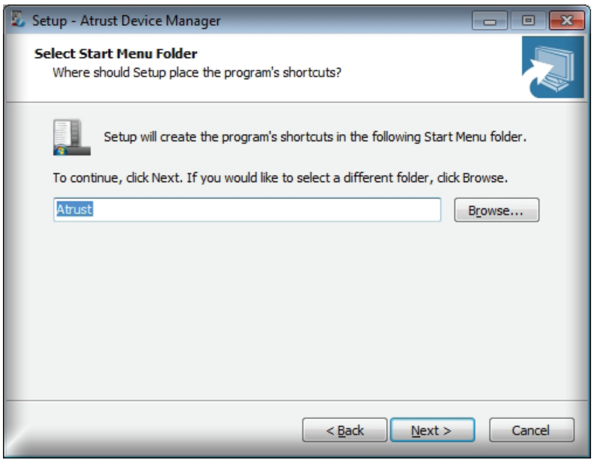
5. Click **Next** to continue.
6. Read the License Agreement, click to check **I accept the agreement**, and then click **Next** to continue.



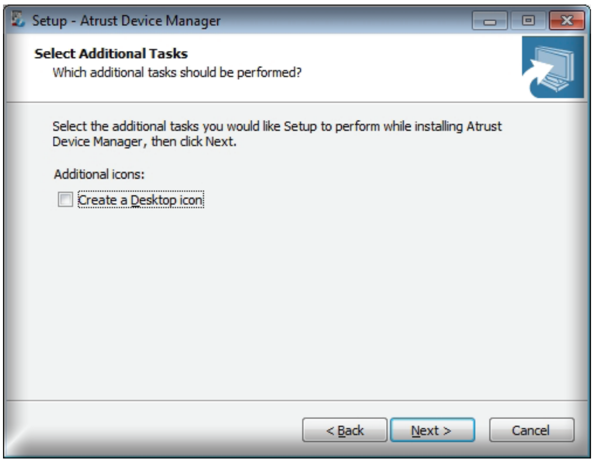
7. Use the default installation directory or click **Browse** to locate the desired one.



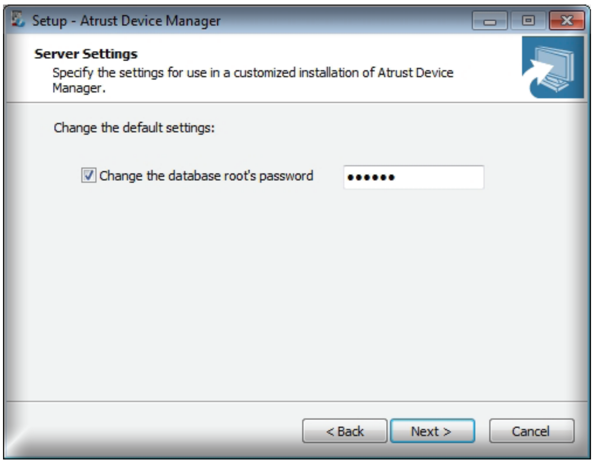
8. Click **Next** to continue.
9. Use the default Start menu folder or type to create a new folder for the shortcuts of programs. Or, click **Browse** to choose an existing folder.



10. Click to check/uncheck **Create a Desktop icon**, and then click **Next** to continue.

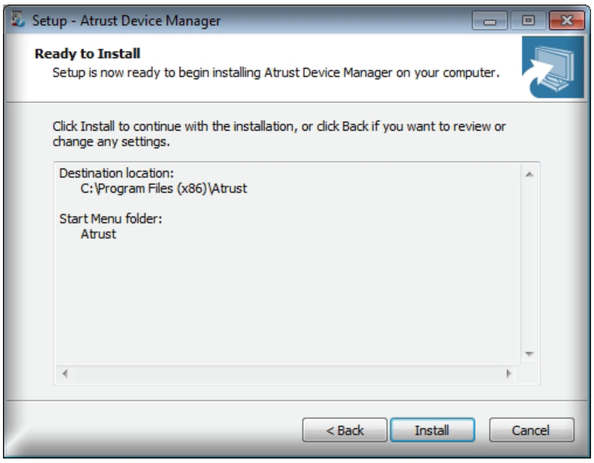


11. Change the default database password for the superuser or use the default. After completion, click **Next** to continue.



> **NOTE**
>
> - A superuser is a user who has full access to the database of Atrust Device Manager.

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.

Please visit the website for detailed instructions on how to install the software.

NOTE

- The Java software or Java Runtime Environment is required for the **Shadow** feature of Atrust Device Manager. This feature enables you to remotely assist a client user. For more information on how to do these, please refer to section "3.4.26 Assisting a Client User Remotely" on page 84.

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 configuration:

1. Click **Start** > **All Programs** > **Atrust** > **Atrust Device Manager** to open the application.

NOTE

- This step may vary if you choose not to use the default Start menu folder for placing this application shortcut during the installation of Atrust Device Manager.

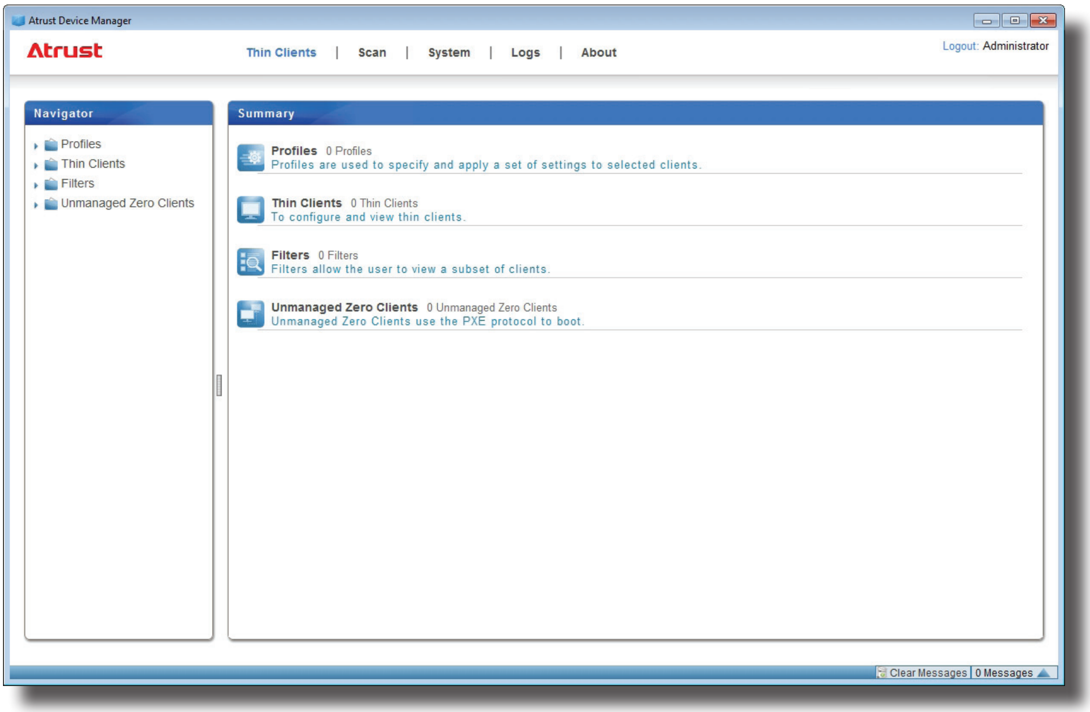
2. A window appears prompting you to choose the service IP address and create an administrator account. Click the drop-down menu to select the desired IP address from the list of available IP addresses. Type the desired account name and password, and then click **Save** to continue.

NOTE

- It's 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).

4. The management interface of Atrust Device Manager appears.



NOTE

- In next chapter, we will describe the functionality 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 7.

NOTE

- It's 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.

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 uninstalling the current Atrust Device Manager. For more information, please refer to section "2.4 Upgrading Atrust Device Manager" on page 11.
- Ensure that you have backed up important data on Atrust Device Manager before proceeding.

1. Click **Start** > **All Programs** > **Atrust** > **Uninstall Atrust Device Manager**.

NOTE

- This step may vary if you choose not to use the default Start menu folder for placing this application shortcut during the installation of Atrust Device Manager.

2. Follow the on-screen instructions to complete the uninstallation.

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 15

3.2 Establishing a Basic Administration environment

System tab overview 17

Available tasks at a glance 18

3.3 Adding Clients into a Managed Group

Scan tab overview 38

Available tasks at a glance 38

3.4 Managing All Your Clients

Thin Clients tab overview 45

Available tasks at a glance 46

3.5 Viewing and Managing Event Logs

Logs tab overview 91

Available tasks at a glance 91

3.6 Viewing Software Information

About tab overview 94

Available tasks at a glance 94

3.1 Atrust Device Manager

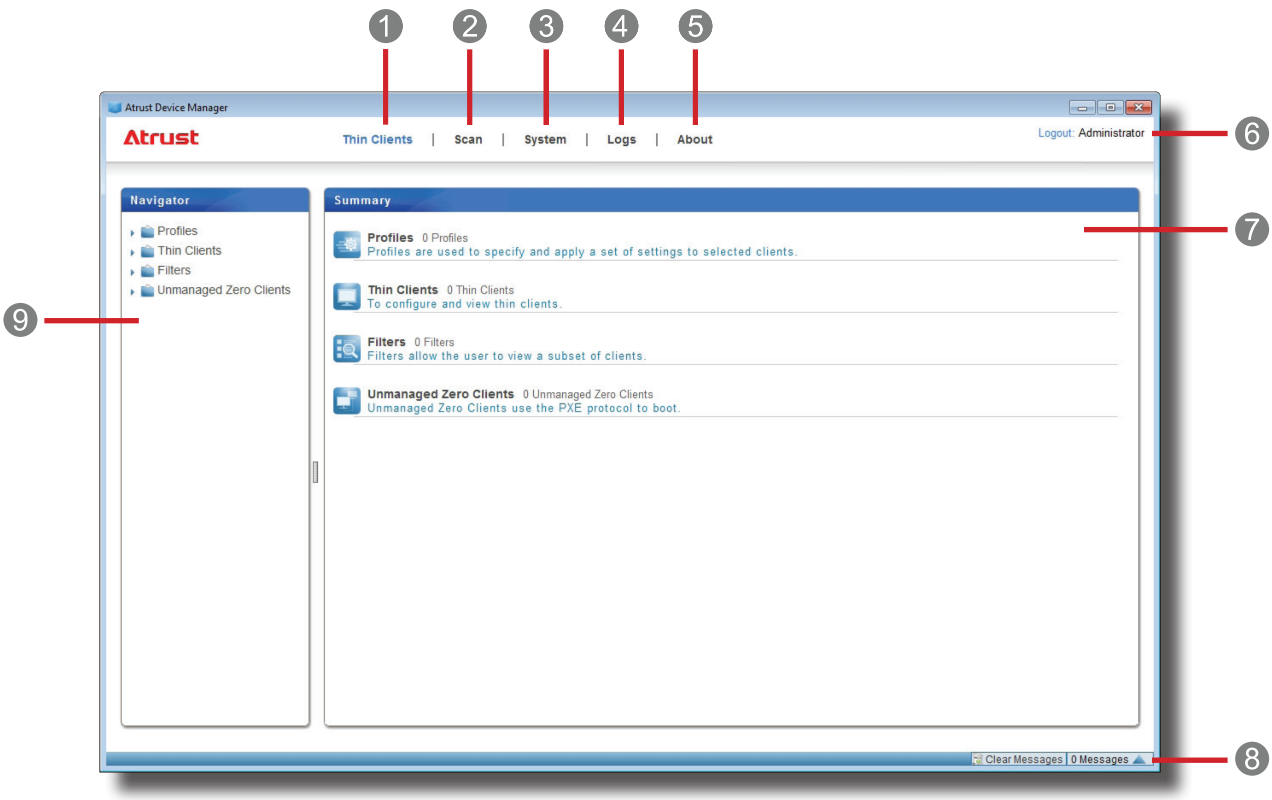
Atrust Device Manager enables you to remotely deploy, manage, update clients, and assist users from a single computer. You can manage clients simply and quickly in groups with a flexible and secure mechanism. Additionally, you can remotely assist users in resolving problems or configuring local settings.

3.1.1 Interface Overview

To access Atrust Device Manager, please do the following:

1. Click **Start** > **All Programs** > **Atrust** > **Atrust Device Manager**.
2. The Atrust Device Manager window appears.

Interface Overview



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	Message Area	Click to view messages about management activities.
9	Navigation Area	Click to select a specific item, option, or task under a tab.

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:

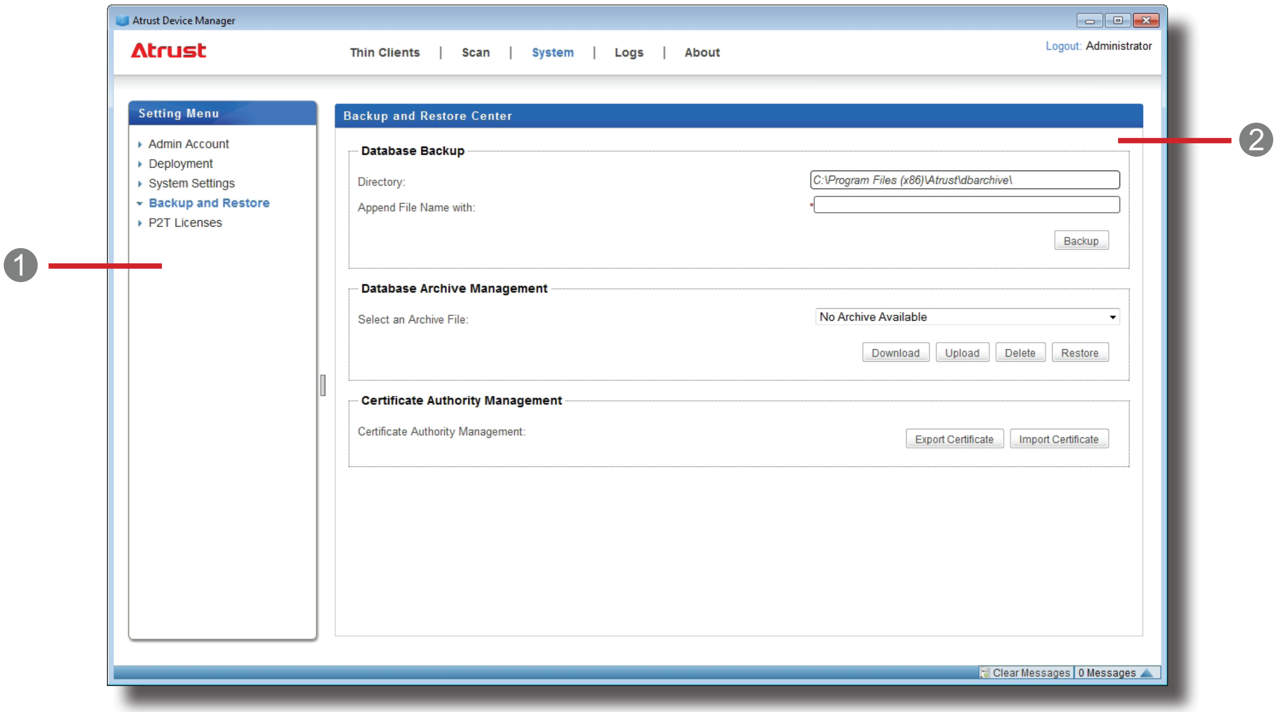
Tab	Function List	Section	Page
System	• creating an administrator account • managing thin client firmware files • managing zero client image files • managing WES package files • managing client snapshots • configuring remote deployment settings • configuring settings for Atrust Device Manager • backing up the management database • managing database archive files • restoring a management database • managing client Certificate Authority files • managing P2T license files	3.2 Establishing a Basic Administration environment	17
Scan	• 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	38
Thin Clients	• 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 • rebooting clients remotely • shutting down clients remotely • waking clients remotely • monitoring the use of clients • controlling clients remotely • digging out profiles/clients with Quick Search • digging out clients with filters	3.4 Managing All Your Clients	45
Logs	• viewing event logs • exporting event logs • emptying event logs	3.5 Viewing and Managing Event Logs	91
About	• viewing information on Atrust Device Manager • viewing Atrust contact information • viewing software license agreement	3.6 Viewing Software Information	94

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.

System Tab Overview



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

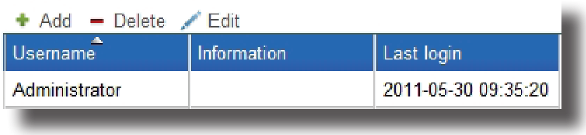
No.	Available Task	Section	Page
1	creating an administrator account	3.2.3	19
2	deleting an administrator account	3.2.3	19
3	editing an administrator account	3.2.3	19
4	importing thin client firmware files	3.2.4	20
5	deleting thin client firmware files	3.2.4	20
6	scanning thin client firmware files	3.2.4	20
7	importing zero client image files	3.2.5	23
8	deleting zero client image files	3.2.5	23
9	importing WES package files	3.2.6	25
10	deleting WES package files	3.2.6	25
11	scanning WES package files	3.2.6	25
12	exporting client snapshots	3.2.7	27
13	importing client snapshots	3.2.7	27
14	deleting client snapshots	3.2.7	27
15	scanning client snapshots	3.2.7	27
16	configuring remote deployment settings	3.2.8	29
17	selecting the service IP address of Atrust Device Manager	3.2.9	31
18	configuring the database source of Atrust Device Manager	3.2.9	31
19	selecting the database source of Atrust Device Manager	3.2.9	31
20	backing up the management database	3.2.12	33
21	downloading a database archive file	3.2.13	34
22	uploading a database archive file	3.2.13	34
23	deleting a database archive file	3.2.13	34
24	restoring a management database	3.2.14	35
25	exporting client Certificate Authority files	3.2.15	35
26	importing client Certificate Authority files	3.2.15	35
27	importing P2T license files	3.2.16	36

3.2.3 Managing Administrator accounts

Creating an Administrator account

To create an administrator account, please do the following:

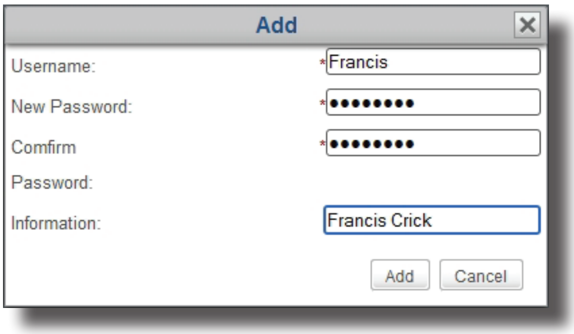
1. On **System** tab, click **Admin Account**.
2. The Account list appears in Management area.



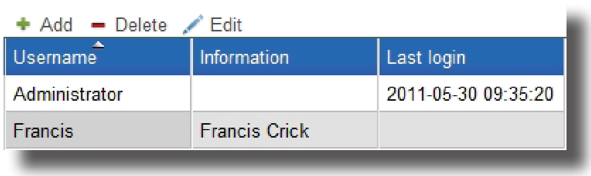
NOTE

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

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



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



Deleting an Administrator account

To delete an administrator 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 administrator 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 Administrator account

To adjust an existing administrator 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 "3.4.22 Updating Client Firmware" on page 80.
- To upgrade your zero client, 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 23.

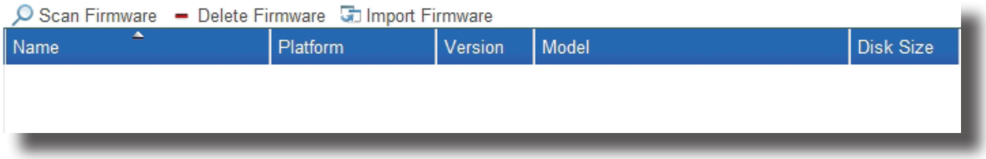
Importing Thin Client Firmware Files

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

NOTE

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

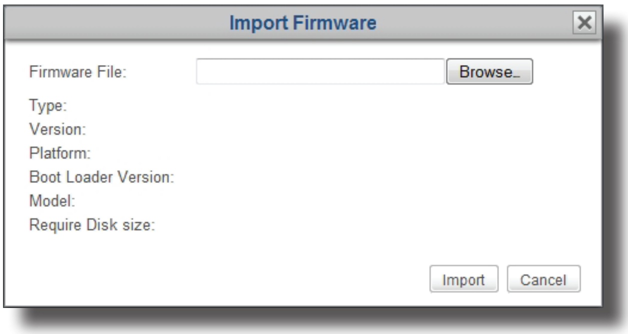
1. On **System** tab, click **Deployment** > **Firmware**.
2. The Firmware list appears.



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.

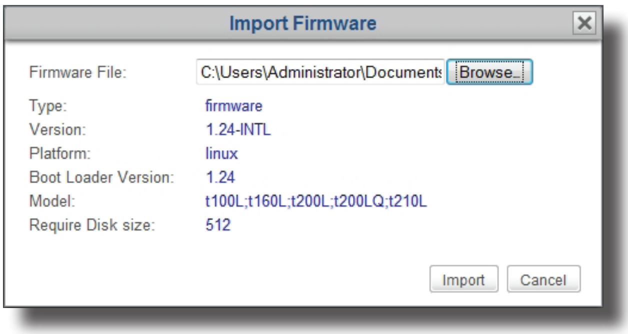


5. Click **Browse** to locate the desired firmware file, and then click **Open** to confirm.

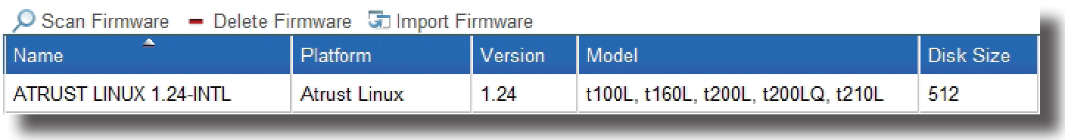
NOTE

- 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.

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



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



Deleting Thin Client Firmware Files

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

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

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

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

Scanning Thin Client Firmware Files

The **Scan Firmware** feature helps you to discover the local or remote firmware files. There are two scenarios that you need the help of this feature. The first scenario is that you choose to update clients with remote firmware files rather than local imported ones. In this scenario, the local list of available firmware in 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 "3.2.8 Configuring Remote Deployment Settings" on page 29.

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 appears 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

A zero client is an endpoint device without any operating system pre-installed. It can only obtain its operating system when it's managed by the Atrust Device Manager software. A managed zero client downloads its operating system from its governing Atrust Device Manager when it is turned on over the network. Both the network connectivity and the governing Atrust Device Manager are prerequisites for its operation.

Before a zero client can download its operating system, you need to import a zero client image file into the governing Atrust Device Manager as the downloadable operating system of the client. Additionally, you can also update your zero client by substituting a newer zero image file for the old one with Atrust Device Manager.

NOTE

- For instructions on how to replace the old zero image file with a newer one for your zero clients, please see section "3.4.22 Updating Client Firmware" on page 80.

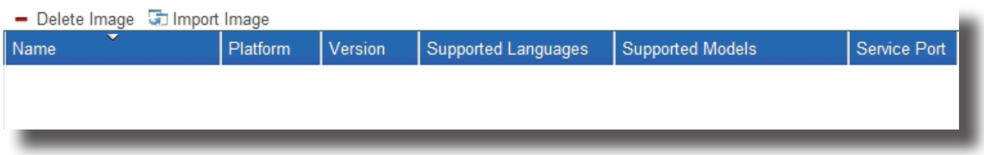
Importing Zero Client Image Files

To import an image file for your zero clients, please do the following:

NOTE

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

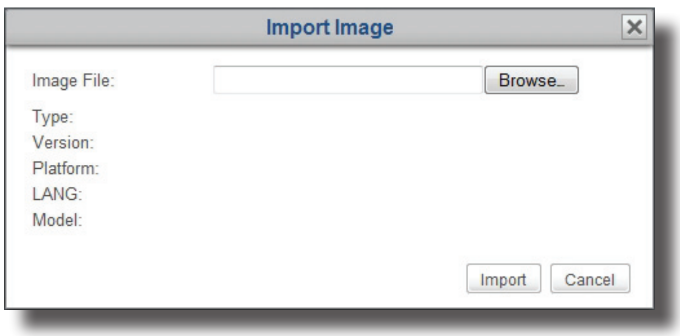
1. On **System** tab, click **Deployment** > **Zero Image**.
2. The Image list appears.



NOTE

- If you never imported zero client image files into Atrust Device Manager, the Image list will be empty as shown above.

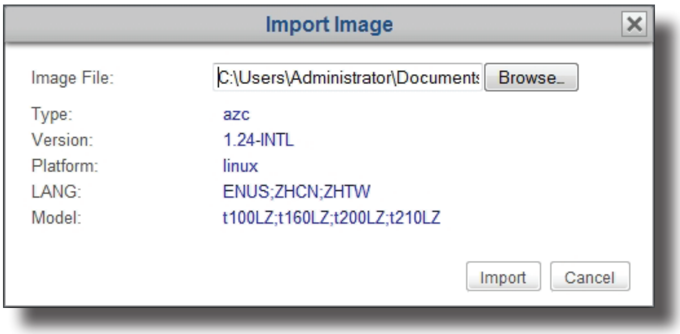
3. Click **Import Image** on the top of the Image list.
4. The Import Image window appears.



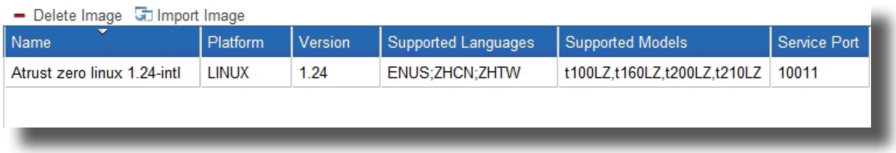
5. Click **Browse** to locate the desired zero image file, and then click **Open** to confirm.

> **NOTE**
> - Atrust Device Manager will automatically perform file check to ensure that the file is a valid image file for zero clients and there is no duplicate in the Image list.

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



7. On completion, the imported image file appears as an entry in the Image list.



Deleting Zero Client Image Files

To delete a zero client image file, please do the following:

> **NOTE**
> - If the selected image file is currently used by your zero clients, deleting the image file will make your zero clients unable to download their operating system from Atrust Device Manager. Ensure that you have replaced the selected image file with a new one for those zero clients before proceeding.

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

> **NOTE**
> - To delete more than one image file, Ctrl-click to select multiple files.

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

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

- For instructions on how to update your WES clients with package files remotely, please refer to "3.4.23 Installing Software Packages" on page 81.

Importing WES Package Files

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

NOTE

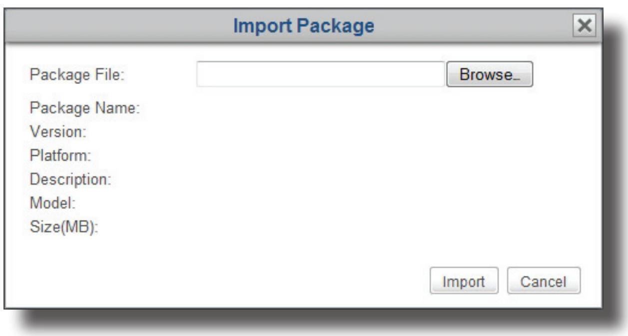
- For information about availability of a newer or up-to-date version of package file (.zip format), please contact your dealer.

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

NOTE

- If you never imported WES package files into Atrust Device Manager, the Package list will be empty as shown above.

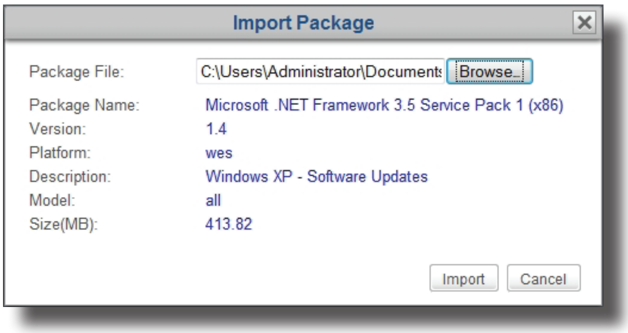
3. Click **Import Package** on the top of the list.
4. The Import Package window appears.



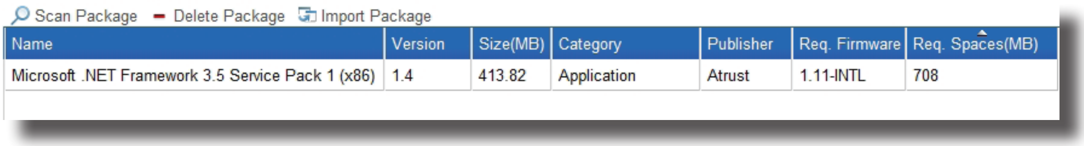
5. Click **Browse** to locate the desired package file, and then click **Open** to confirm.

> **NOTE**
> - Atrust Device Manager will automatically perform file check to ensure that the file is a valid package file for WES-based clients and there is no duplicate in the Package list.

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



7. On completion, the imported package file appears in the Package list.



Deleting WES Packages

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

1. On **System** tab, click **WES Package**.
2. The Package list appears.
3. Click to select the desired package file, and then click **Delete Package**.
4. The Delete Package window appears prompting you for confirmation.
5. Click **Delete** to confirm.
6. 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 "3.2.8 Configuring Remote Deployment Settings" on page 29.

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 appears 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 backup of a client at a specific point of time, which you can use to restore your client to that system state.

NOTE

- Atrust t-series zero clients (t100LZ/t160LZ/t200LZ/t210LZ) and Atrust t50L thin client do not support this feature.
- For instructions on how to take a system snapshot for clients, please refer to section "3.4.24 Taking Client Snapshots" on page 82.

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.

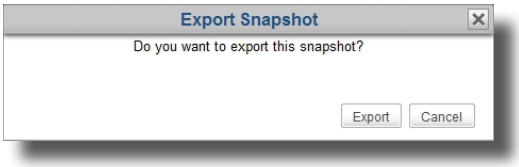
Scan Snapshot   Delete Snapshot   Import Snapshot   Export Snapshot

Name	Description	Location	Platform	Version	Model	Disk Size
1.29-INTL	t160L-000E66-110623d	/001FD8000E66-1/	Atrust Linux	1.29	t160L	512
1.29-INTL	t160L-000E8E-110623a	/001FD8000E8E-1/	Atrust Linux	1.29	t160L	512
1.29-INTL	t160L-000E66-110623e	/001FD8000E66-2/	Atrust Linux	1.29	t160L	512
1.29-INTL	t160L-000E66-110624a	/001FD8000E66-3/	Atrust Linux	1.29	t160L	512
1.12-INTL	t200W-000AB2-110624c	/001FD8000AB2-1/	Windows Embedded Standard	1.12	t200W	2048
1.13-INTL	t200W-00084E-110629a	/001FD800084E-1/	Windows Embedded Standard	1.13	t200W	1024
1.31-INTL	t160L-000E66-110629a	/001FD8000E66-4/	Atrust Linux	1.31	t160L	512
1.31-INTL	t160L-000E8E-110629a	/001FD8000E8E-2/	Atrust Linux	1.31	t160L	512

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 files.

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 "3.2.8 Configuring Remote Deployment Settings" on page 29.

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 appears 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 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 or snapshots	import or create all required files on the same computer where the governing Atrust Device Manager is installed	default
using remote updates or snapshots	configure settings to get all needed files from another computer	

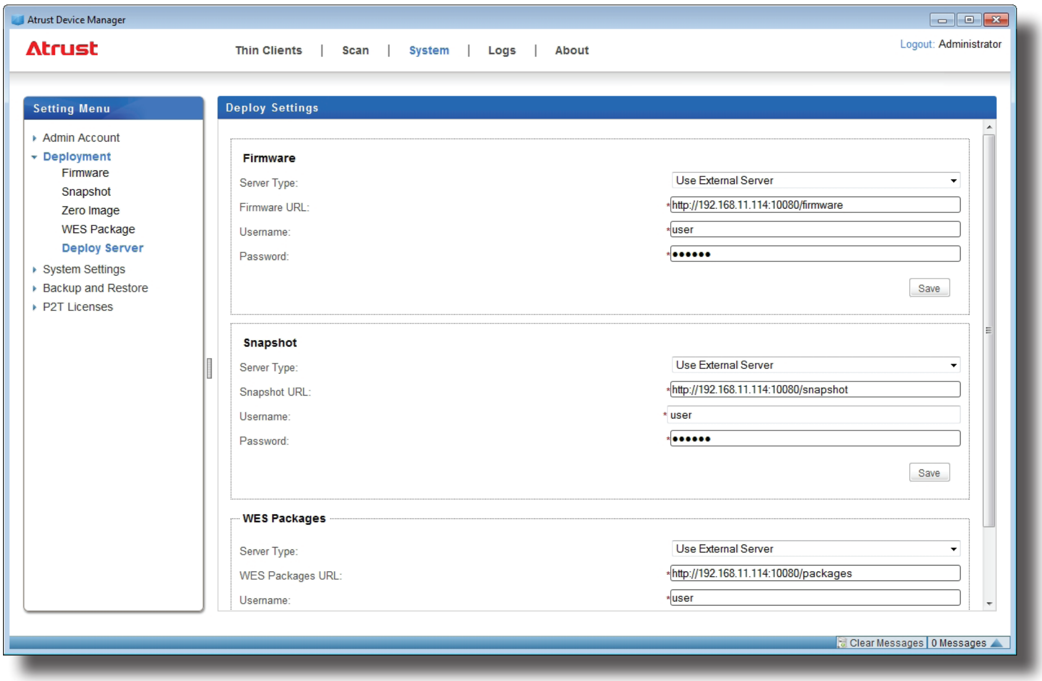
NOTE

- In Atrust Device Manager, the default is to use local updates or snapshots.

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 Settings pane appears in Management area.

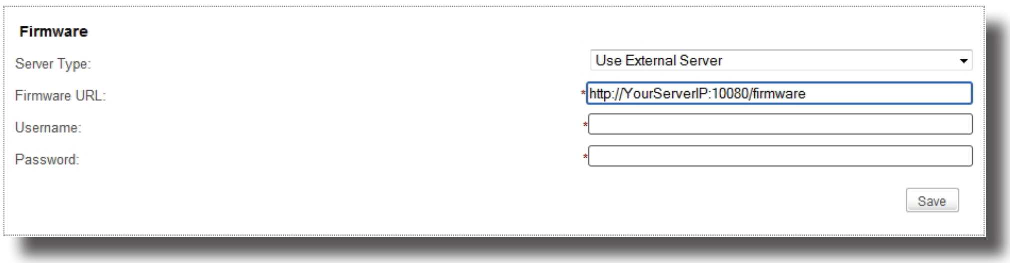


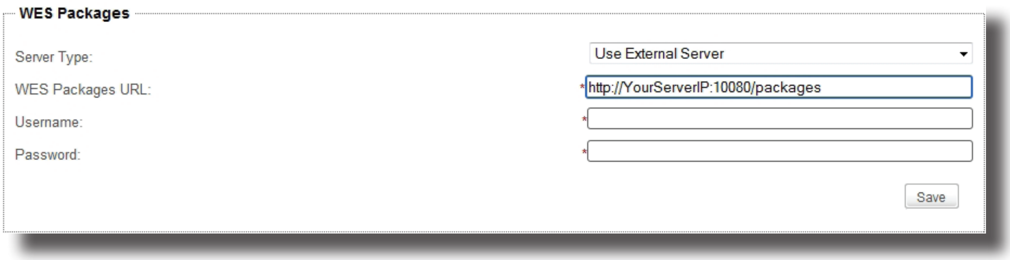
3. Click the drop-down menu on each section (**Firmware**, **Snapshot**, and **WES Packages**) to select **Use Internal Server**, and then click **Save** to apply.

Maintaining or Deploying Clients with Remote Updates or Snapshots

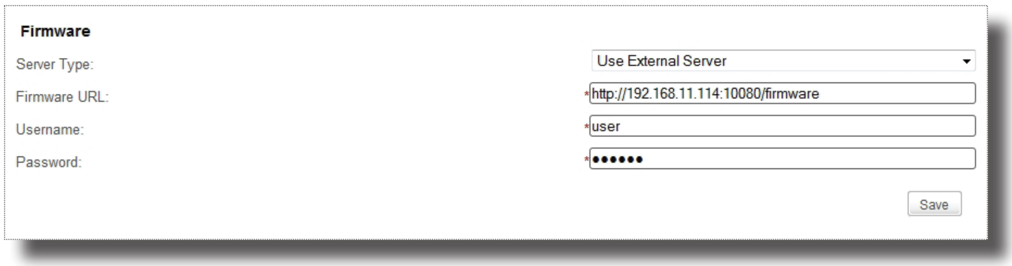
To maintain or deploy clients with external updates or snapshots, please do the following:

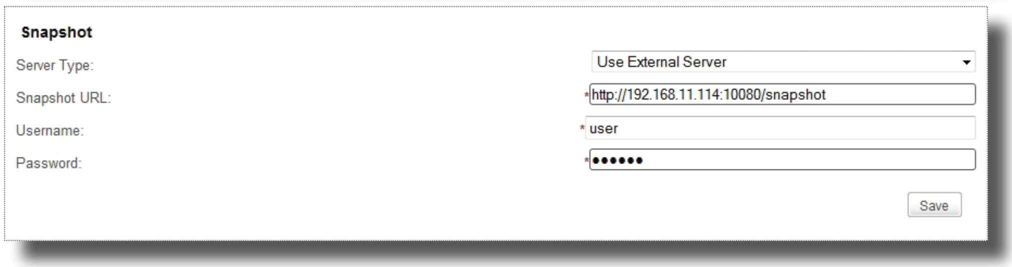
1. On **System** tab, Click **Deployment** > **Deploy Server**.
2. The Deploy Settings pane appears in Management area.
3. Click the drop-down menu on a section (Firmware, Snapshot, or WES Packages) to select **Use External Server**, new fields appear for configuration.

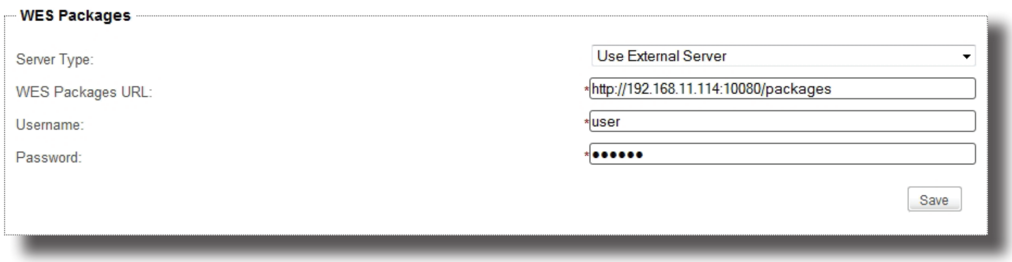




4. In Firmware URL field, replace **YourServerIP** in the original URL with the IP address of another computer where you want to get updates and snapshots, type in the default credentials with **user** as the username and **secret** as the password, and then click **Save** to apply.







3.2.9 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.
3. Click **Save** to apply.

NOTE

- It's 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.

3.2.10 Configuring the Database Source of Atrust Device Manager

By default, the management database of Atrust Device Manager is stored on the computer where Atrust Device Manager is installed. The corresponding management scenario is that you manage all your clients by accessing the same computer. Atrust Device Manager also offers the option that you can put the management database on a different computer/server. Then, with Atrust Device Manager, you can manage clients anywhere (on any Atrust Device Manager compatible computer) by accessing the external and centralized management database.

Using Local Management Database

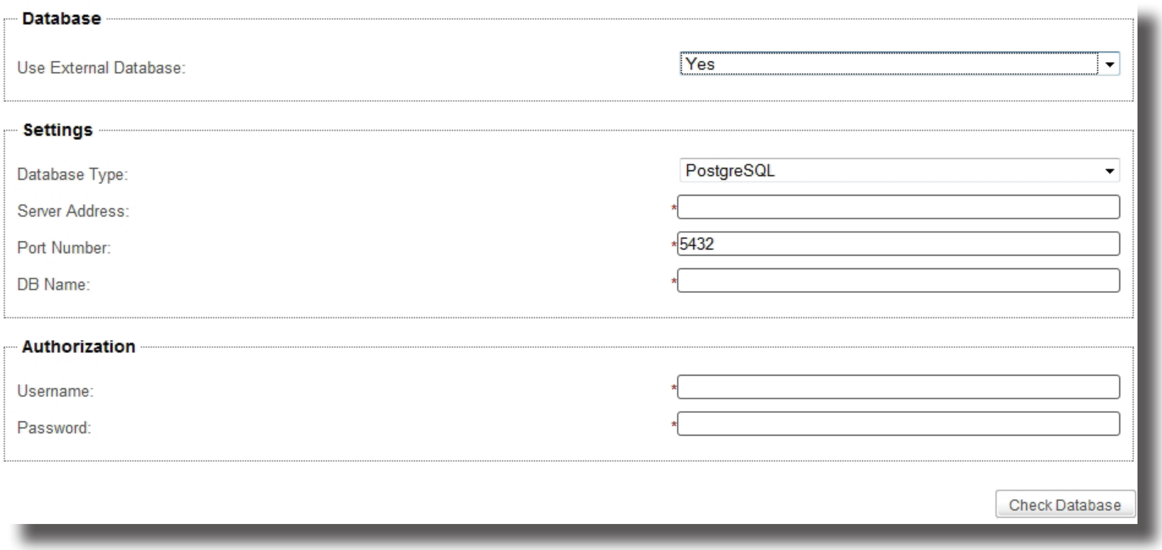
To use the local management database, please do the following:

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 appears 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 username and password for access of database.
7. Click **Check Database** to connect to the remote and centralized database.

3.2.11 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.

3.2.12 Backing Up the Management Database

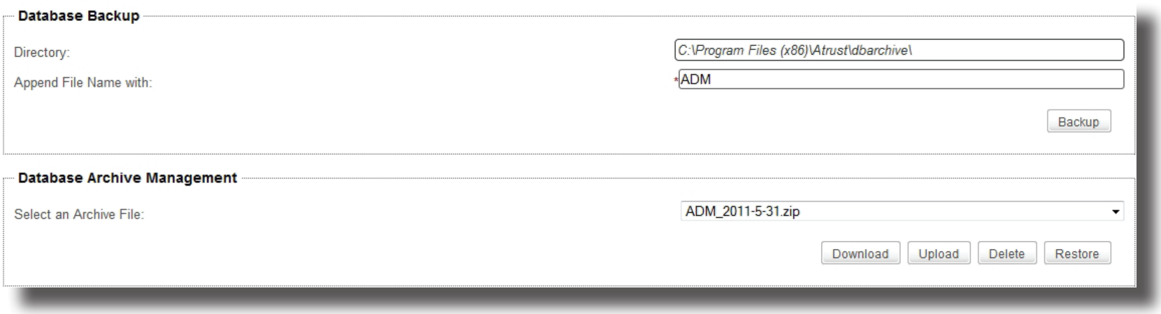
To back up the management database of Atrust Device Manager, please do the following:

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

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.
4. On completion, the backup file appears at the top of the drop-down menu of database archive in Database Archive Management section.



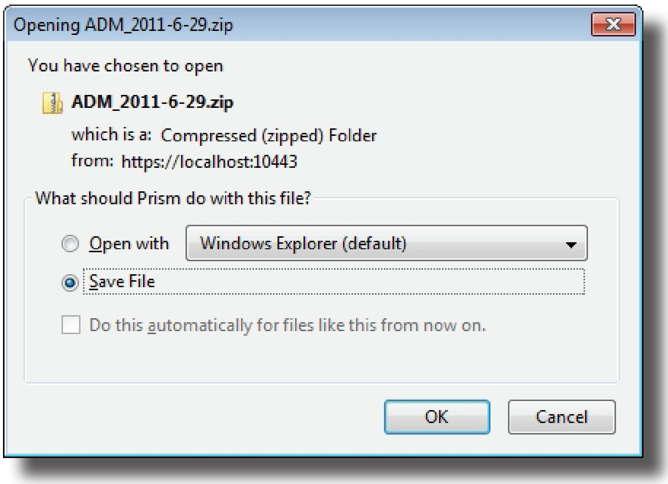
3.2.13 Managing Database Archive Files

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 drop-down menu to select the desired database archive file, and then click **Download**.

3. Click to check **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 list.

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 archive file.

3.2.14 Restoring a Management Database

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 drop-down menu to select the desired archive file.

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

3.2.15 Managing Client Certificate Authority Files

With Certificate Authority files for clients, your Atrust Device Manager are authorized to manage clients remotely. Your client is not managed by any Atrust Device Manager by factory default. To manage a client, you need to add it into a managed group under the governing Atrust Device Manager. Once this is done, the governing Atrust Device Manager obtains a Certificate Authority file to be able to manage that client.

NOTE

- Detailed instructions on how to add a client into a managed group under your Atrust Device Manager will be introduced in section "3.3.3 Client Detection and Management" on page 39.

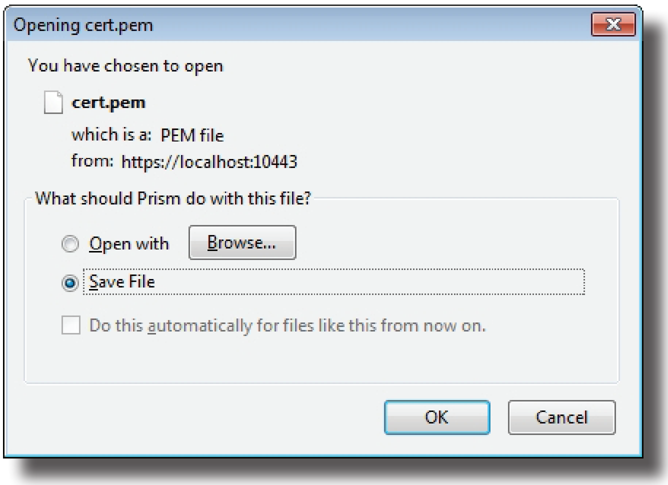
You can back up Certificate Authority files using the **Export Certificate** feature and restore them using the **Import Certificate** feature.

Exporting Certificate Authority Files

To export Certificate Authority files for managed clients, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Certificate Authority Management section, click **Export Certificate**.

3. In the opened window, click to check **Save File**, and then click **OK** to confirm.

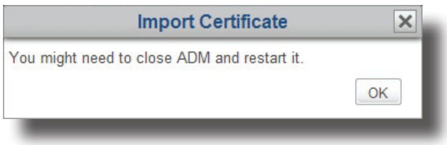


4. In the opened window, navigate to the desired directory, and then click **Save** to export the Certificate Authority files for managed clients.

Importing Certificate Authority Files

To import Certificate Authority files for managed clients, please do the following:

1. On **System** tab, click **Backup and Restore**.
2. In Certificate Authority Management section, click **Import Certificate**.
3. In the opened window, locate the desired Certificate Authority files, and then click **Open** to import Certificate Authority files.
4. The Import Certificate window appears to notify you that relaunching Atrust Device Manager is needed.



5. Click **OK** to confirm.

3.2.16 Managing P2T License Files

Atrust P2T Converter is also one of applications developed by Atrust that enables you to easily convert an existing personal computer into an Atrust thin client. The personal computer then runs as an Atrust Linux based client and is manageable by Atrust Device Manager. This software can help you extend the service life of existing computers and reduce the cost of IT transformation.

TIP

- P2T Converter is the abbreviation of ***PC to TC Converter***. Here ***TC*** is the acronym for ***Thin Client***.

To convert an existing computer into an Atrust thin client, you need to install P2T Converter on that computer. For detailed instructions, please refer to the Installation Guide for P2T Converter.

NOTE

- From now on, we will refer to the computer which P2T Converter has been installed on it as a P2T client for short.

To get your P2T client ready for use, you need to add your P2T client into a managed group under Atrust Device Manager and obtain a P2T license from Atrust Device Manger.

NOTE

- For instructions on how to add your P2T client into a managed group under Atrust Device Manager, please refer to section "3.3.3 Client Detection and Management" on page 39.

You need to import the license file(s) into Atrust Device Manager, preparing licenses for your P2T clients. The number of licenses determines how many P2T clients you could have.

To import P2T license files into Atrust Device Manager for your P2T clients, please do the following:

1. On **System** tab, click **P2T Licenses**.
2. In Import P2T License section, click **Import**.

3. In the opened window, locate the desired P2T license file, and then click **Open**.

NOTE

- The file name extension of a license file is **.lis**.

4. The license file is imported and available number of P2T licenses is shown in Available P2T Licenses section.

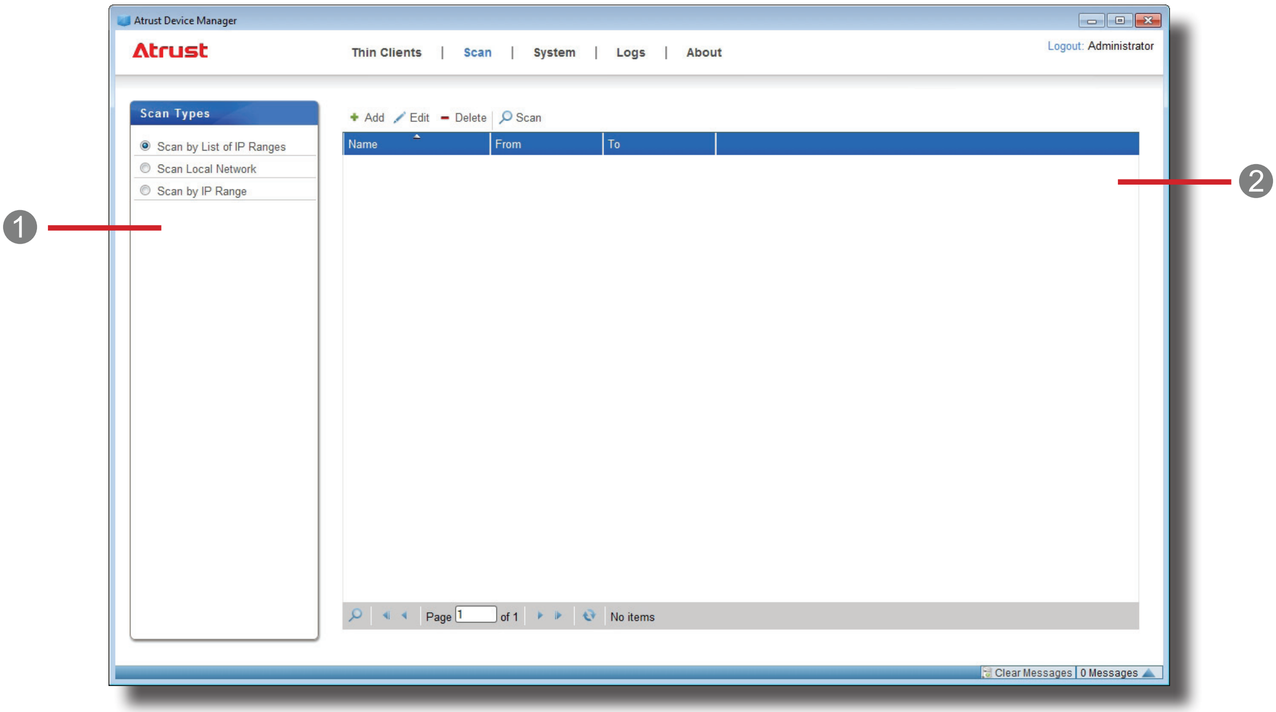
5. Repeat steps 2 through 4 to import other license files.

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. 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	Click to check 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	40
2	discovering clients in a specified range of IP addresses	3.3.5	41
3	discovering clients using predefined IP range lists	3.3.6 3.3.7	42 43

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 methods provided on **Scan** tab. To look for a zero client, just connect it to your local network and then turn it on. Your Atrust Device Manager can automatically detect any zero client, including both the managed (by another computer) and unmanaged, when the zero client is connected to your local network and is turned on.

NOTE

- A zero client is an endpoint device without any operating system pre-installed. It can only obtain its operating system when it's managed by the Atrust Device Manager software. A managed zero client downloads its operating system from its governing Atrust Device Manager when it is turned on over the network. Both the network connectivity and the governing Atrust Device Manager are prerequisites for its operation.

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

Type	Model	Prerequisites	Method	Section	Page
Thin Client	t100L, t100W t160L, t160W t200L/LQ, t200W/WQ t210L, t210W t50L	• clients are connected to the local network • clients are powered up	Manual Scan	3.3.4 3.3.5 3.3.6	40 41 42
Zero Client	t100LZ t160LZ t200LZ	• before clients are powered up, the Atrust Device Manager used to manage zero clients is installed and the computer where the Atrust Device Manager is installed is connected to your local network • the zero image file(s) as the operating system of zero clients is imported into Atrust Device Manager and ready for download • clients are connected to the local network • clients are powered up	Automatic Detection	3.4.3	47

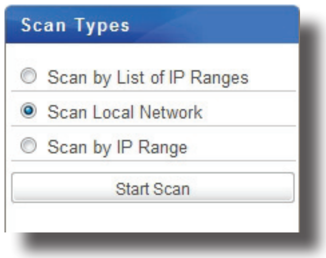
NOTE

- 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 detailed instructions on how to manage your clients remotely, please refer to section "3.4 Managing All Your Clients" on page 45.

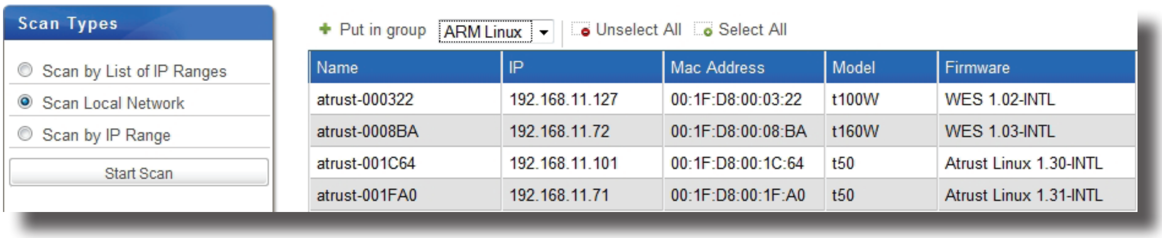
3.3.4 Discovering Clients in the Whole Range of a Local Network

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, click to check **Scan Local Network**.



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



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 48.
> - 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.

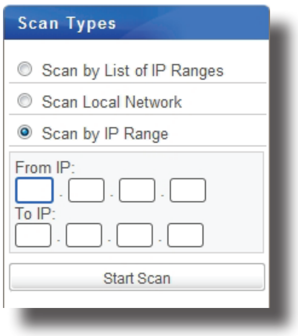
5. On completion, the client(s) is managed by your Atrust Device Manager.

> **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.

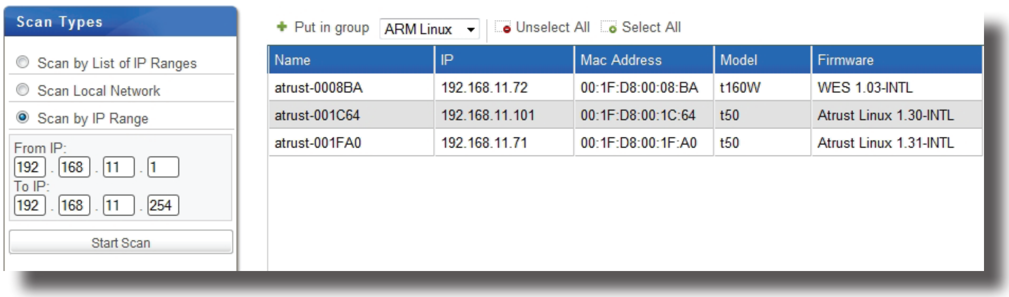
3.3.5 Discovering Clients in a Specified Range of IP addresses

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, click to check **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.



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 48.
- 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.

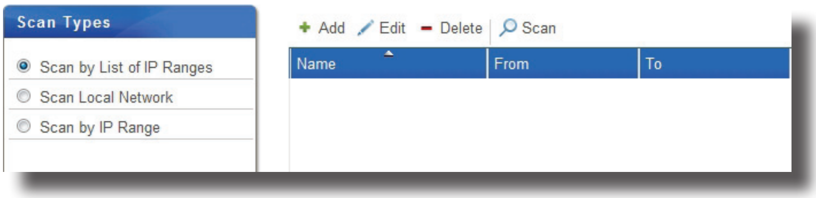
3.3.6 Creating and Managing an IP Range List

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

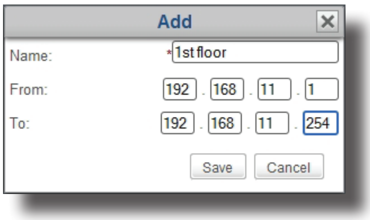
Creating an IP Range List

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

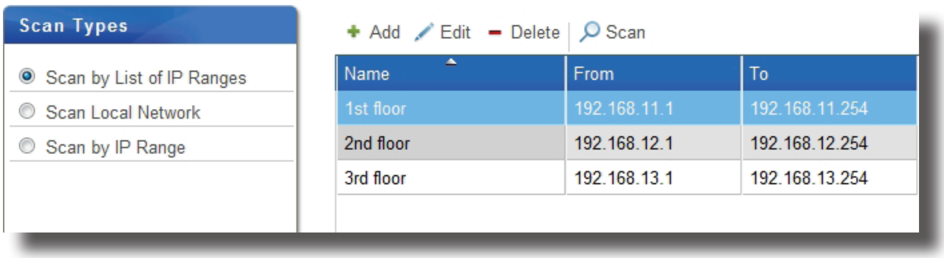
1. On **Scan** tab, click to check **Scan by List of IP Ranges**.
2. Click **Add** on the top of the IP Range list.



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:

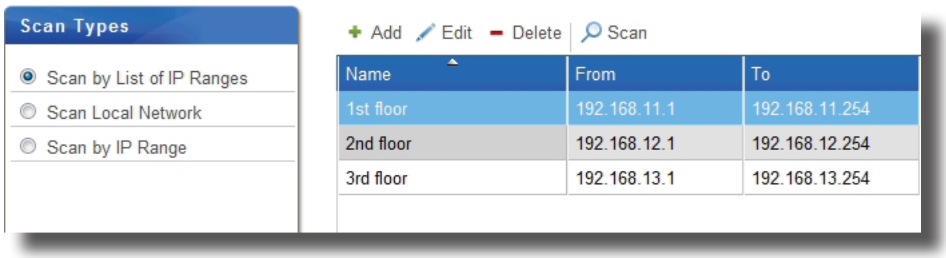
1. On **Scan** tab, click to check **Scan by List of IP Ranges**.
2. The IP Range list appears in Management area.
3. Click **Add**, **Edit**, or **Delete** to make changes to your IP Range list.

3.3.7 Discovering Clients using a Predefined IP Range List

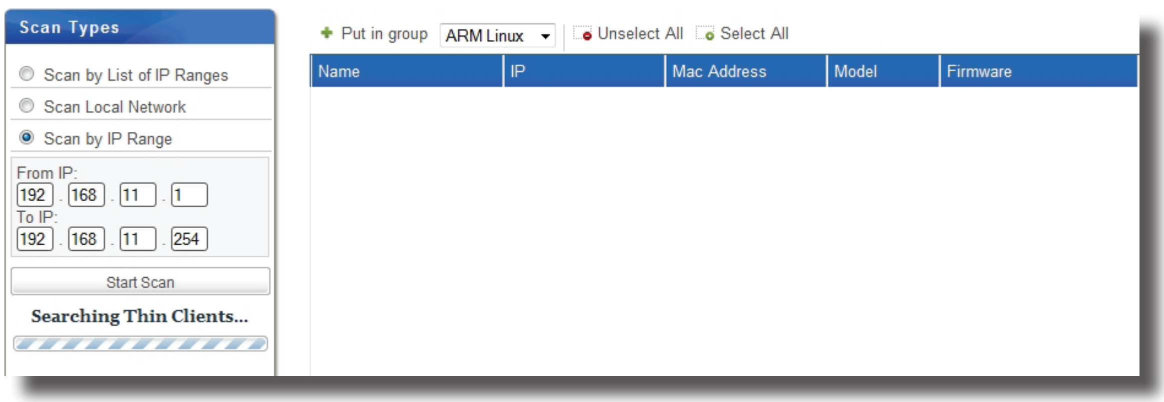
To discover unmanaged clients using a predefined IP Range list and add the desired client(s) into a managed group under Atrust Device Manager, please do the following:

> **NOTE**
>
> - If you haven't create any IP Range list, please refer to "3.3.6 Creating and Managing an IP Range List" on page 42 for instructions.

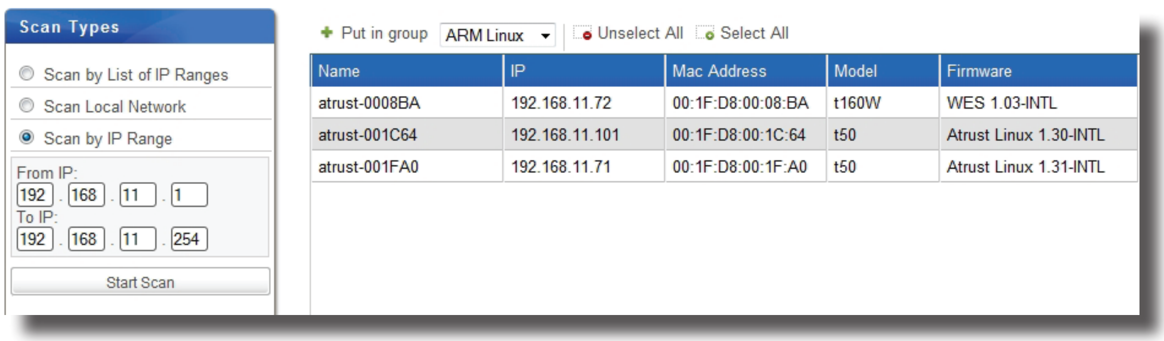
1. On **Scan** tab, click to check **Scan by List of IP Ranges**.
2. The IP Range list appears.
3. Click to select the desired IP range, and then click **Scan** to look for unmanaged clients within the range.



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



5. 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 48.
> - 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.

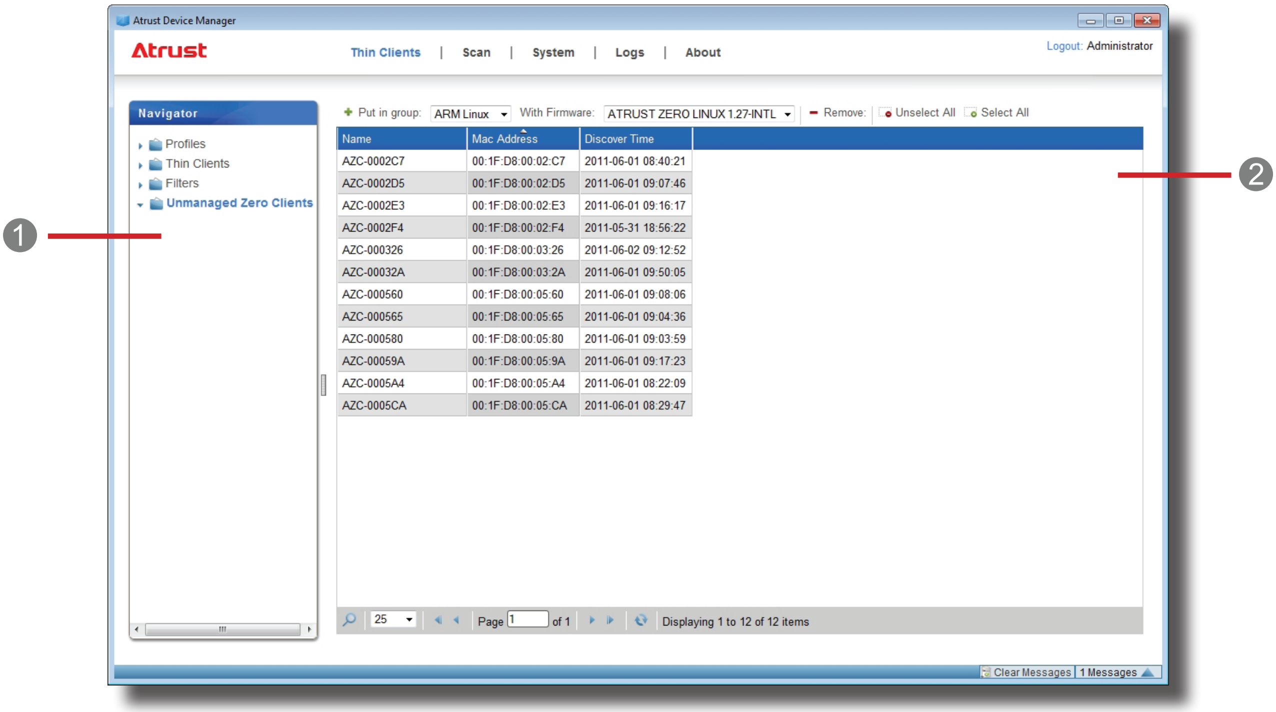
> **NOTE**
>
> - Whichever group you add a client to (including **Ungrouped**), once **Put in group** is executed successfully, the client will be managed by your Atrust Device Manager.

3.4 Managing All Your Clients

3.4.1 Thin Clients Tab Overview

Thin Clients 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	47
2	creating client groups	3.4.4	48
3	managing client groups	3.4.5	49
4	managing clients in a group	3.4.6 3.4.7	50 51
5	creating setting profile groups	3.4.10	53
6	managing setting profile groups	3.4.11	54
7	creating client setting profiles	3.4.12	55
8	managing client setting profiles	3.4.13	58
9	using individualized client settings	3.4.14	61
10	using hybrid client settings	3.4.15	63
11	pushing settings to clients through your local network	3.4.16	64
12	pulling settings from clients through your local network	3.4.17	67
13	editing or viewing basic information about a client	3.4.18	70
14	rebooting clients through your local network	3.4.19	71
15	shutting down clients through your local network	3.4.20	73
16	waking clients through your local network	3.4.21	77
17	updating client firmware	3.4.22	80
18	installing software packages	3.4.23	81
19	taking client snapshots	3.4.24	82
20	restoring client snapshots	3.4.25	84
21	assisting a client user remotely	3.4.26	84
22	monitoring a client remotely	3.4.26	84
23	controlling a client remotely	3.4.26	84
24	digging out profiles or managed clients with Quick Search	3.4.27	87
25	digging out managed clients with filters	3.4.28	87
26	managing your client filters	3.4.29	89

3.4.3 Getting Your Zero Client Ready for Use

To get your zero client ready for use, please do the following:

NOTE

- For more information on client types and management, including both zero and thin clients, please refer to section "3.3.3 Client Detection and Management" on page 39.

1. Ensure that you have turned off Windows Firewall of your computer where the Atrust Device Manager software is installed.

   To turn off Windows Firewall of your computer, please do the following:

   1) Click **Start** > **Control Panel** > **System and Security** > **Windows Firewall** > **Turn Windows Firewall on or off**.
   2) Click to check **Turn off Windows Firewall** for your computer, and then click **OK** to apply.

NOTE

- The type of network (public or private) for your computer may vary, depending on the network settings of your computer. Select the correct type of network to turn off its Windows Firewall.
- If you don't turn off Windows Firewall for your computer, Atrust Device Manager will fail to manage zero clients.

2. On **Thin Clients** tab, click **Unmanaged Zero Clients**.
3. The Zero Client list appears in Management area.

NOTE

- As of when your Atrust Device Manager was installed and connected to your local network, all zero clients which were ever connected to the local network and turned on will be recorded and shown in this Zero Client list. Some of them might have already been managed by another instance of Atrust Device Manager on another computer.

4. Connect your zero client to your local network, and then turn it on.
5. Your Atrust Device Manager will detect this newly added device over the network and add it to the Zero Client list.
6. Use the MAC address of your zero client to identify it on the list.

NOTE

- The MAC address is a unique identifier assigned to a network interface. Since your zero client is equipped with a LAN port, the unique MAC address of this network interface can be used to identify your zero client. You can find this information on a label attached to your product.

7. Click to select your zero client, select the desired client group and firmware version from the drop-down menus, and then click **Put in group**.

NOTE

- Ensure that you have already imported zero image files into your Atrust Device Manager. Zero clients don't pre-install any operating system and only download their operating system from the governing Atrust Device Manager when is started up. While adding a zero client into a managed group under your Atrust Device Manager, you need to provide and specify which image file to be used for producing the operating system. Otherwise, an error message appears prompting you to provide and specify a firmware file (zero image file).
- To import zero image files into your Atrust Device Manager, please refer to "3.2.5 Managing Zero Client Image Files" on page 23.
- The default client group is **Ungrouped**. You can change the group of a zero client at a later time. To create new client groups, please refer to "3.4.4 Creating Client Groups" on page 48.
- To select multiple clients, just click to select each individual client. You can also use **Select All** and **Unselect All** above the Zero Client list to select/unselect clients.

8. On completion, the zero client 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.

3.4.4 Creating Client Groups

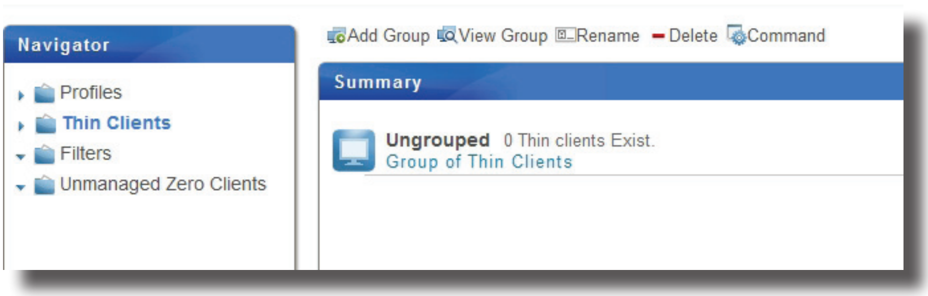
You can create a client group for putting a set of clients together for ease of management.

NOTE

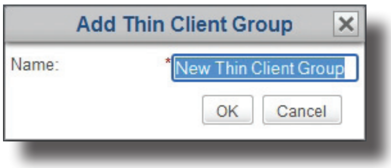
- The default client group is **Ungrouped**. You can change a client's group if needed.

To create a client group, please do the following:

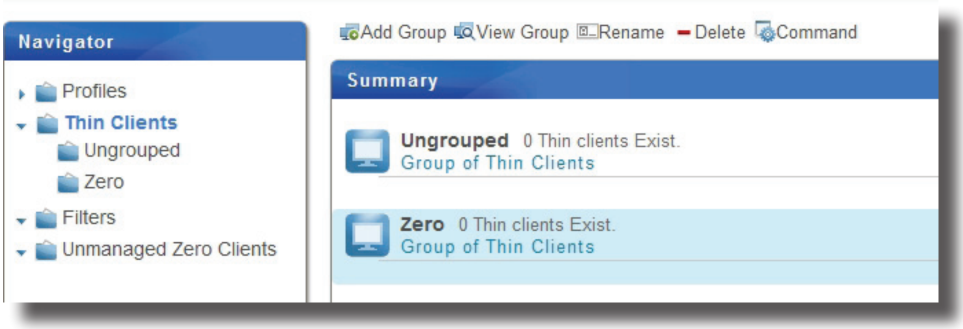
1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. Click **Add Group** on the top of the Management area.



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

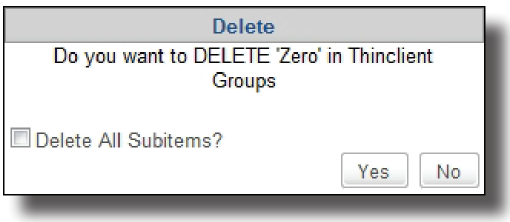
To rename a client group, please do the following:

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 your 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** unchecked, 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, click to check **Delete All Subitems**, and then click **Yes** to confirm. All clients in this group will be removed from your Atrust Device Manger.

NOTE

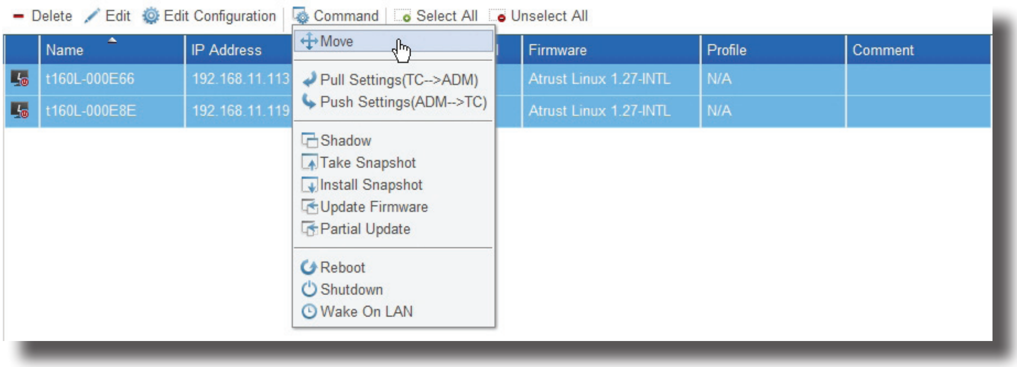
- Removing a client from your Atrust Device Manager will release the client from the management of Atrust Device Manager. If the removed is a zero client then that client will become unbootable due to the lack of an opearating system downloaded from and provided by the governing Atrust Device Manager while starting up the zero client.

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:

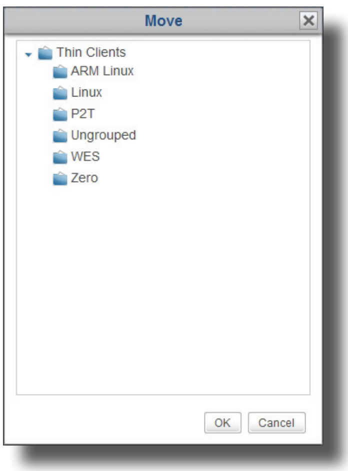
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. Click to select the desired client, and then click **Command** on the top of the Client list to open the Command menu.



NOTE

- To select more than one client, Ctrl-click or use **Sellect 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 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.

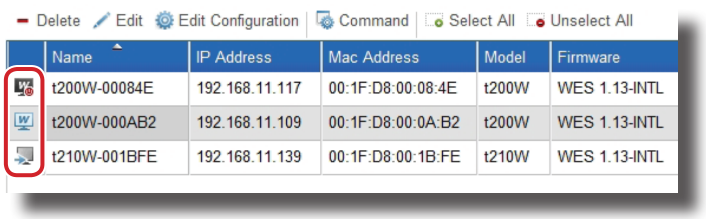
> **NOTE**
>
> • To select more than one client, Ctrl-click or use **Select All** to select multiple clients.

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. If the removed is a zero client then that client will become unbootable due to the lack of an opearating system downloadable from and provided by the governing Atrust Device Manager while booting up the zero client.

3.4.8 Understanding Client Status Icons

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

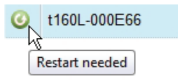


The status icon changes according to different states of a client. Five types of icons are available:

Understanding Client Status Icons		
State	**Icon**	**Description**
Online		Indicates that a client is turned on at the moment.
Offline		Indicates that a client is turned off at the moment.
Reboot needed		Indicates that you need to reboot a client for configuration changes 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 corresponding client.
pushed		Indicates that Atrust Device Manager has pushed a configuration change to a client.

NOTE

- The icon made up of a little display with a letter ***L***, ***W***, or ***Z*** on its screen indicates that the client is a Linux-based, WES-based (Windows Embedded Standard) thin client, or a Zero client.
- A tooltip pops up as shown below 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. Atrust t-series clients can meet a wide range of forms and needs. But to get your client ready for use, you need to configure client settings to meet the needs in your desktop virtualization plan.

NOTE

- The available settings may vary, depending on different client models. For detailed information on available settings of different product models, please refer to chapter 4 "Configuring Client Settings" on page 97.

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 software is a built-in application for all Atrust t-series client products. This application 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 software. 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 97.

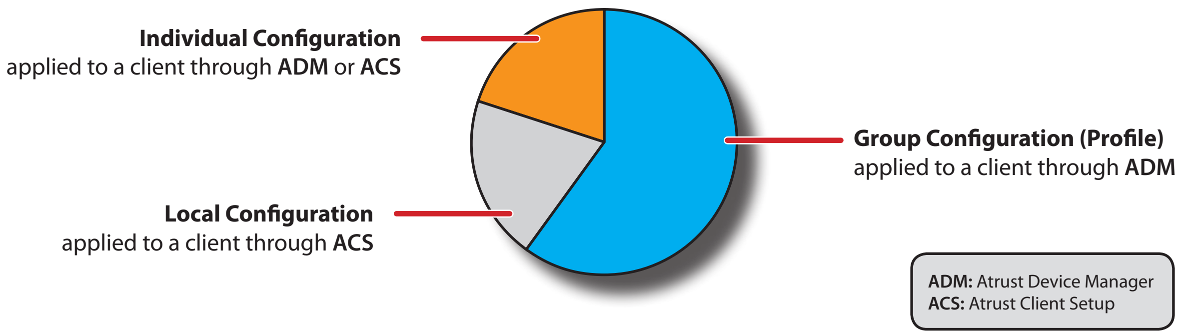
Group Configuration and Individual Configuration

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.

Client Configuration



Method	Configuration Type	Software	Section	Page
Local	local configuration	Atrust Client Setup (ACS)	4.2 4.5	99 104
	individual configuration	Atrust Client Setup (ACS)	4.2 4.5	99 104
Remote	group configuration	Atrust Device Manager (ADM)	3.4.12	55
	individual configuration	Atrust Device Manager (ADM)	3.4.14	61

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.

A blue lock icon indicates that the current value of the corresponding setting item comes from a group configuration. A 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.

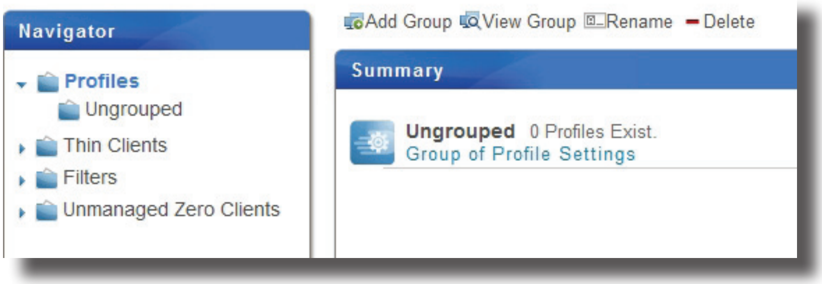
A setting profile group is a set of profiles grouped together for ease of management.

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:

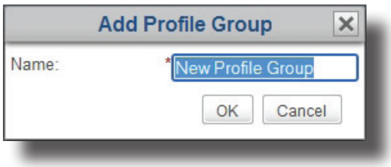
1. On **Thin Clients** tab, click **Profiles**.
2. The Profile Group list appears.



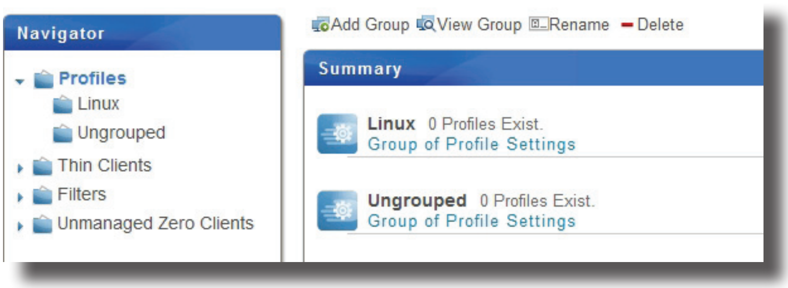
NOTE

- **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.

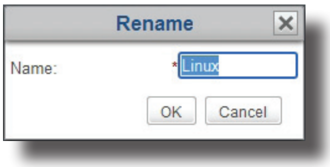


3.4.11 Managing Setting Profile Groups

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.

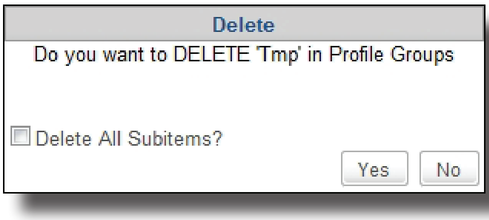


4. Type in the new name for the profile group, and then click **OK** to confirm.

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** unchecked, 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, click to check **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 fo 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 52.

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

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

Step 2: Specify the applicable scope of the setting profile

STEP 1: Create a set of shared client settings

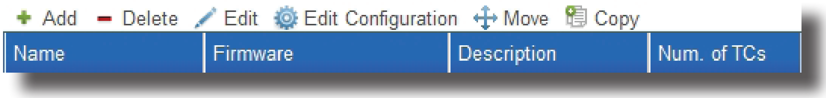
To create a client setting profile (group configuration), please do the following:

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

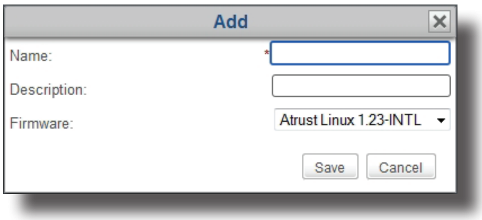
NOTE

- You need to select the profile group to which the new profile belongs first. You can use the system default (**Ungrouped**), and change the group at a later time if necessary. For detailed instructions on how to create a profile group, please refer to section "3.4.10 Creating Setting Profile Groups" on page 53.

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



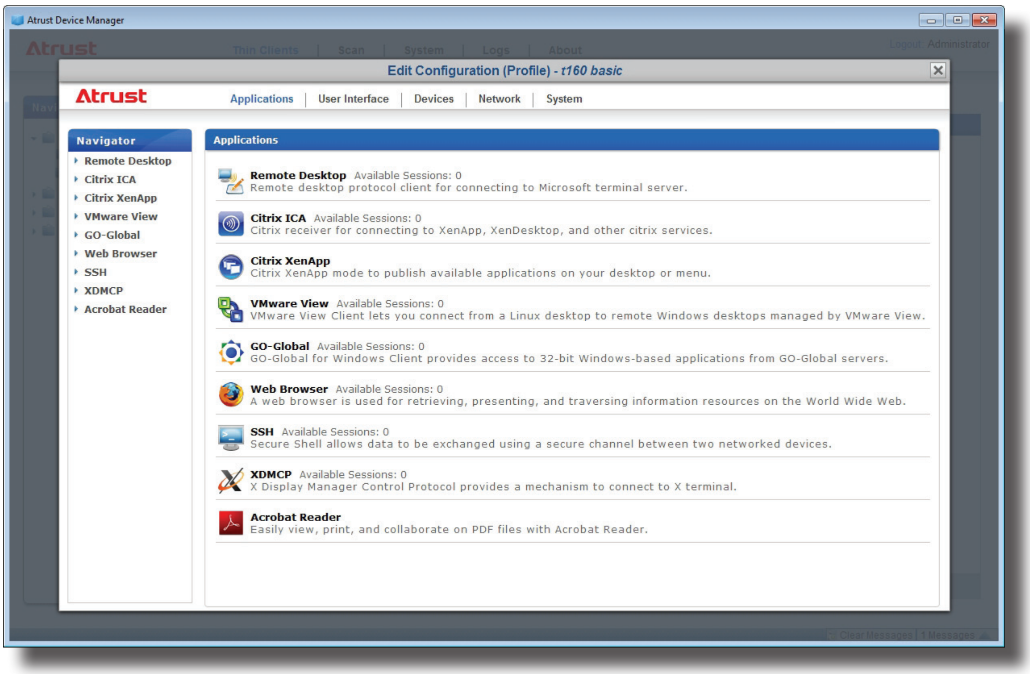
3. The Add window appears prompting for the name, description, and firmware version of this profile.



NOTE

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

4. Type in the desired name, description, and firmware version for this profile, 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.

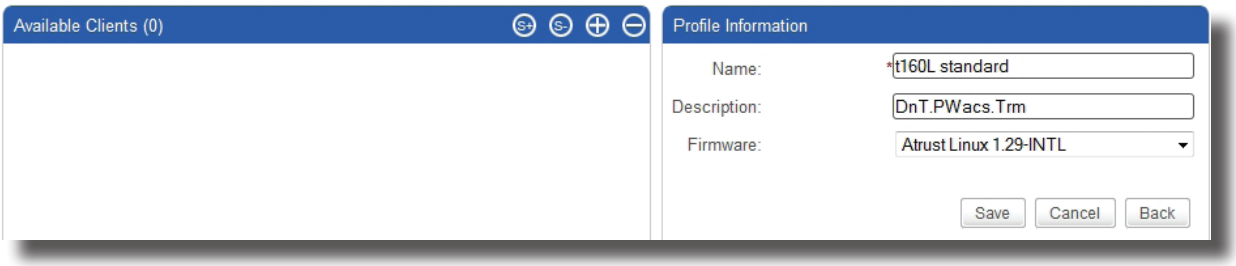
> **NOTE**
>
> - The Edit Configuration window for the profile (group configuration) is just like a remote version of Atrust Client Setup on a client. You can simply edit client settings for this setting profile through this window. For detailed instructions on how to configure client settings, please refer to “Configuring Client Settings” on page 97.

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

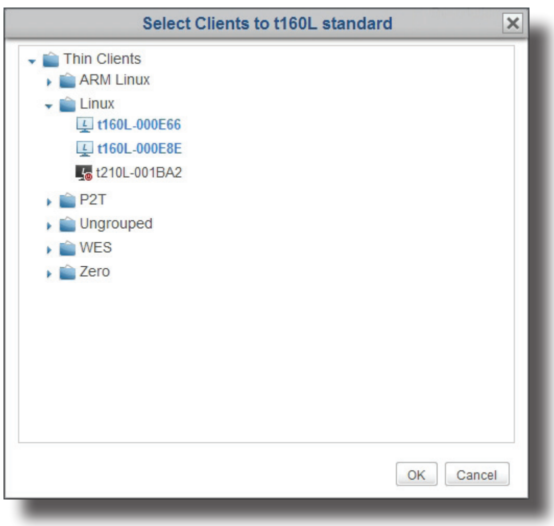
To specify the applicable scope of the setting profile, please do the following:

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



3. Click ⊕ at the right top of the Available Clients pane.
4. 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 expend 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 48 and "3.3.3 Client Detection and Management" on page 39 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 64.

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

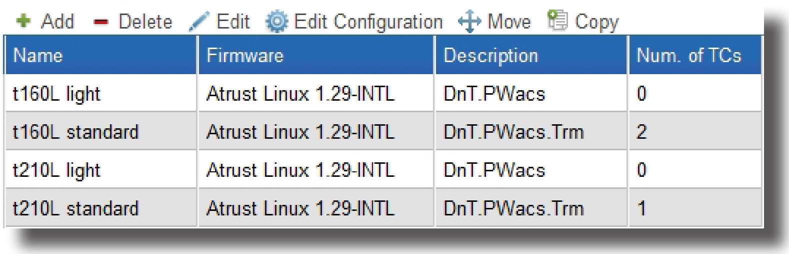
- Only a well defined setting profile is actually used for remote configuration of multiple clients. If the applicable scope of a setting profile is not specified, the profile (group configuration) doesn't affect any client.
- From now on, we will call a client configuration set up by applying a shared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



Name	Firmware	Description	Num. of TCs
t160L light	Atrust Linux 1.29-INTL	DnT.PWacs	0
t160L standard	Atrust Linux 1.29-INTL	DnT.PWacs.Trm	2
t210L light	Atrust Linux 1.29-INTL	DnT.PWacs	0
t210L standard	Atrust Linux 1.29-INTL	DnT.PWacs.Trm	1

3. Click to select the desired setting profile.
4. Select **Edit Configuration** to adjust client settings for the selected profile or select **Edit** to adjust the profile information and/or the applicable scope of the selected profile.
   - 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 55.

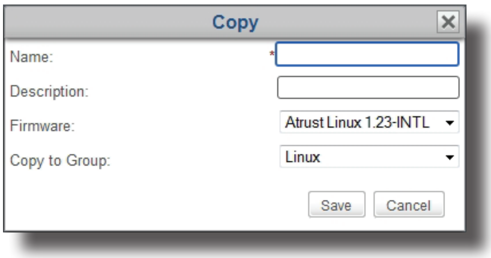
- To adjust the applicable scope of this profile, use to make desired changes, and then click **Save** to apply.

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, firmware version, profile group for this profile, and then click **Save** to confirm.



NOTE

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

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

NOTE

- The following steps are simliar 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 55.

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

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

NOTE

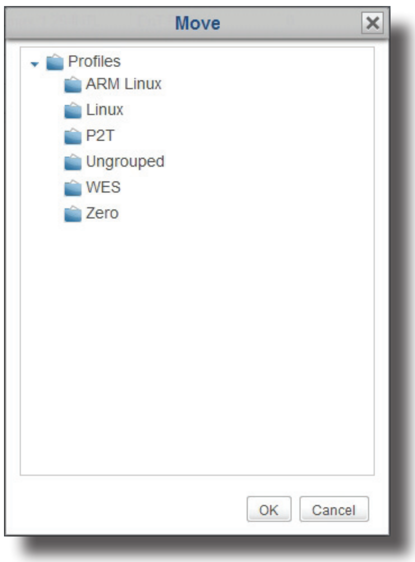
- If you create a new profile by copying a well-defined setting profile, only the part of client settings is copied. The applicable scope of the original profile is not included.

9. Click to select the newly created profile, and then click **Edit** on the top of the Profile list.
10. Both the Profile Information and Available Clients panes appear in Management area.
11. Click at the right top of the Available Clients pane.
12. 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.
13. Click on arrows to expend 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.
14. After completion, click **OK** to confirm the selection of applicable clients.
15. 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.

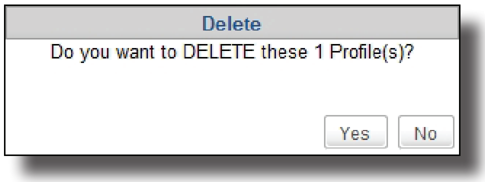


5. Click to select the desired profile group, and then click **OK** to confirm.
6. The selected setting profile is moved to the desired profile group.

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 fo 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.

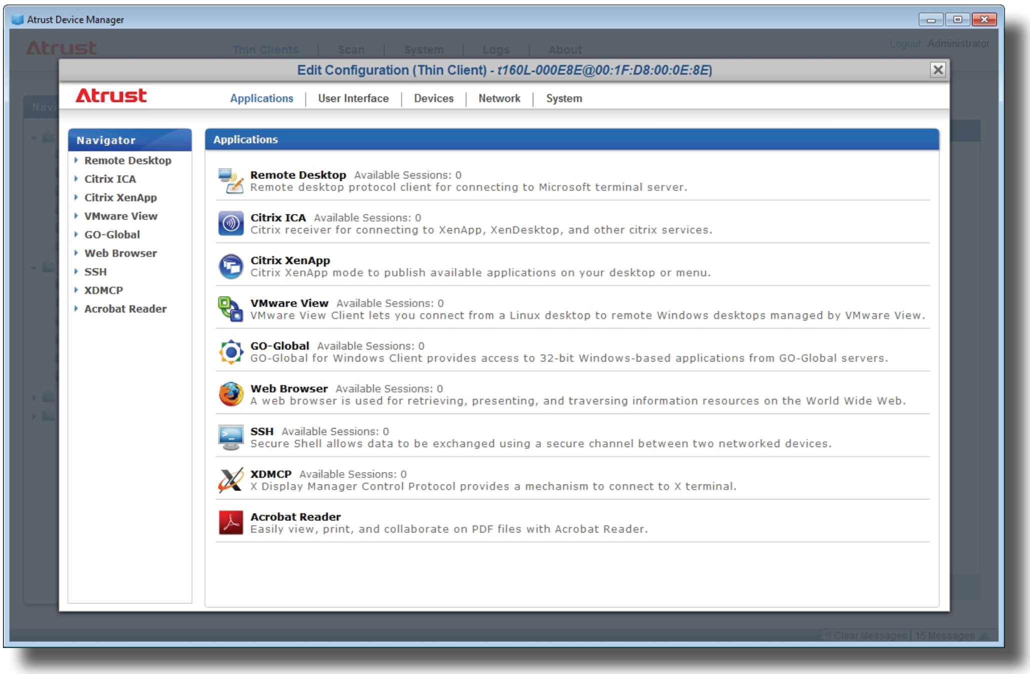
NOTE

- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 52.

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.

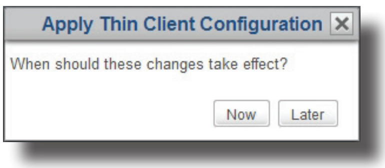


5. Use this window to edit the individual configuration.

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 63 for more details).
- For detailed instructions on how to configure specific client settings, please refer to chapter 4 "Configuring Client Settings" on page 97.

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 52.

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 55.

STEP 2: Apply an individual configuration to the client

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

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 61.

3.4.16 Pushing Settings to Clients through Your Local Network

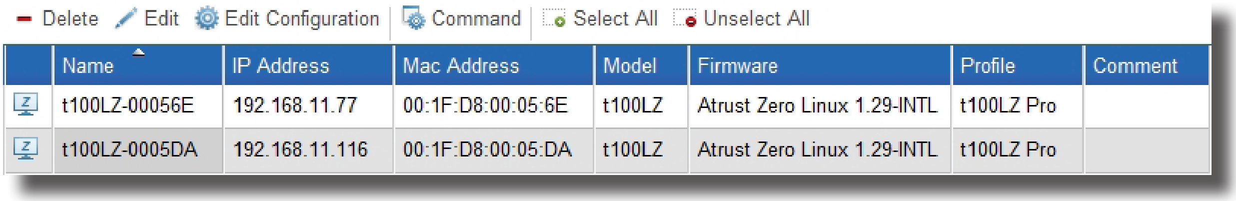
The **Push Settings** feature enables you to sync up client configuration on a client with the one set up in remote Atrust Device Manager. You can then configure client settings remotely through your local network.

> **NOTE**
>
> - Some settings can only be configured locally on clients. See section "3.4.9 Client Settings" on page 52 and chapter 4 "Configuring Client Settings" on page 97 for more details.

Pushing Settings to a Client

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

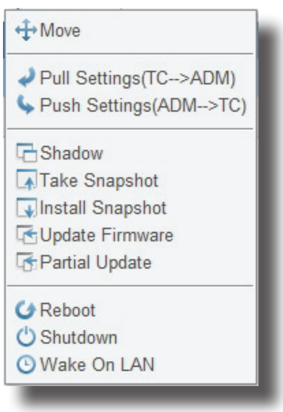
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.



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

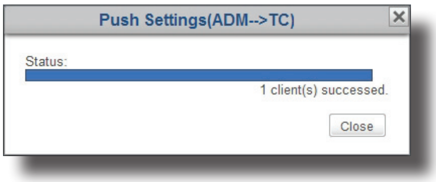
> **NOTE**
>
> - To select more than one client, Ctrl-click to select the desired clients.
> - Ensure that all selected clients are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 51.

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.

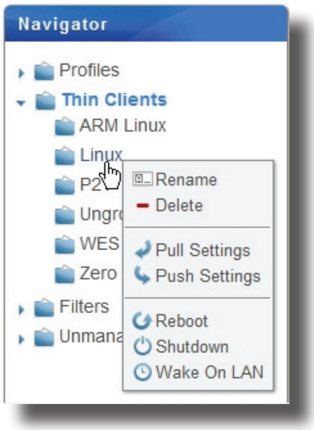


9. After completion, click **Close** to exit.
10. Check the status of the client through the Status icon in front of it. If needed, restart the client to complete the configuration changes on the client.

Pushing Settings to a Client Group

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

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

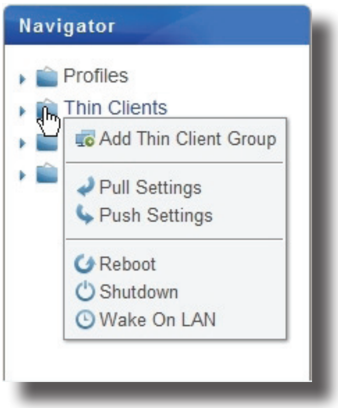
- Ensure that all clients in the group are powered up. Otherwise, you may fail to push settings to some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 51.

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:

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 51.

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

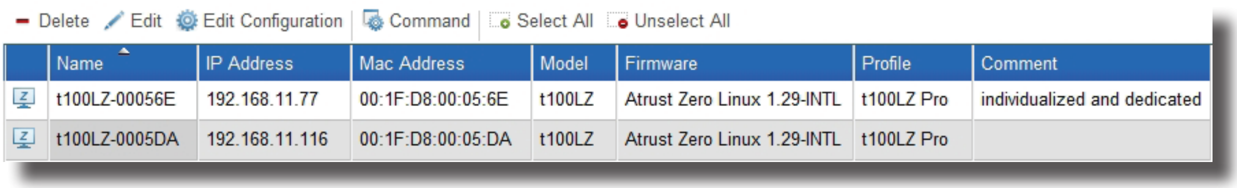
The **Pull Settings** feature enables you to retrieve settings from a client and store in Atrust Device Manager, which help you sync up the client configuration in Atrust Device Manager with the one set up locally on a client.

> **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 52 and chapter 4 "Configuring Client Settings" on page 97 for more details.

Pull Settings from a Client

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

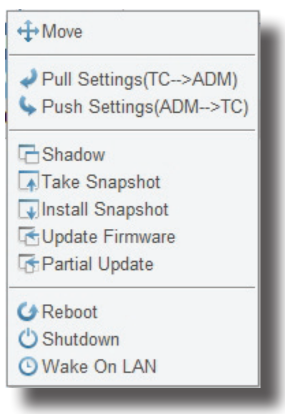
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and click to select the client group to which the desired client belongs.
2. The Client list appears.



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

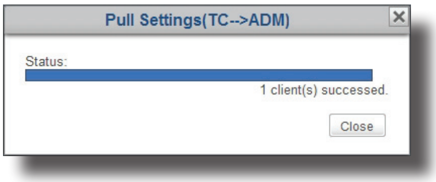
> **NOTE**
> - To select more than one client, Ctrl-click to select the desired clients.
> - Ensure that all selected clients are powered up. Otherwise, you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 51.

4. The Command menu appears.



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

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

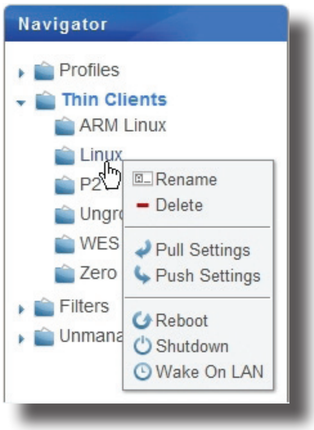


9. After completion, click **Close** to exit.

Pull Settings for a Client Group

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

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



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

NOTE

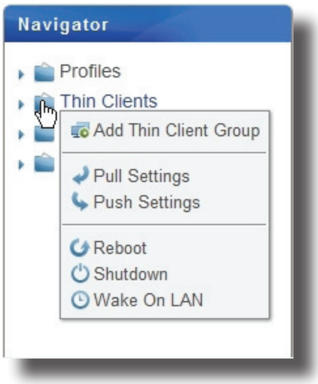
- Ensure that clients in the selected group are all powered up. Otherwise you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 51.

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

Pull Settings for all Client Group

To pull settings fro 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.

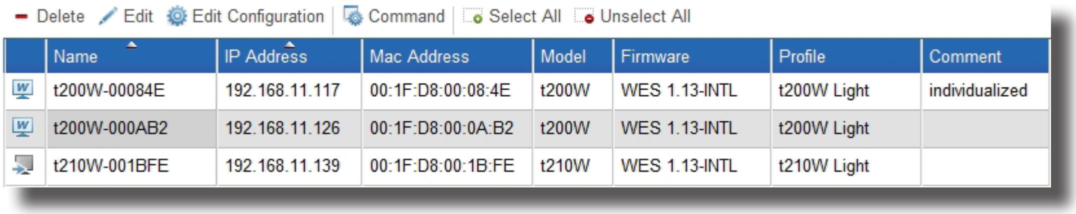
> **NOTE**
>
> - Ensure that all clients are powered up. Otherwise, you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 51.

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

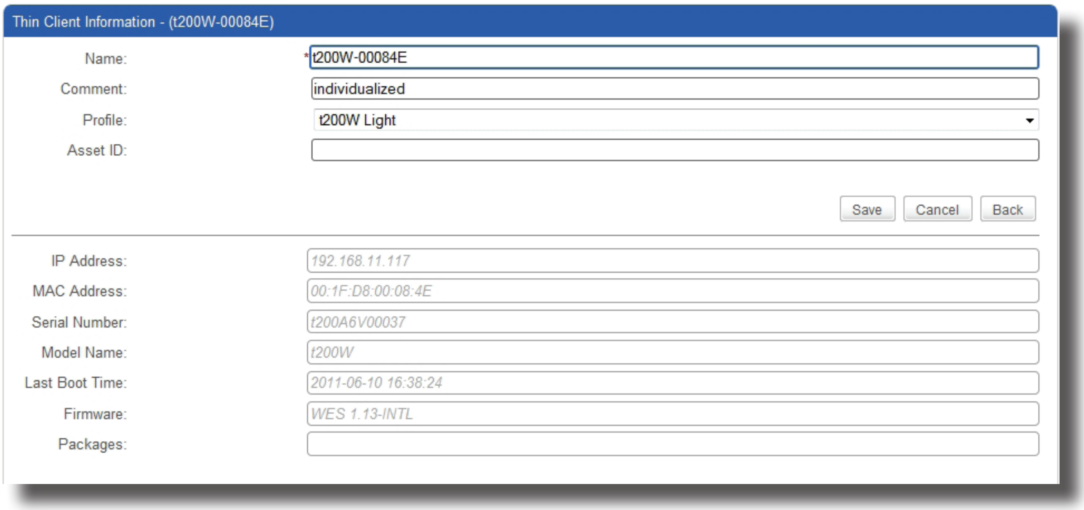
3.4.18 Editing or Viewing the Basic Information about a Client

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.



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.



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.

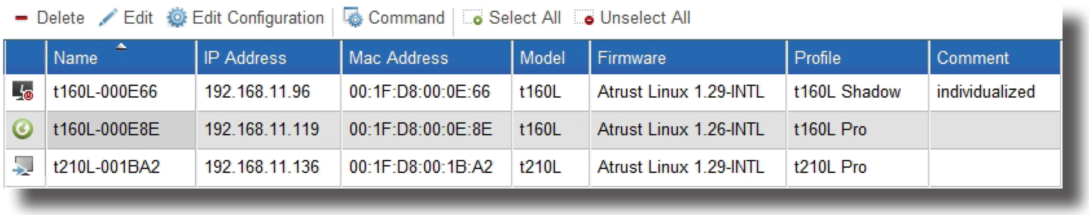
3.4.19 Rebooting Clients through Your Local Network

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

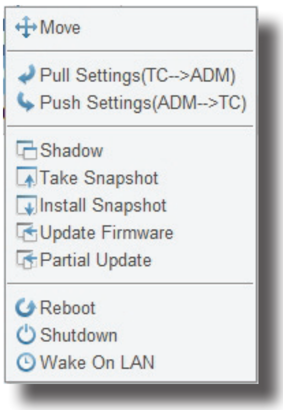
To restart a client through your local network, please do the following:

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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t160L-000E66	192.168.11.96	00:1F:D8:00:0E:66	t160L	Atrust Linux 1.29-INTL	t160L Shadow	individualized
	t160L-000E8E	192.168.11.119	00:1F:D8:00:0E:8E	t160L	Atrust Linux 1.26-INTL	t160L Pro	
	t210L-001BA2	192.168.11.136	00:1F:D8:00:1B:A2	t210L	Atrust Linux 1.29-INTL	t210L Pro	

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



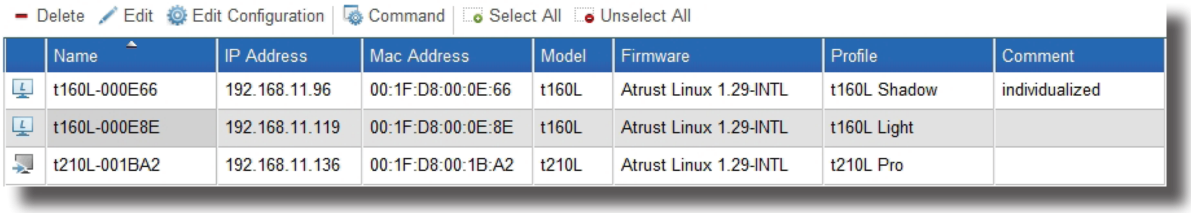
4. Click to select **Reboot**.

> **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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t160L-000E66	192.168.11.96	00:1F:D8:00:0E:66	t160L	Atrust Linux 1.29-INTL	t160L Shadow	individualized
	t160L-000E8E	192.168.11.119	00:1F:D8:00:0E:8E	t160L	Atrust Linux 1.29-INTL	t160L Light	
	t210L-001BA2	192.168.11.136	00:1F:D8:00:1B:A2	t210L	Atrust Linux 1.29-INTL	t210L Pro	

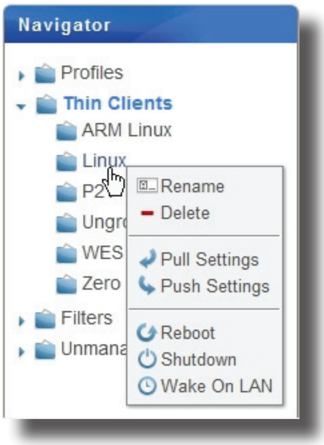
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

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.

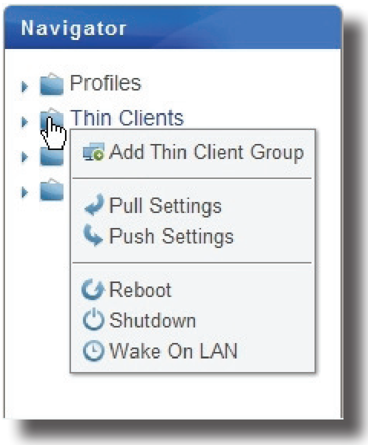
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

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.

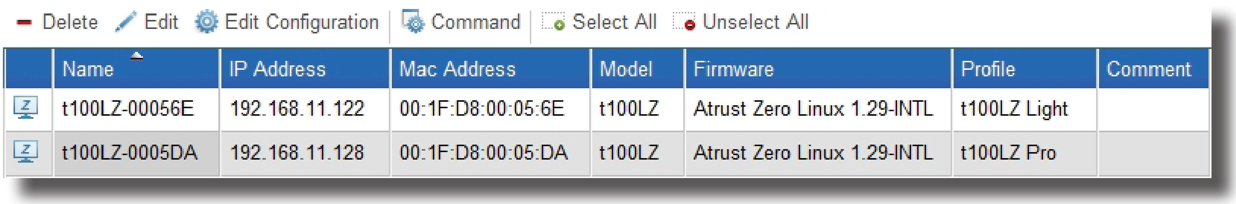
> **NOTE**
> - For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

3.4.20 Shutting Down Clients through Your Local Network

Shutting Down a Client through Your Local Network

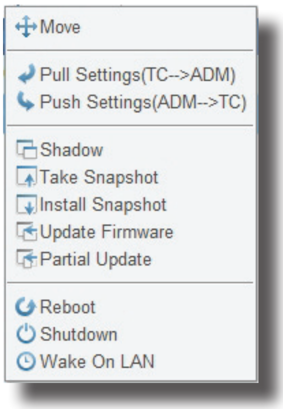
To shut down a client through your local network, please do the following:

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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t100LZ-00056E	192.168.11.122	00:1F:D8:00:05:6E	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Light	
	t100LZ-0005DA	192.168.11.128	00:1F:D8:00:05:DA	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Pro	

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



4. Click to select **Shutdown**.

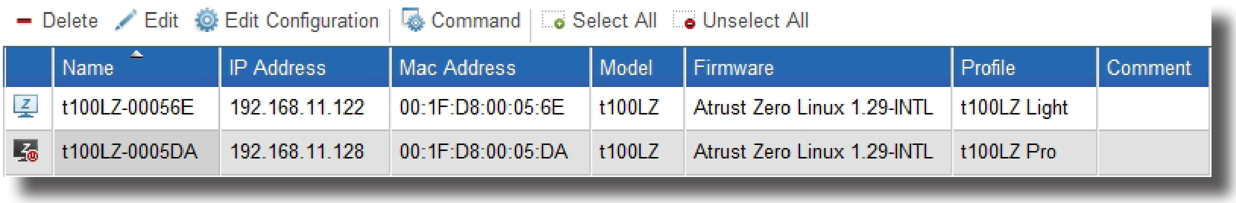
NOTE

- 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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t100LZ-00056E	192.168.11.122	00:1F:D8:00:05:6E	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Light	
	t100LZ-0005DA	192.168.11.128	00:1F:D8:00:05:DA	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Pro	

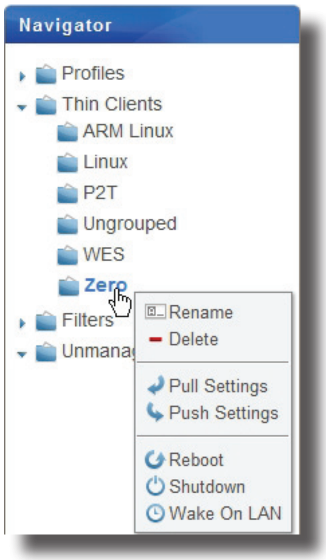
NOTE

- For information on the meanings of the Status icons, please refer to “3.4.8 Understanding Client Status Icons” on page 51.

Shutting Down a Client Group through Your Local Network

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

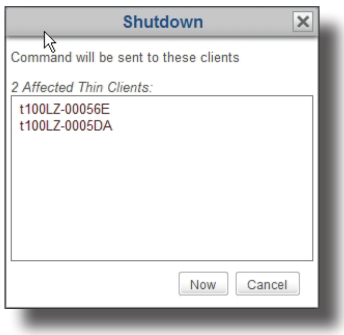
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree.
2. Right-click on the desired client group to open a popup menu.



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.



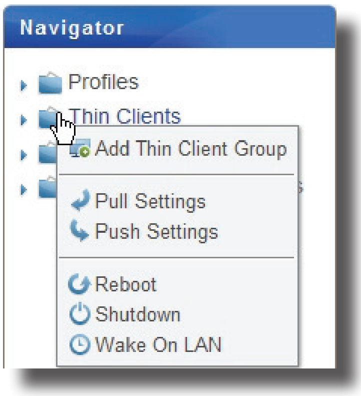
5. Click **Now** to confirm.
6. On each client of this group, a warning message appears to notify the user of the planned shutdown and allow the user to cancel the action if necessary.
7. After completion, the Status icons will indicate clients of this group are off-line.

> **NOTE**
> - For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

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.

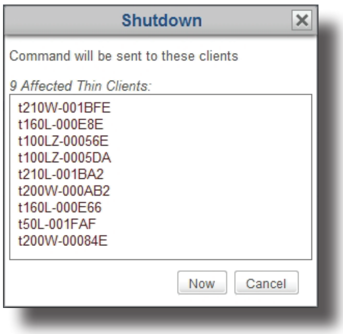


2. Click to select **Shutdown**.

WARNING

- Ensure that no important tasks are performed on 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 51.

3.4.21 Waking Clients through Your Local Network

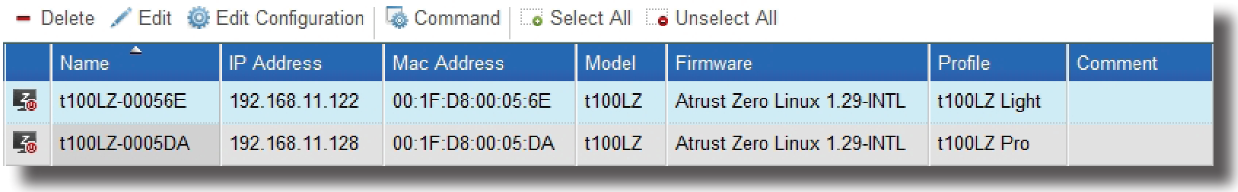
The **Wake on LAN** feature enables you to wake multiple clients through your local network if clients are connected to power outlets and the local network.

> **NOTE**
> - t50L does not support the **Wake On LAN** feature.

Waking a Client through Your Local Network

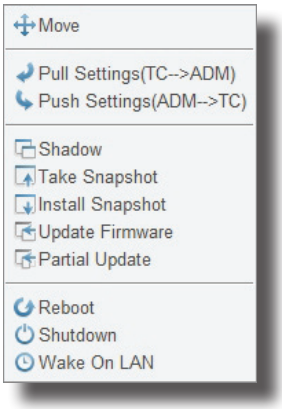
To wake a client through your local network, please do the following:

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.



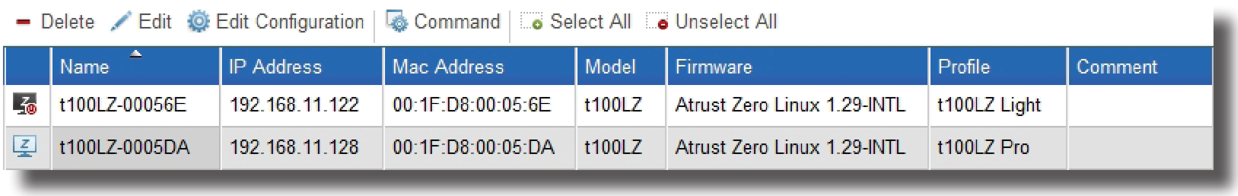
	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t100LZ-00056E	192.168.11.122	00:1F:D8:00:05:6E	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Light	
	t100LZ-0005DA	192.168.11.128	00:1F:D8:00:05:DA	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Pro	

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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t100LZ-00056E	192.168.11.122	00:1F:D8:00:05:6E	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Light	
	t100LZ-0005DA	192.168.11.128	00:1F:D8:00:05:DA	t100LZ	Atrust Zero Linux 1.29-INTL	t100LZ Pro	

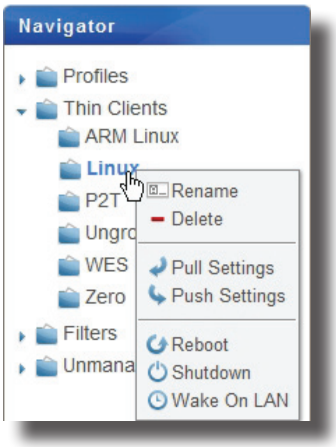
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

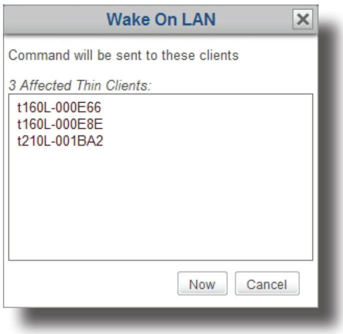
Waking a Client Group through Your Local Network

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.

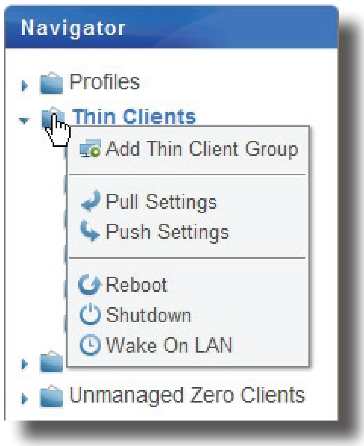
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 51.

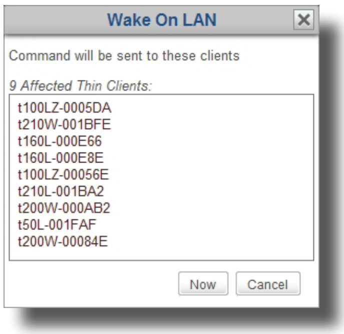
Waking All Client Groups through Your Local Network

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 51.

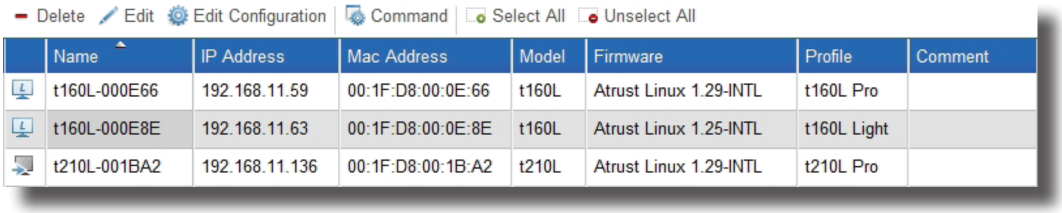
3.4.22 Updating Client Firmware

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

NOTE

- Updating client firmware will NOT erase any client configuration.

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.

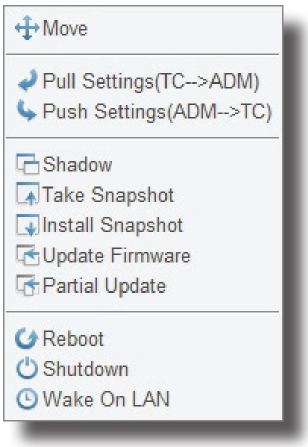
NOTE

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

WARNING

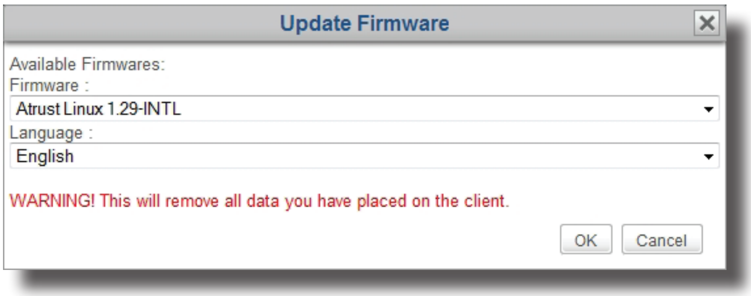
- Ensure that no important tasks are performed on the selected clients.

4. The Command menu appears.



5. Click to select **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.

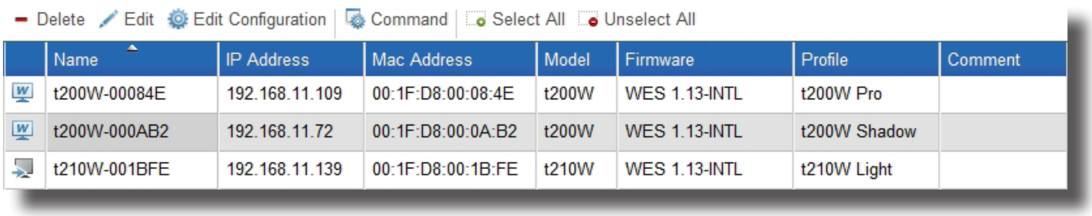
3.4.23 Installing Software Packages

To install a software package for your client, please do the following:

NOTE

- Installing additional software packages is allowed only for WES-based (Windows Embedded Standard) clients.

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



Name	IP Address	Mac Address	Model	Firmware	Profile	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.

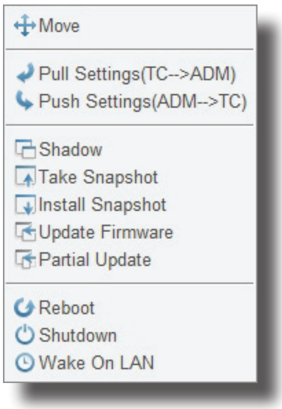
NOTE

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

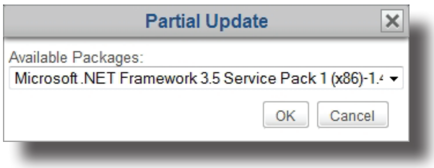
WARNING

- 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 "3.4.18 Editing or Viewing the Basic Information about a Client" on page 70.

3.4.24 Taking Client Snapshots

A snapshot is the system backup of a client at a specific point of time, which you can use to restore your client to that system state.

NOTE

- Atrust t-series zero clients (t100LZ/t160LZ/t200LZ/t210LZ) and Atrust t50L thin client don't support the **Snapshot** feature.

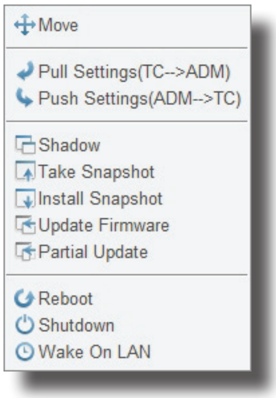
To take a system snapshot for a client, please do the following:

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.

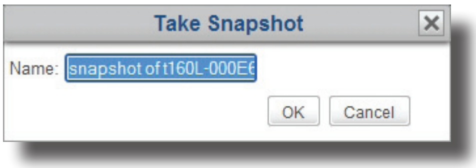
NOTE

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

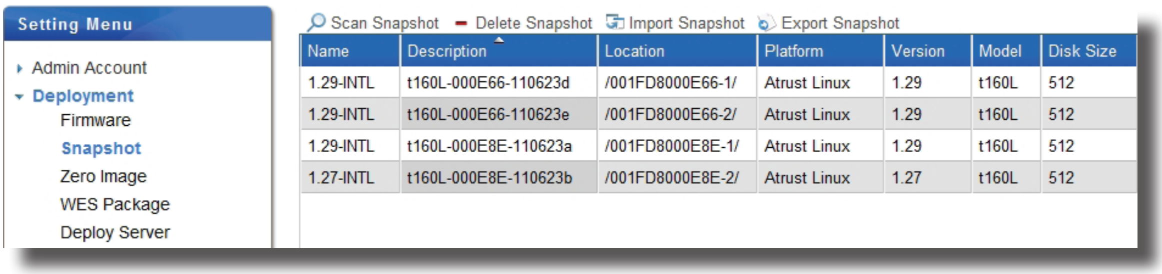
4. The Command menu appears.



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.



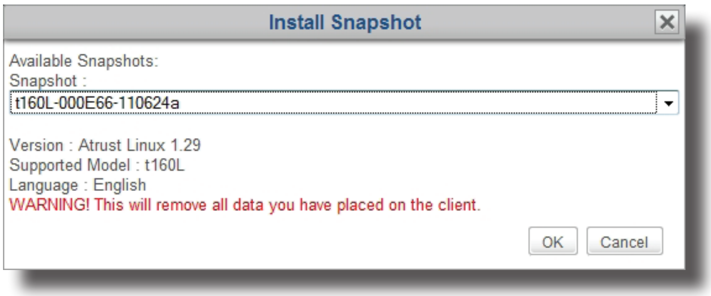
NOTE

- To access the Snapshot list, click **System** tab, and then click **Deployment** > **Snapshot**.
- Refer to section "3.2.7 Managing Client Snapshots" on page 27 for instructions on how to manage your snapshots.

3.4.25 Restoring Client Snapshots

To restore a system backup 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.

3.4.26 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's required to execute the **Shadow** feature.
- Atrust t50L doesn't support 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.

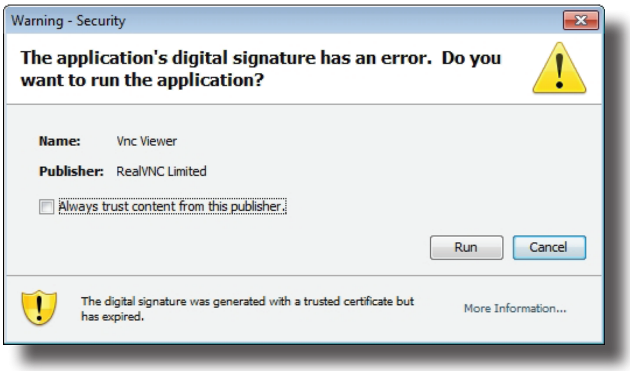
NOTE

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

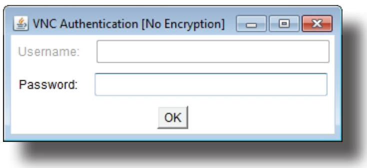
4. The Command menu appears.
5. Click to select **Shadow**.
6. The Java software is launched displaying an animated picture on the screen as below.

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.

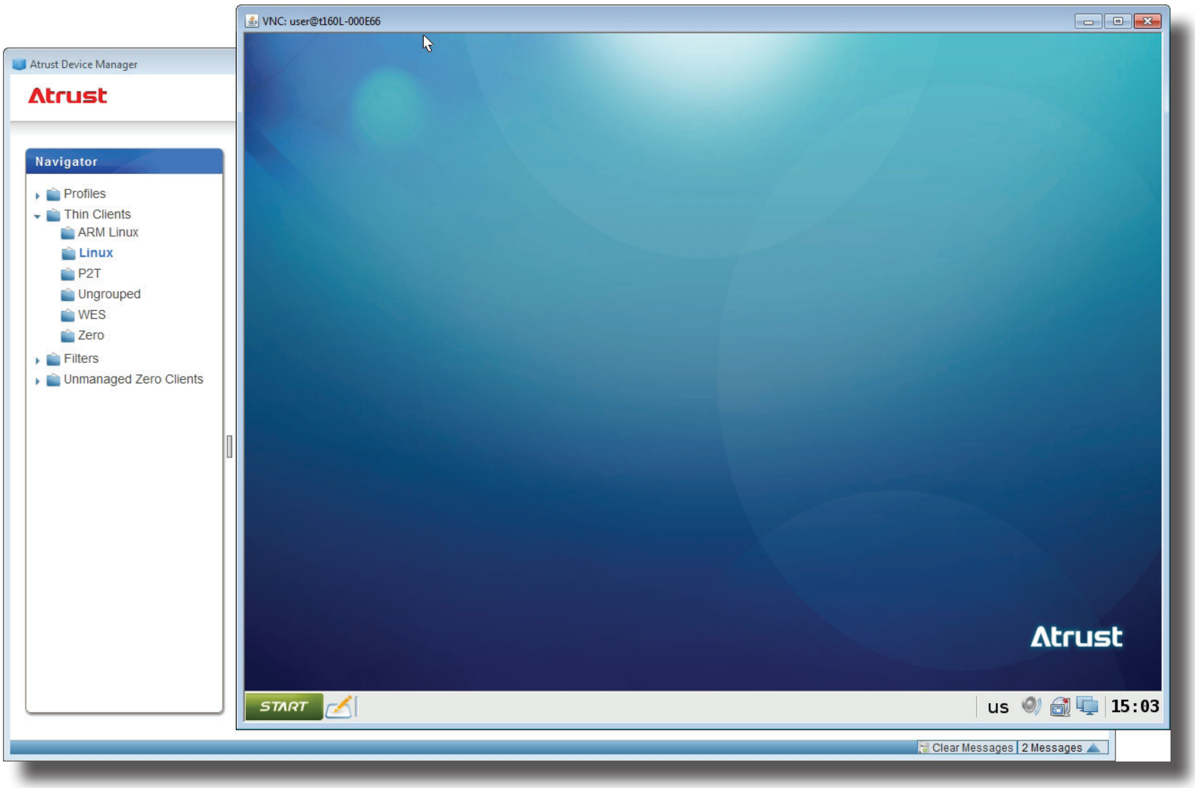


9. The VNC Authentication window may appear prompting you for the Shadow password.



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.

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

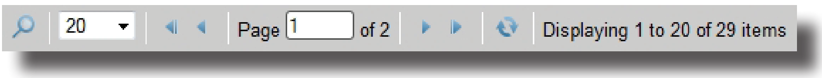
At the bottom of each Profile, Client, Zero Client, or Log list, you can access Quick Search to help you dig out the profiles, clients, or event logs.

NOTE

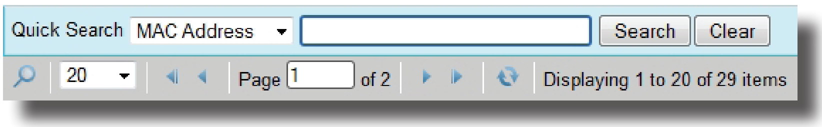
- Event logs will be introduced on section “3.5.1 Logs Tab Overview” on page 91.
- You can also use filters to find out the desired clients within the managed clients. For details, please refer to section “3.4.28 Digging Out Clients with Filters” on page 87.

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 **Thin Clients** tab, click **Unmanaged Zero Clients** to open the Zero 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.

3.4.28 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

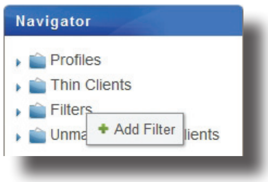
- You can also use Quick Search to dig out clients within managed clients and unmanaged zero clients. For details, please refer to “3.4.27 Digging Out Profiles, Clients, or Event Logs with Quick Search” on page 87.

Adding a Filter

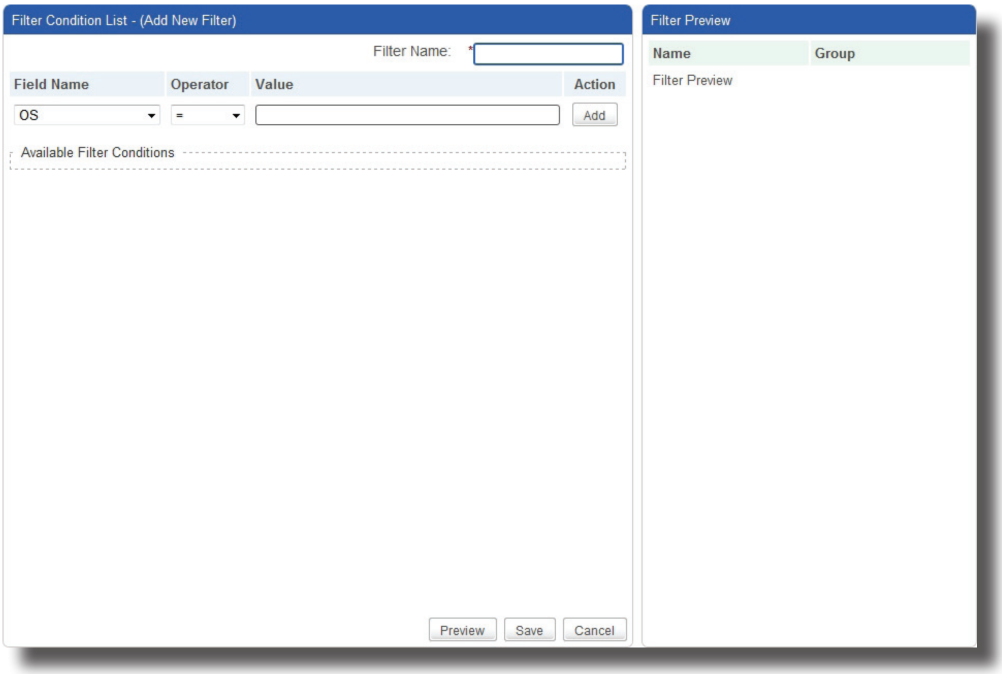
To add a filter, please do the following:

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 Filter Condition List and Filter Preview panes appear in Management area.



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

NOTE

- The available operators and their meanings are as follows:

Available Operators for Filter Conditions	
Filter	Meaning
=	is equal to
!=	is not equal to
~=	is similar to
>	is greater than
>=	is greater than or equal to
<	is less than
<=	is less than or equal to

- Most information about a client, which can be used as filter conditions, are available in the Thin Client Information pane. To access Thin Client Information pane, please refer to section "3.4.18 Editing or Viewing the Basic Information about a Client" on page 70 for detailed instructions.

7. Click **Add** to add a condition to a filter.

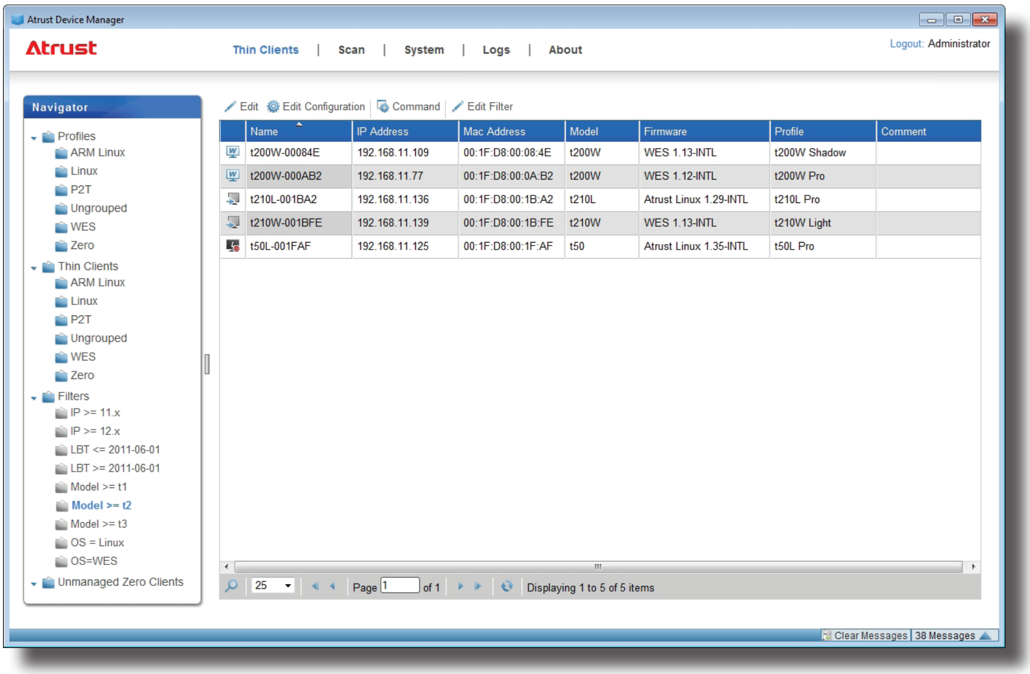
8. Repeat steps 5 through 7 to add a new condition.
9. Click **Preview** to view the result of a filter. The result is displayed in the Filter Preview pane.
10. Click **Save** to create the filter.

Using a Client Filter

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

To use a client filter, please do the following:

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



3.4.29 Managing Your Filters

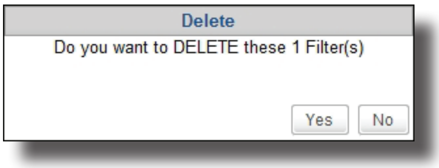
Deleting a Filter

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:

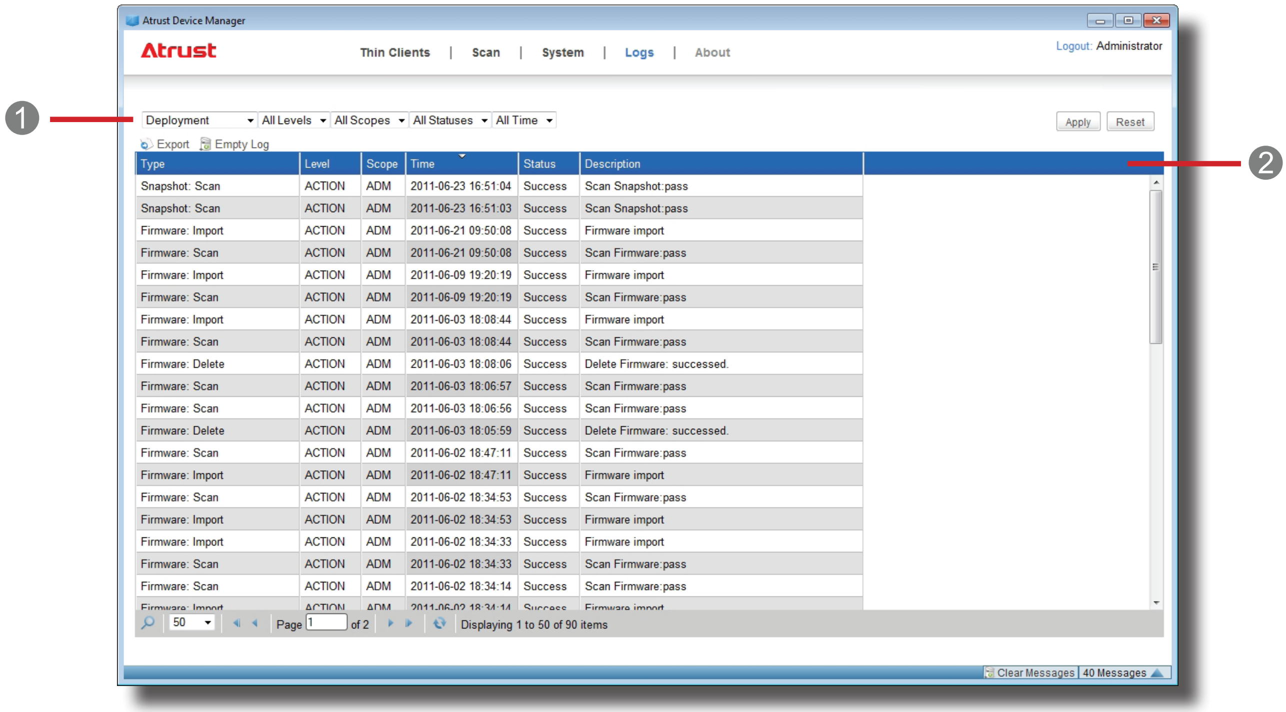
1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.
3. Click to select the desired filter, and then click **Edit** on the top of the Filter list.
4. The Filter Condition List and Filter Preview panes appear in Management area.
5. Adjust conditions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

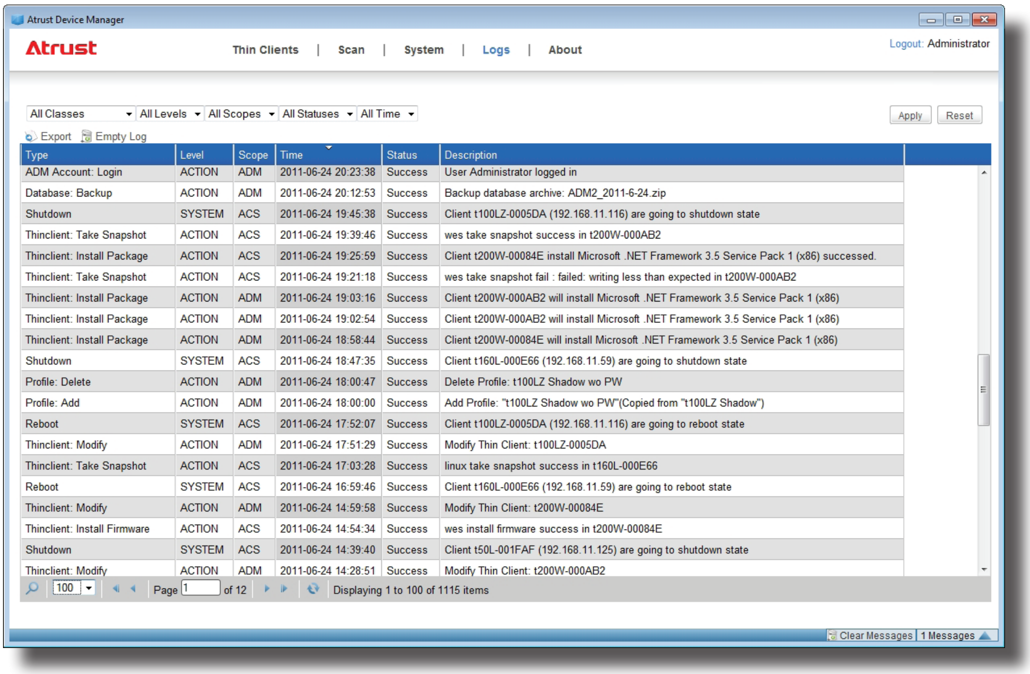
3.5.2 Available Tasks at a Glance

No.	Available Task	Section	Page
1	viewing your event logs	3.5.3	92
2	exporting your event logs	3.5.4	92
3	emptying your event logs	3.5.5	93

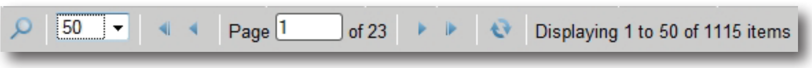
3.5.3 Viewing Event Logs

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

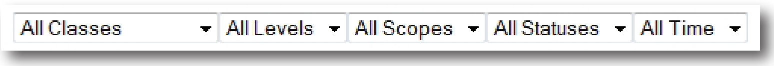
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.



- 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:

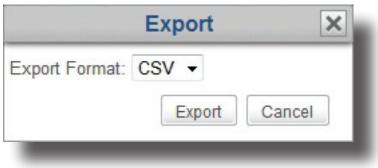
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.

- 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.

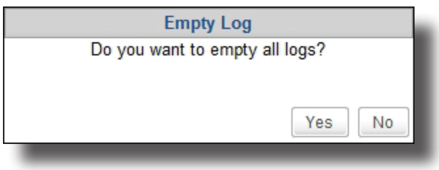
3.5.5 Emptying Event Logs

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 don't 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.

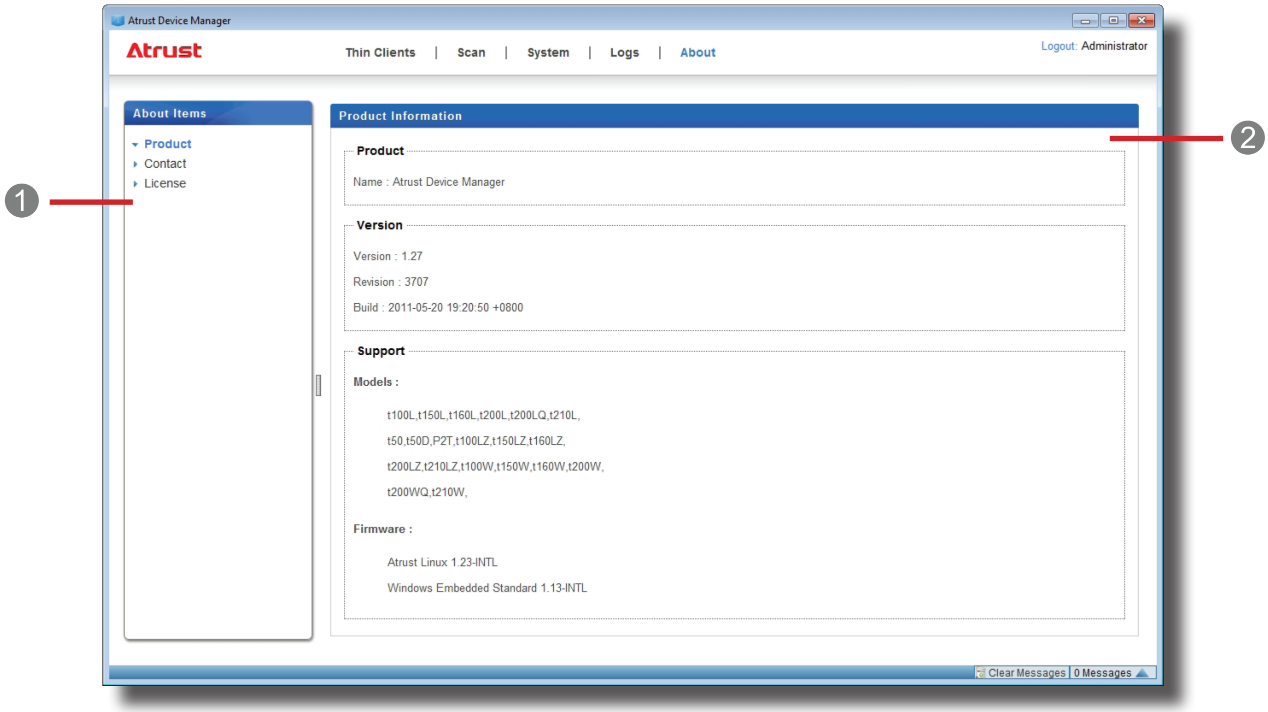
> **NOTE**
> - A new log entry about emptying log will be added to the Log list.

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	95
2	viewing Atrust contact information	3.6.4	95
3	viewing Atrust Software License Agreement	3.6.5	95

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.

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 99

4.2 Client Settings at a Glance

available client setting items on Atrust Device Manager and Atrust Client Setup 99

4.3 Editing or Adjusting a Group Configuration

how to edit or adjust a group configuration (profile) shared by a group of clients 101

4.4 Editing or Adjusting an Individual Configuration

how to edit or adjust an individual configuration applied only to a single client 102

4.5 Configuring Client Settings with Atrust Client Setup

how to configure client settings with Atrust Client Setup 104

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. Atrust t-series clients can meet a wide range of desktop virtualization forms and needs. But, to get your t-series client ready for use, you need to configure 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 and the used operating system.
- Some setting items are only available locally on clients. You can adjust those settings through Atrust Client Setup.
- All settings that are only available locally on clients are marked with an asterisk (*) in the table below.

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure RDP (Remote Desktop Protocol) connection settings and create a desktop shortcut for Remote Desktop sessions.
	Citrix ICA		Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create a desktop shortcut for accessing application/desktop delivery services.
	Citrix XenApp		Click to configure Citrix XenApp connection settings and create a Start menu and/or desktop folder for accessing application delivery services.
	VMware View		Click to configure VMware View Client connection settings and create a desktop shortcut for accessing desktop delivery services.
	GO-Global		Click to configure GO-Global Client connection settings and create a desktop shortcut for accessing application delivery services.
	Web Browser		Click to configure general (for WES-based clients only) or specific browser session settings. A desktop shortcut is created for specific browser sessions launched with the desired initial web page. The used Web browser may vary, depending on the operating system of your client model.
	SSH		Click to configure SSH (Secure Shell) session settings and create a desktop shortcut for SSH sessions.
	XDMCP		Click to configure XDMCP (X Display Manager Control Protocol) connection settings and create a desktop shortcut for accessing desktop delivery services.
	Acrobat Reader		Click to enable/disable Acrobat Reader on your client.

Tab	Setting	Icon	Description
User Interface	Display		Click to configure your display settings.
	Desktop		Click to customize your system language and desktop.
	Keyboard		Click to adjust your keyboard settings.
	Mouse		Click to adjust your mouse settings.
	Screensaver		Click to configure your screensaver settings.
Devices	USB Storage		Click to configure settings for USB storage devices.
	Audio		Click to configure settings for audio devices.
	Printer *		Click to add local or network printers for your client.
Network	Ethernet *		Click to configure your wired network settings.
	PPPoE *		Click to configure PPPoE connection settings and create an Internet connection.
	VPN *		Click to configure VPN (Virtual Private Network) connection settings and create a secure and reliable connection over the Internet.
	Hosts		Click to create the mapping of IP addresses to the names of host servers. You can then use the name of a host server instead of its IP address wherever you need to specify an IP address while configuring client settings.
	Wireless *		Click to configure your wireless network settings and create a wireless connection.

Tab	Setting	Icon	Description
System	Time and Date		Click to configure date and time settings.
	Password		Click to configure your password settings.
	Firmware Update *		Click to update firmware from the host server. This feature is only applicable when this client is managed by the Atrust Device Manager software (see the note below).
	Snapshot		Click to take a snapshot (system backup at a specific point of time) for your client, which you can use to restore your client to that system state when needed.
	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.
	Miscellaneous		Click to change the name of the client.
	Terminal		Click to enable/disable the execution of the text-based (command-line) functions.
	FBWF		Click to figure FBWF (File Based Write Filter) settings. Enabling FBWF option will redirect all writes targeted for disk volumes to a RAM cache. All system changes will only affect the session where the changes are made.

4.3 Editing or Adjusting a Group Configuration

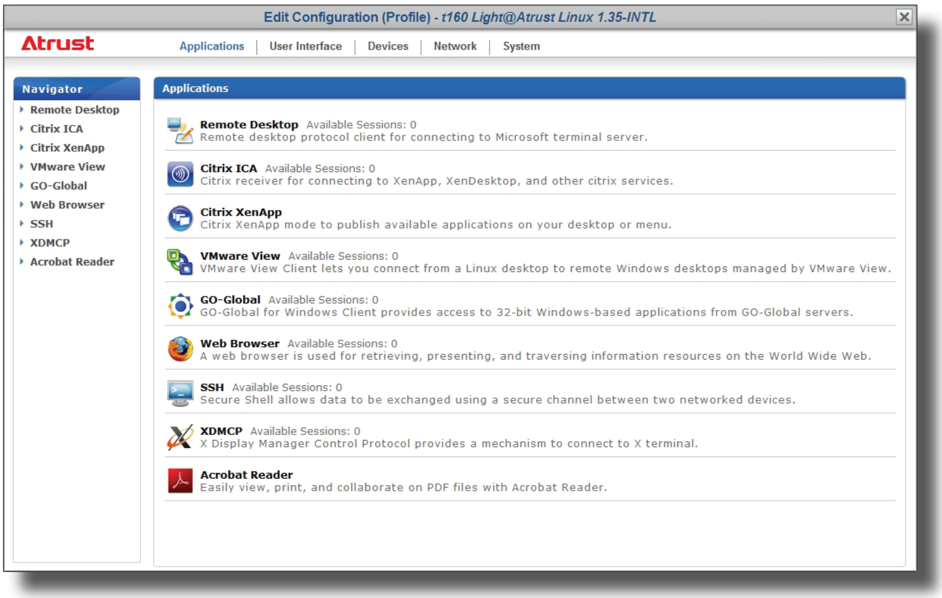
On Atrust Device Manager, you can edit client settings for a group of clients through the Edit Configuration window for a profile (group configuration). Through this window, all remotely configurable settings can be edited, then you can push settings to the target group of clients defined in that profile 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 55.
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 52.
- 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 102.

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 globe icon located close to a setting item to enable the adjustment of the value.

> **NOTE**
>
> - The gray globe icon will become blue when you click it to enable the adjustment of the value.
> - When a globe icon becomes blue, 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.

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.

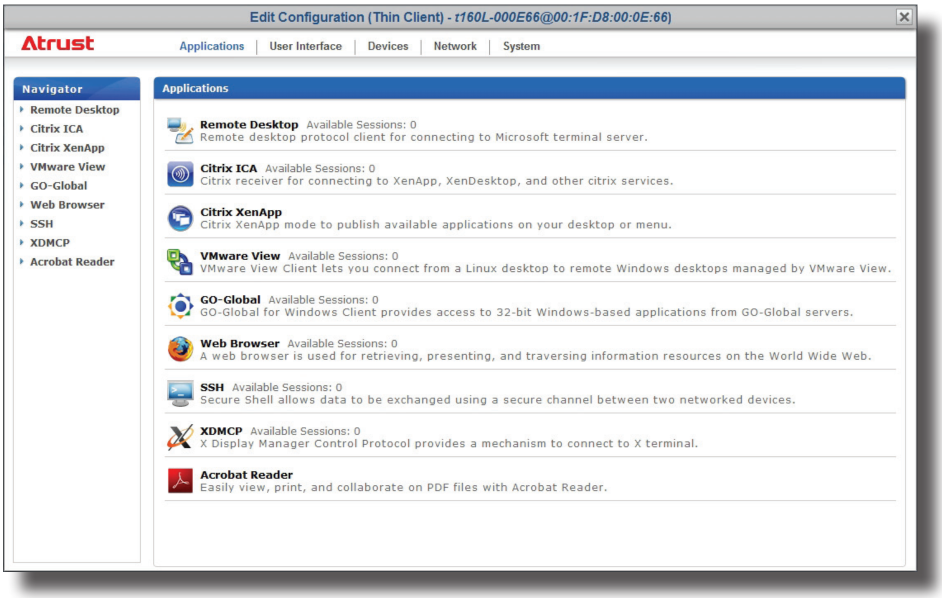
> **NOTE**
>
> - In this section, we will focus on the editing/adjusting of an individual configuration in greater detail. For general instructions on how to create an individual configuration or on how to open the Edit Configuration window for a client, please refer to section "3.4.14 Using Individualized Client Settings" on page 61.

NOTE

- To have a basic understanding of client configuration, please refer to section “3.4.9 Client Settings” on page 52.
- 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 individual clients.

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.

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.

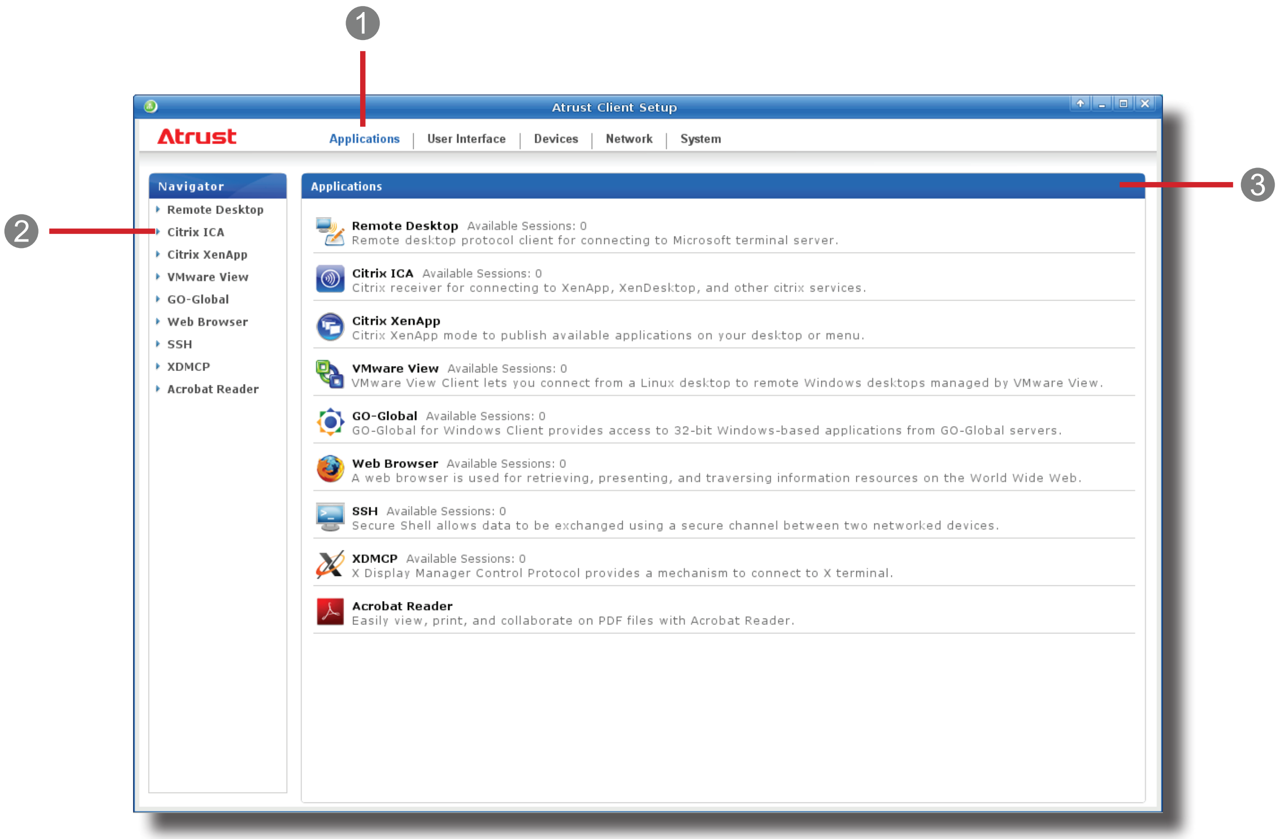
NOTE

- For the list of client settings only locally accessible on clients, please refer to section "4.2 Client Settings at a Glance" on page 99.
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 52.

4.5.1 Atrust Client Setup for Linux-based Clients

To access Atrust Client Setup on a Linux-based client, please do the following:

1. Click **START** > **Settings** > **Atrust Client Setup**.
2. The Atrust Client Setup window appears.

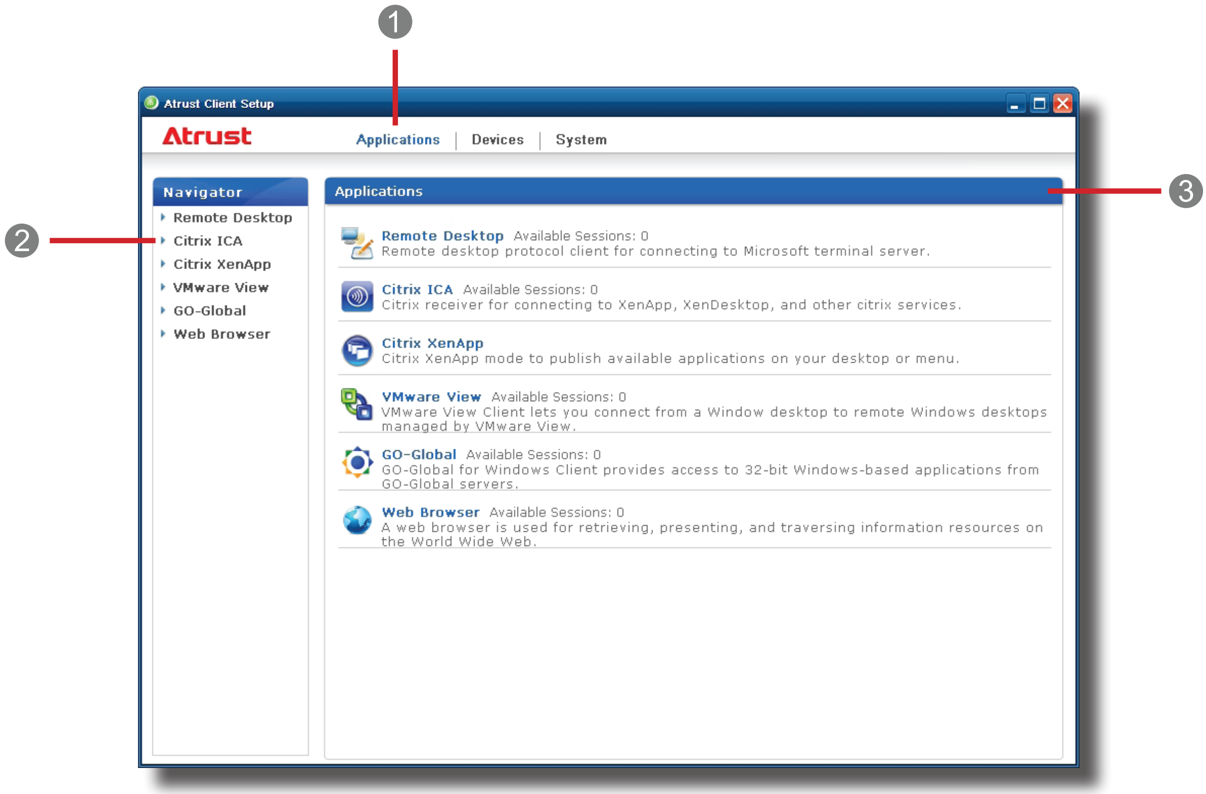


Interface Elements		
No.	**Name**	**Description**
1	Main Menu area	Click to select a category of client settings.
2	Navigation area	Click to select a setting item under a category.
3	Configuration area	Configure setting values when a setting item is selected.

4.5.2 Atrust Client Setup for WES-based Clients

To access Atrust Client Setup on a WES-based (Windows Embedded Standard) client, please do the following:

1. Click **Start** > **All Programs** > **Atrust Client Setup**.
2. The Atrust Client Setup window appears.



Interface Elements

No.	Name	Description
1	Main Menu area	Click to select a category of client settings.
2	Navigation area	Click to select a setting item under a category.
3	Configuration area	Configure setting values when a setting item is selected.

Atrust

Taiwan

Tel: +886 3 3288837
Fax: +886 3 3288973

3F, No.361, Fusing 1st Rd.,
Gueishan Township,
Taoyuan County 333, Taiwan

China

Tel: +86 21 60875428
Fax: +86 21 60875427

No.738, Shangcheng Rd.,
Shanghai, China