User's Manual

Atrust Device Manager

Remote and Group Management for Clients

Atrust

Version 2.41

Copyright and Trademark Statements

Disclaimer

Atrust Computer Corp. ("Atrust") makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Atrust is not liable for technical or editorial errors or omissions contained herein. The information in this document is subject to change without notice.

Trademark statements

Atrust is a trademark of Atrust Computer Corp.

Microsoft, Windows, and Windows Server are trademarks and/or registered 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 all-in-one, mobile, t-series zero / thin clients with the Atrust Device Manager console.

Manual Structure and Subjects

Chapter	Subject
1	Provides an overview of the Atrust Device Manager console.
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	**Enter**
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

1

Overview

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

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:

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

But still you need a powerful console for managing a large number of endpoint devices in a desktop virtualization infrastructure. Atrust Device Manager 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
- Pushing custom settings to a large number of clients
- Updating firmware and installing software packages for clients
- Taking client snapshots for mass deployment, system backup, and recovery
- Rebooting, powering off, and waking clients through the local network
- Scheduling automatically performed tasks
- Helping users to troubleshoot problems remotely
- Identifying clients and managing IT assets with automatically-captured client information

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 console. 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.

1.3 Supported Platforms

Atrust Device Manager supports the following operating systems:

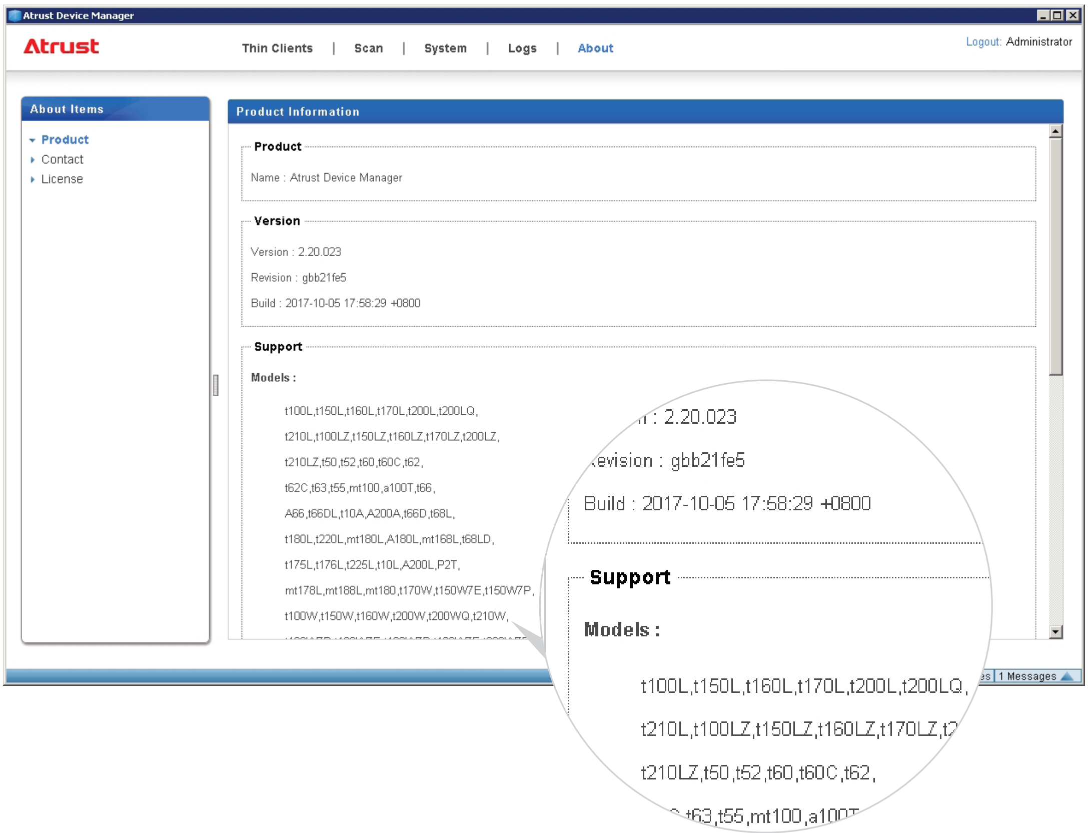
- Windows 7 / 8.1 / 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

NOTE

- To support Windows Server 2003, you will need version ***2.08.xx*** of Atrust Device Manager. Ensure that you get the right version if Windows Server 2003 is used.

1.4 Supported Endpoint Devices

On Atrust Device Manager, you can get information about supported endpoint devices through **About** tab.



Product Information

Product

Name : Atrust Device Manager

Version

Version : 2.20.023

Revision : gbb21fe5

Build : 2017-10-05 17:58:29 +0800

Support

Models :

t100L,t150L,t160L,t170L,t200L,t200LQ,
t210L,t100LZ,t150LZ,t160LZ,t170LZ,t200LZ,
t210LZ,t50,t52,t60,t60C,t62,
t62C,t63,t55,mt100,a100T,t66,
A66,t66DL,t10A,A200A,t66D,t68L,
t180L,t220L,mt180L,A180L,mt168L,t68LD,
t175L,t176L,t225L,t10L,A200L,P2T,
mt178L,mt188L,mt180,t170W,t150W7E,t150W7P,
t100W,t150W,t160W,t200W,t200WQ,t210W,

n : 2.20.023
Revision : gbb21fe5
Build : 2017-10-05 17:58:29 +0800
Support
Models :
t100L,t150L,t160L,t170L,t200L,t200LQ,
t210L,t100LZ,t150LZ,t160LZ,t170LZ,t2
t210LZ,t50,t52,t60,t60C,t62,
t63,t55,mt100,a100T

1.5 System and Network Requirements

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

- 1.0 GHz processor or the equivalent
- 1.0 GB free memory
- 2.0 GB free space for installation (100 GB or more for firmware and snapshot management)
- 1.0 Gb NIC bandwidth

The network requirements for the operation of Atrust Device Manager are as follows:

- DHCP server or DHCP-capable router (for **Update Firmware** & **Take Snapshot** features, see page 102 & 107)
- ***Wired*** networking for managed clients
- ***Same*** network segment for both Atrust Device Manager and managed clients
- Different segment, NAT, or VPN is not supported or needs special routing configuration

2

Installing and Upgrading Atrust Device Manager

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

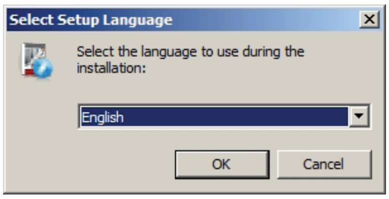
2.1 Installing Atrust Device Manager

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

NOTE

- Before proceeding, ensure that:
  - ✧ Your operating system is supported (see section 1.3 on page 4)
  - ✧ Your computer meets system requirements (see section 1.5 on page 5)
- 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 "2.3 Upgrading Atrust Device Manager" on page 15.

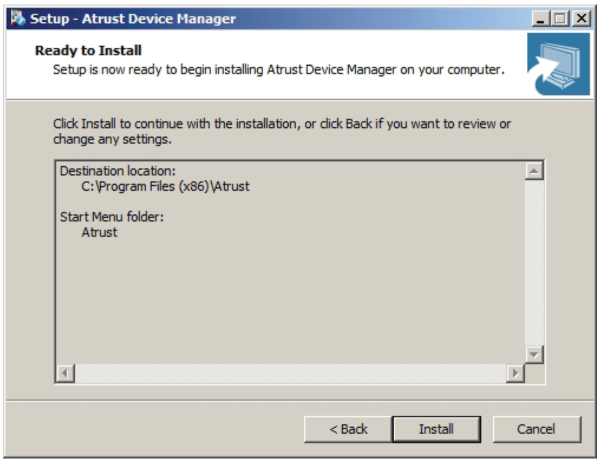
1. Get a copy of the installation program of Atrust Device Manager for your computer.
2. Log in to your computer with an administrator account, and then locate and double-click that program.
3. Select the language used during the installation, and then click **OK** to apply.


Select Setup Language

Select the language to use during the installation:

English

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


Setup - Atrust Device Manager

Ready to Install
Setup is now ready to begin installing Atrust Device Manager on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

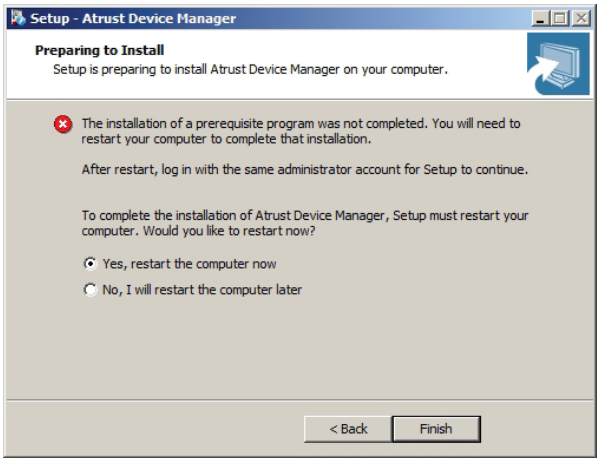
Destination location:
C:\Program Files (x86)\Atrust

Start Menu folder:
Atrust

NOTE

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

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



Preparing to Install
Setup is preparing to install Atrust Device Manager on your computer.

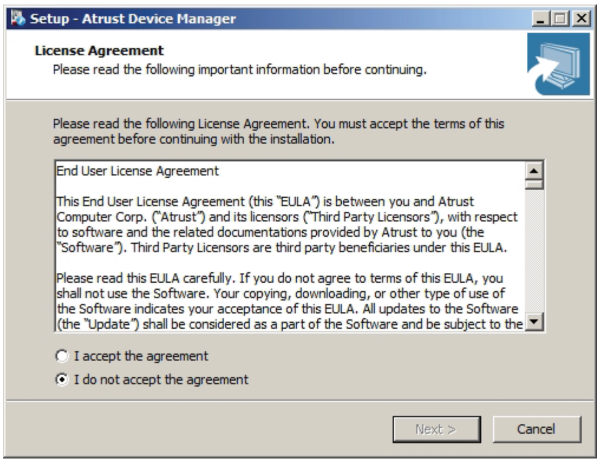
The installation of a prerequisite program was not completed. You will need to restart your computer to complete that installation.

After restart, log in with the same administrator account for Setup to continue.

To complete the installation of Atrust Device Manager, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now
○ No, I will restart the computer later

6. After restart, the License Agreement page appears. Read this agreement, click to check **I accept the agreement**, and then click **Next** to continue.



License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

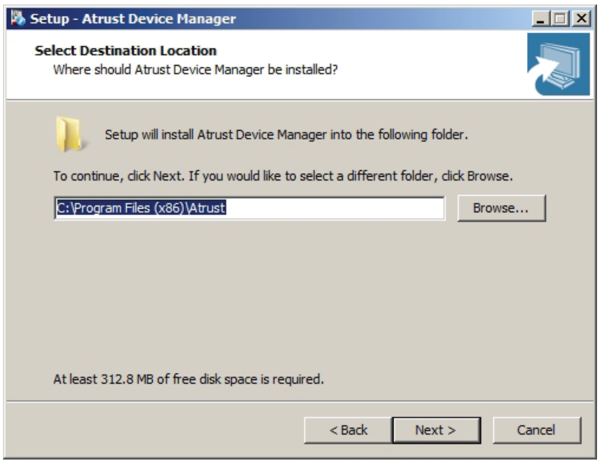
End User License Agreement

This End User License Agreement (this "EULA") is between you and Atrust Computer Corp. ("Atrust") and its licensors ("Third Party Licensors"), with respect to software and the related documentations provided by Atrust to you (the "Software"). Third Party Licensors are third party beneficiaries under this EULA.

Please read this EULA carefully. If you do not agree to terms of this EULA, you shall not use the Software. Your copying, downloading, or other type of use of the Software indicates your acceptance of this EULA. All updates to the Software (the "Update") shall be considered as a part of the Software and be subject to the

○ I accept the agreement
● I do not accept the agreement

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



Select Destination Location
Where should Atrust Device Manager be installed?

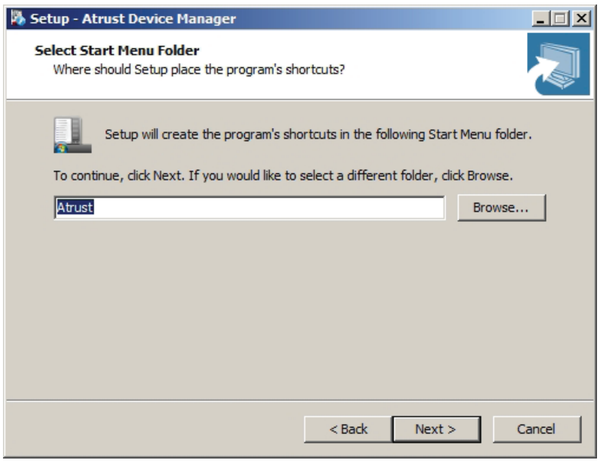
Setup will install Atrust Device Manager into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Atrust

At least 312.8 MB of free disk space is required.

8. 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.



Setup - Atrust Device Manager

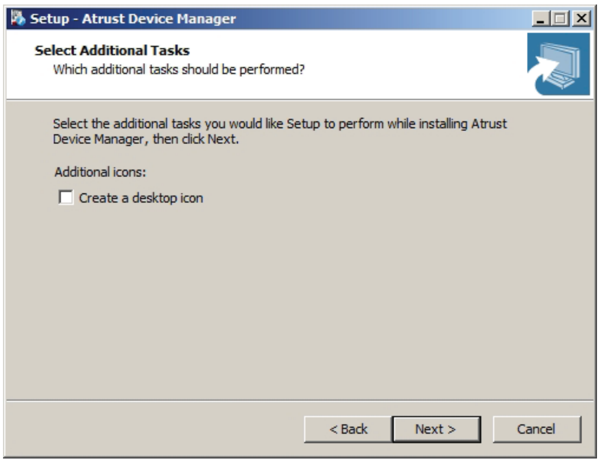
Select Start Menu Folder
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Atrust

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



Setup - Atrust Device Manager

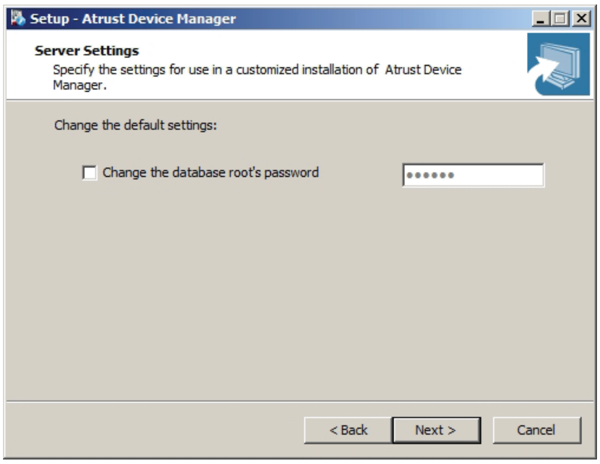
Select Additional Tasks
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Atrust Device Manager, then click Next.

Additional icons:

☐ Create a desktop icon

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



Setup - Atrust Device Manager

Server Settings
Specify the settings for use in a customized installation of Atrust Device Manager.

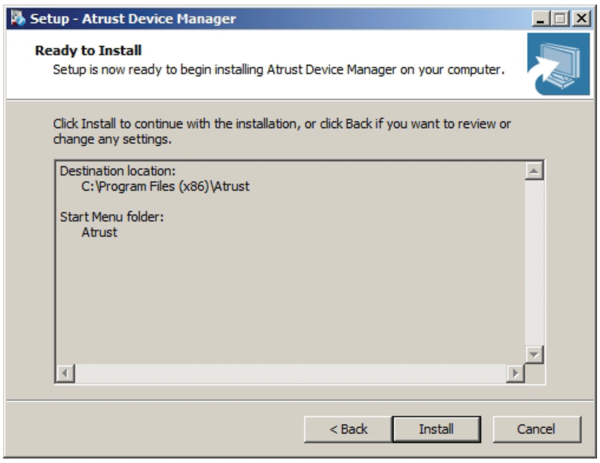
Change the default settings:

☐ Change the database root's password ••••••

NOTE

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

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



Setup - Atrust Device Manager

Ready to Install

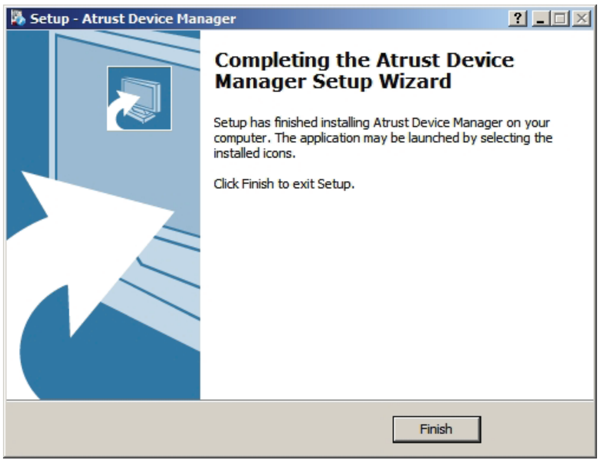
Setup is now ready to begin installing Atrust Device Manager on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files (x86)\Atrust

Start Menu folder:
Atrust

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



Setup - Atrust Device Manager

Completing the Atrust Device Manager Setup Wizard

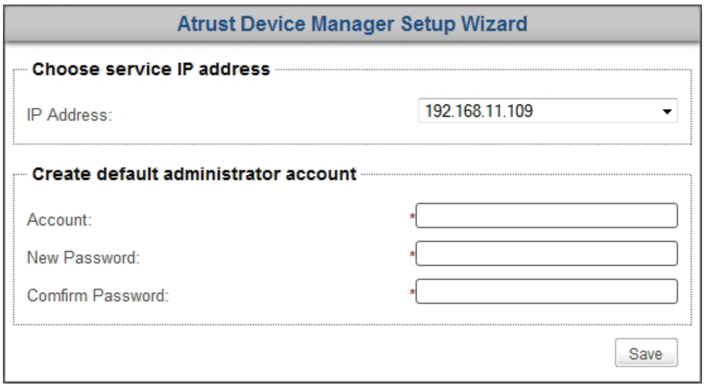
Setup has finished installing Atrust Device Manager on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

2.2 Initial Setup

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

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



Atrust Device Manager Setup Wizard

Choose service IP address

IP Address: 192.168.11.109

Create default administrator account

Account: *

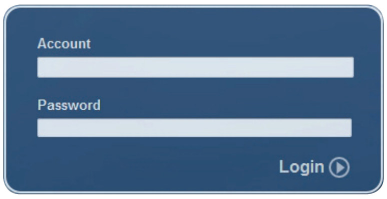
New Password: *

Comfirm Password: *

NOTE

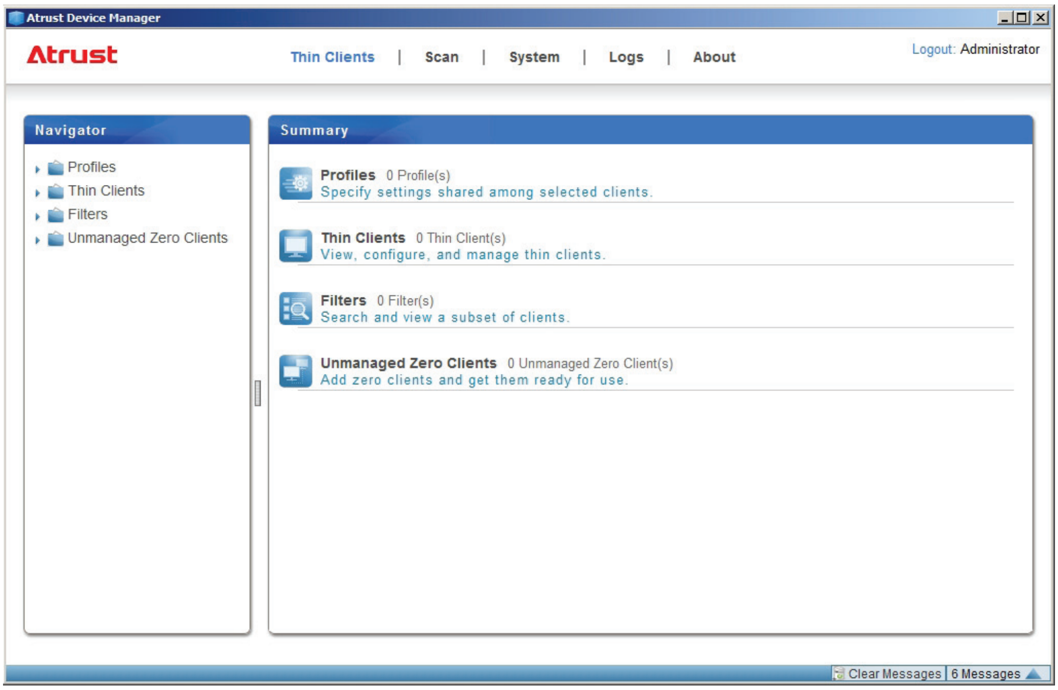
- Your not connected LAN port may appear in the list of available IP addresses with the address value **0.0.0.0**.
- It's strongly recommended to use a fixed IP address as the service IP of Atrust Device Manager. The change of the service IP may make all the managed clients become unmanageable.

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.

Atrust Device Manager



Profiles 0 Profile(s)
Specify settings shared among selected clients.

Thin Clients 0 Thin Client(s)
View, configure, and manage thin clients.

Filters 0 Filter(s)
Search and view a subset of clients.

Unmanaged Zero Clients 0 Unmanaged Zero Client(s)
Add zero clients and get them ready for use.

NOTE

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

2.3 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 9.

NOTE

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

WARNING

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

2.4 Uninstalling Atrust Device Manager

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

NOTE

- To ***upgrade*** your Atrust Device Manager, it's recommended ***not*** to uninstall the current Atrust Device Manager. For more information, please refer to section "2.3 Upgrading Atrust Device Manager" on page 15.
- Ensure that you have backed up important data on Atrust Device Manager before proceeding.

WARNING

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

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

3

Using Atrust Device Manager

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

3.1 Atrust Device Manager

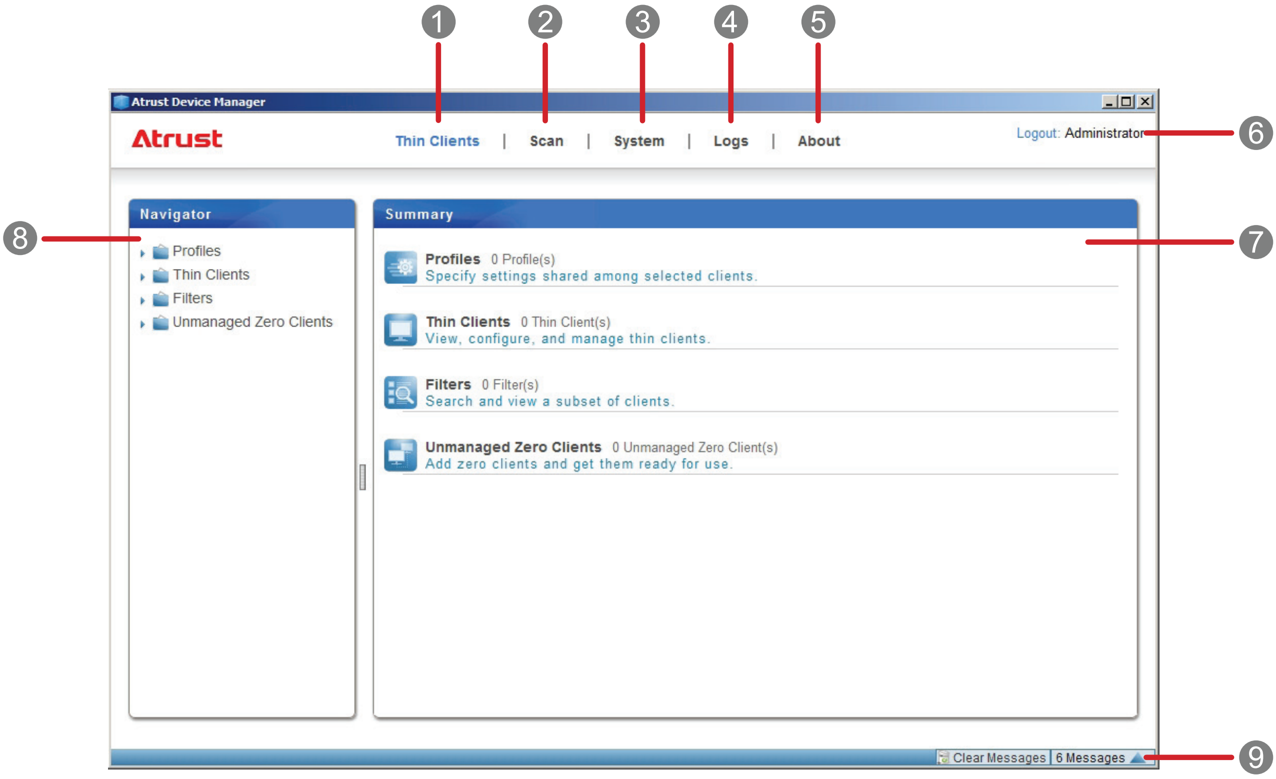
Atrust Device Manager enables you to remotely deploy, manage, update clients, and assist users from a single computer. You can manage clients simply and quickly in groups with a flexible and secure mechanism. Additionally, you can remotely assist users in resolving problems or configuring local settings.

3.1.1 Interface Overview

To access Atrust Device Manager, please do the following:

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

Interface Overview



Profiles 0 Profile(s)
Specify settings shared among selected clients.

Thin Clients 0 Thin Client(s)
View, configure, and manage thin clients.

Filters 0 Filter(s)
Search and view a subset of clients.

Unmanaged Zero Clients 0 Unmanaged Zero Client(s)
Add zero clients and get them ready for use.

Interface Elements

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

3.1.2 Available Tasks at a Glance

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

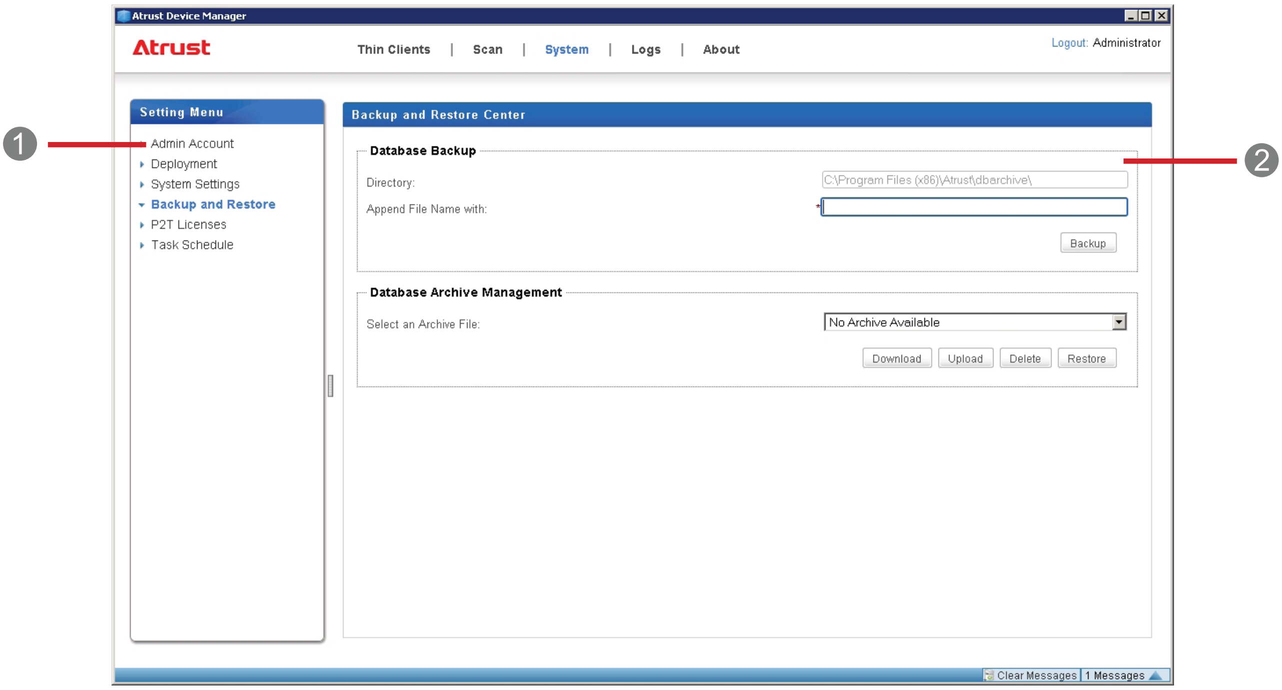
Tab	Function List	Section	Page
System	• Creating accounts for administration • Configuring deployment settings • Managing thin client firmware files • Managing zero client image files • Managing WES package files • Managing client snapshots • Managing certificates of remote computers • Configuring settings for Atrust Device Manager • Backing up the management database • Managing database archive files • Restoring management database • Managing P2T license files • Scheduling automatically performed tasks	3.2 Establishing a Basic Administration Environment	21
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 • Looking for clients including those password-protected	3.3 Adding Clients into a Managed Group	52
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 • Pushing certificates to clients • Sending messages to clients • Rebooting clients remotely • Shutting down clients remotely • Waking clients remotely • Updating client firmware • Installing/Uninstalling software packages • Taking/Restoring client snapshots • Monitoring the use of clients • Controlling clients remotely • Exporting client data • Digging out profiles/clients with Quick Search • Digging out clients with filters	3.4 Managing All Your Clients	60
Logs	• Viewing event logs • Exporting event logs • Emptying event logs	3.5 Viewing and Managing Event Logs	116
About	• Viewing information on Atrust Device Manager • Viewing Atrust contact information • Viewing software license agreement	3.6 Viewing Software Information	120

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



C:\Program Files (x86)\Atrust\dbarchive\

No Archive Available

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

3.2.2 Available Tasks at a Glance

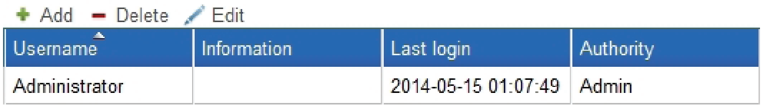
No.	Available Task	Section	Page
1	Creating accounts for administration	3.2.3	23
2	Deleting an account	3.2.3	23
3	Editing an account	3.2.3	23
4	Configuring deployment settings	3.2.4	24
5	Importing thin client firmware files	3.2.5	26
6	Deleting thin client firmware files	3.2.5	26
7	Scanning thin client firmware files	3.2.5	26
8	Importing zero client image files	3.2.6	29
9	Deleting zero client image files	3.2.6	29
10	Importing WES package files	3.2.7	32
11	Deleting WES package files	3.2.7	32
12	Scanning WES package files	3.2.7	32
13	Exporting client snapshots	3.2.8	35
14	Importing client snapshots	3.2.8	35
15	Deleting client snapshots	3.2.8	35
16	Scanning client snapshots	3.2.8	35
17	Importing certificates of remote computers	3.2.9	38
18	Deleting certificates of remote computers	3.2.9	38
19	Selecting the service IP address of Atrust Device Manager	3.2.10	40
20	Configuring auto-logout for Atrust Device Manager	3.2.11	40
21	Enabling or disabling Auto Registration	3.2.12	41
22	Setting password protection for managed thin clients	3.2.13	42
23	Configuring the database source of Atrust Device Manager	3.2.14	43
24	Selecting the interface language of Atrust Device Manager	3.2.15	44
25	Backing up the management database	3.2.16	44
26	Downloading a database archive file	3.2.17	45
27	Uploading a database archive file	3.2.17	45
28	Deleting a database archive file	3.2.17	45
29	Restoring a database archive file	3.2.18	46
30	Importing P2T license files	3.2.19	46
31	Scheduling automatically performed tasks	3.2.20	48

3.2.3 Managing Accounts for Administration

Creating an Account

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

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

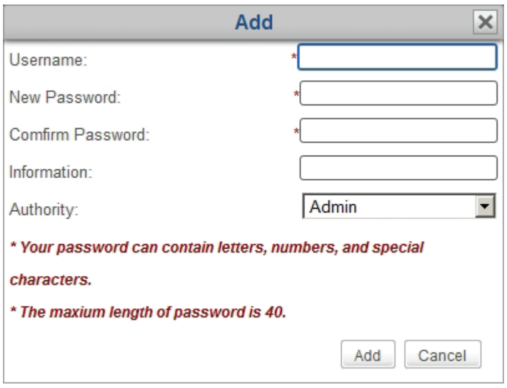


Username	Information	Last login	Authority
Administrator		2014-05-15 01:07:49	Admin

NOTE

- When you log in to Atrust 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.



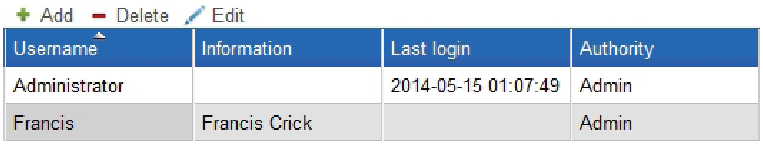
* Your password can contain letters, numbers, and special characters.

* The maxium length of password is 40.

NOTE

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

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



Username	Information	Last login	Authority
Administrator		2014-05-15 01:07:49	Admin
Francis	Francis Crick		Admin

Deleting an Account

To delete an account, please do the following:

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

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

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

Adjusting an Account

To adjust an existing account, please do the following:

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

> **NOTE**
>
> - To add or edit the description in the Information field for the selected account, you need to type the current password.

6. Click **Modify** to apply.

3.2.4 Configuring Deployment Settings

You can deploy, maintain, and upgrade your thin clients from a 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 (external Deploy server) with needed files.

Adding an External Deploy Server

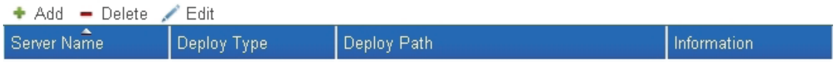
To add an external Deploy server, please do the following:

> **NOTE**
>
> - If no external Deploy server is added, the local host, that is, the computer where the Atrust Device Manager console is installed, will be the default Deploy server.

1. Ensure that the external Deploy server has been set up.

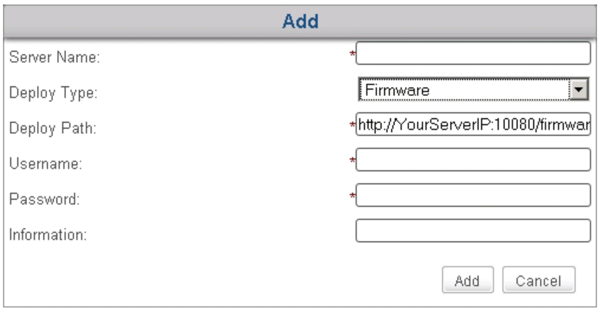
> **NOTE**
>
> - To set up a Deploy server, just install Atrust Device Manager on a computer running one of supported platforms. For information on supported platforms of Atrust Device Manager, please refer to "1.3 Supported Platforms" on page 4.

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



> **NOTE**
>
> - If you never added Deploy servers, the Deploy Server list will be empty as shown above.

4. Click **Add** to open the Add window.
5. Select the Deploy type (firmware, snapshot, or WES package), type the server name, the Deploy URL of the server, **user** as the user name, **secret** as the password, and then click **Add** to confirm. Atrust Device Manager will check the validity *first* before adding that server.

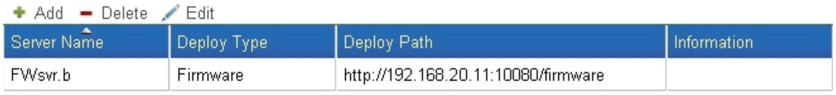


Deploy Type: Firmware

Deploy Path: *http://YourServerIP:10080/firmwar

> **NOTE**
>
> - You can choose a desired name for that server in the Server Name field; the server name here is not necessarily the same as the actual name of the computer.

6. The newly added server will appear in the Deploy Server list.



Server Name	Deploy Type	Deploy Path	Information
FWsvr.b	Firmware	http://192.168.20.11:10080/firmware	

Editing an External Deploy Server

To edit an external Deploy server, please do the following:

1. On **System** tab, click **Deployment** > **Deploy Server**.
2. The Deploy Server list appears in Management area.
3. Click to select the desired server.
4. Click **Edit** on the top of the list.
5. Adjust fields or menu in the appeared window, and then click **Modify** to apply.

Deleting an External Deploy Server

To delete an external Deploy server, please do the following:

1. On **System** tab, click **Deployment** > **Deploy Server**.
2. The Deploy Server list appears in Management area.
3. Click to select the desired server.

> **NOTE**
>
> - To delete more than one server, Ctrl-click to select multiple servers.

4. Click **Delete** on the top of the list.
5. A message appears prompting for confirmation.
6. Click **OK** to confirm.
7. The selected server is removed from the list.

3.2.5 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 into Atrust Device Manager.

> **NOTE**
>
> - For instructions on how to update firmware for clients remotely, please see section “3.4.24 Updating Client Firmware” on page 102.
> - 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 “3.2.6 Managing Zero Client Image Files” on page 29.

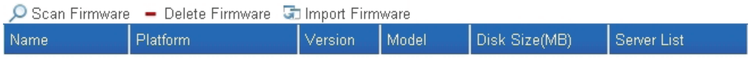
Importing Thin Client Firmware Files

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.

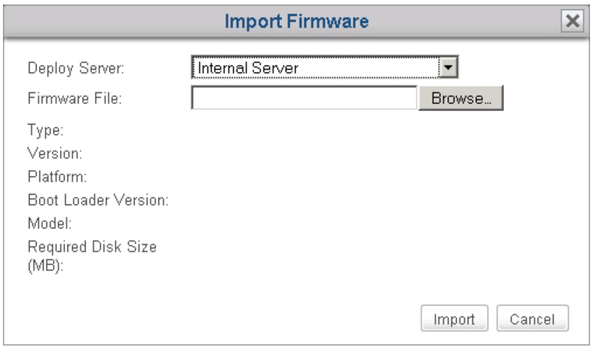


Name	Platform	Version	Model	Disk Size(MB)	Server List

NOTE

- If you never added external Deploy servers or imported firmware files into Atrust Device Manager, the Firmware list will be empty as shown above.
- All firmware files located on external Deploy servers will also be shown on the Firmware list if you added Deploy servers to the Atrust Device Manager console. For information on Deploy servers, please refer to "3.2.4 Configuring Deployment Settings" on page 24.

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



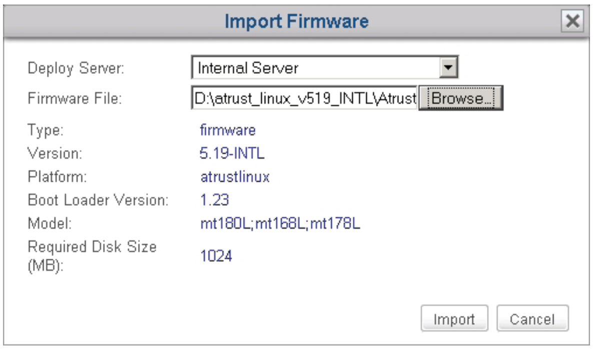
Deploy Server: Internal Server
Firmware File:
Type:
Version:
Platform:
Boot Loader Version:
Model:
Required Disk Size (MB):

5. Select where to import the firmware file: the local host (internal server) or an external Deploy server, 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 on the same computer.

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



Deploy Server: Internal Server

Firmware File: D:\atrust_linux_v519_INTL\Atrust

Type: firmware

Version: 5.19-INTL

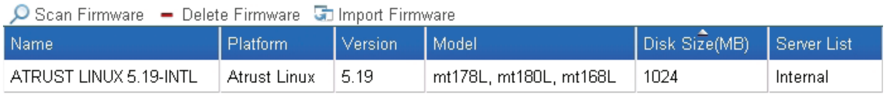
Platform: atrustlinux

Boot Loader Version: 1.23

Model: mt180L;mt168L;mt178L

Required Disk Size (MB): 1024

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

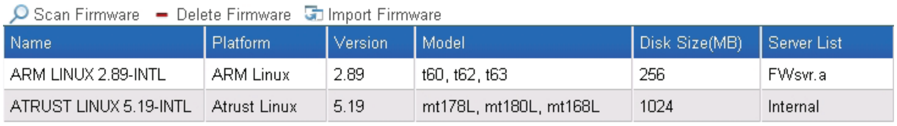


Name	Platform	Version	Model	Disk Size(MB)	Server List
ATRUST LINUX 5.19-INTL	Atrust Linux	5.19	mt178L, mt180L, mt168L	1024	Internal

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.



Name	Platform	Version	Model	Disk Size(MB)	Server List
ARM LINUX 2.89-INTL	ARM Linux	2.89	t60, t62, t63	256	FWsvr.a
ATRUST LINUX 5.19-INTL	Atrust Linux	5.19	mt178L, mt180L, mt168L	1024	Internal

NOTE

- All firmware files located on external Deploy servers will also be shown on the Firmware list if you added Deploy servers to the Atrust Device Manager console. For information on Deploy servers, please refer to "3.2.4 Configuring Deployment Settings" on page 24.

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 might need the help of this feature. The first scenario is when you import firmware files directly on external Deploy server side. In this scenario, the local list of available firmware in Atrust Device Manager may be not in sync with the remote list of firmware on another computer which you added as a Deploy server. The **Scan Firmware** feature can synchronize your local list with the remote one.

NOTE

- For information on Deploy servers, please refer to section "3.2.4 Configuring Deployment Settings" on page 24.

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

NOTE

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

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

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

3.2.6 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 console. 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 "3.4.24 Updating Client Firmware" on page 102.

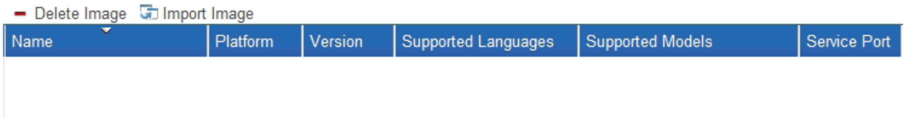
Importing Zero Client Image Files

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.

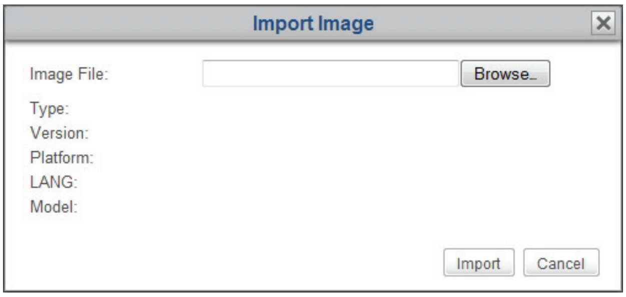


Name	Platform	Version	Supported Languages	Supported Models	Service Port

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.

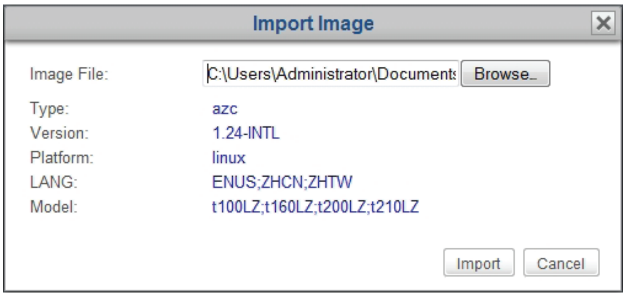


Image File: C:\Users\Administrator\Document:

Type: azc

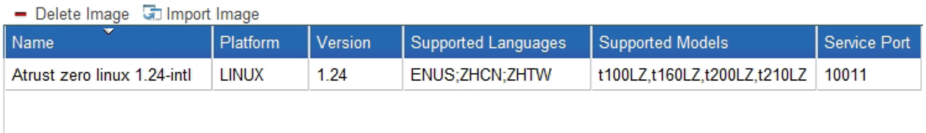
Version: 1.24-INTL

Platform: linux

LANG: ENUS;ZHCN;ZHTW

Model: t100LZ;t160LZ;t200LZ;t210LZ

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



Name	Platform	Version	Supported Languages	Supported Models	Service Port
Atrust zero linux 1.24-intl	LINUX	1.24	ENUS;ZHCN;ZHTW	t100LZ,t160LZ,t200LZ,t210LZ	10011

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.

3.2.7 Managing WES Package Files

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

NOTE

- The Windows Embedded Standard version of your client may not support multiple user interface packs. In this case, installing a language pack for a client will replace its display (user interface) language with the new one.
- For instructions on how to update your WES clients with package files remotely, please refer to "3.4.25 Installing and Uninstalling Software Packages" on page 105.

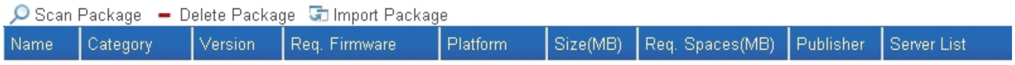
Importing WES Package Files

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.

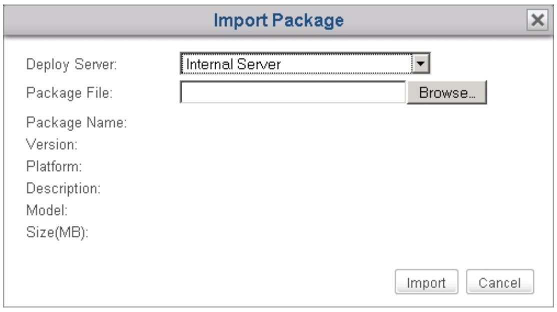
1. On **System** tab, click **Deployment** > **WES Package**.
2. The Package list appears.



NOTE

- If you never add external Deploy servers or imported WES package files into Atrust Device Manager, the Package list will be empty as shown above.
- All WES package files located on external Deploy servers will also be shown on the Package list if you added Deploy servers to the Atrust Device Manager console. For information on Deploy servers, please refer to "3.2.4 Configuring Deployment Settings" on page 24.

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

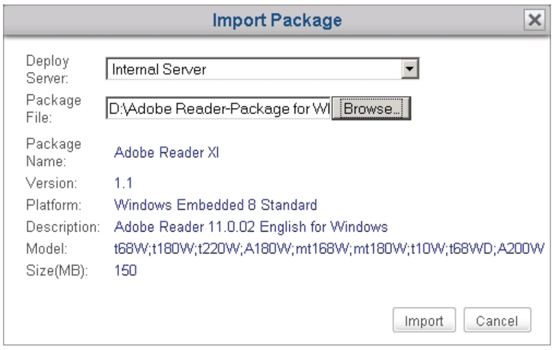


Deploy Server: Internal Server
Package File:
Package Name:
Version:
Platform:
Description:
Model:
Size(MB):

5. Select where to import the package file: the local host (internal server) or an external Deploy server, click **Browse** to locate the desired package file, and then click **Open** to confirm.

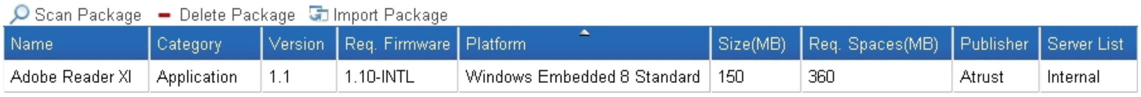
> **NOTE**
>
> - Atrust Device Manager will automatically perform file check to ensure it's a valid package file for Windows Embedded-based clients and there is no duplicate on the same computer.

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



Deploy Server: Internal Server
Package File: D:\Adobe Reader-Package for WI
Package Name: Adobe Reader XI
Version: 1.1
Platform: Windows Embedded 8 Standard
Description: Adobe Reader 11.0.02 English for Windows
Model: t68W;t180W;t220W;A180W;mt168W;mt180W;t10W;t68WD;A200W
Size(MB): 150

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

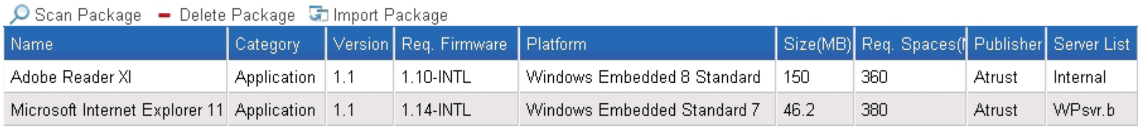


Name	Category	Version	Req. Firmware	Platform	Size(MB)	Req. Spaces(MB)	Publisher	Server List
Adobe Reader XI	Application	1.1	1.10-INTL	Windows Embedded 8 Standard	150	360	Atrust	Internal

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.



Name	Category	Version	Req. Firmware	Platform	Size(MB)	Req. Spaces(I	Publisher	Server List
Adobe Reader XI	Application	1.1	1.10-INTL	Windows Embedded 8 Standard	150	360	Atrust	Internal
Microsoft Internet Explorer 11	Application	1.1	1.14-INTL	Windows Embedded Standard 7	46.2	380	Atrust	WPsvr.b

NOTE

- All WES package files located on external Deploy servers will also be shown on the Package list if you added Deploy servers to the Atrust Device Manager console. For information on Deploy servers, please refer to "3.2.4 Configuring Deployment Settings" on page 24.

3. Click to select the desired package file, and then click **Delete Package**.

NOTE

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

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 might need the help of this feature. The first scenario is when you import package files directly on external Deploy server side. 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 which you added as a Deploy server. 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 package files on another computer for client management, please refer to section "3.2.4 Configuring Deployment Settings" on page 24.

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

NOTE

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

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

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

3.2.8 Managing Client Snapshots

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

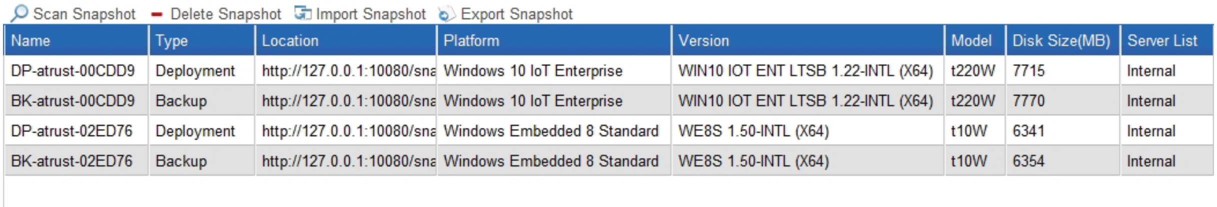
NOTE

- Atrust t-series zero clients download their operating system while connecting to the local network. Therefore, there is no need to take any local system copy. Atrust t-series zero clients include t100LZ, t160LZ, t200LZ, t210LZ etc.
- Only Windows Embedded-based thin clients support this feature.
- For instructions on how to take a system snapshot for clients, please refer to section "3.4.26 Taking Client Snapshots" on page 107.

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.

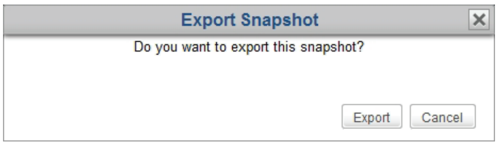


Name	Type	Location	Platform	Version	Model	Disk Size(MB)	Server List
DP-atrust-00CDD9	Deployment	http://127.0.0.1:10080/sna	Windows 10 IoT Enterprise	WIN10 IOT ENT LTSB 1.22-INTL (X64)	t220W	7715	Internal
BK-atrust-00CDD9	Backup	http://127.0.0.1:10080/sna	Windows 10 IoT Enterprise	WIN10 IOT ENT LTSB 1.22-INTL (X64)	t220W	7770	Internal
DP-atrust-02ED76	Deployment	http://127.0.0.1:10080/sna	Windows Embedded 8 Standard	WE8S 1.50-INTL (X64)	t10W	6341	Internal
BK-atrust-02ED76	Backup	http://127.0.0.1:10080/sna	Windows Embedded 8 Standard	WE8S 1.50-INTL (X64)	t10W	6354	Internal

NOTE

- The Snapshot list might be empty, if you never added external Deploy servers, 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.


Export Snapshot

Do you want to export this snapshot?

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. Select where to import the snapshot file: the local host (internal server) or an external Deploy server, 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 on the same computer.

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.

> **NOTE**
>
> - All snapshots located on external Deploy servers will also be shown on the Snapshot list if you added Deploy servers to the Atrust Device Manager console. For information on Deploy servers, please refer to “3.2.4 Configuring Deployment Settings” on page 24.

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 might need the help of this feature. The first scenario is when you import snapshots directly on external Deploy servers. 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 which you added as a Deploy server. 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 snapshots on another computer for client management, please refer to section "3.2.4 Configuring Deployment Settings" on page 24.

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

NOTE

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

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

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

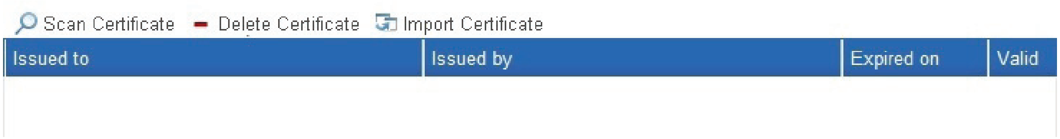
3.2.9 Managing Certificates of Remote Computers

Thin clients are simple endpoint devices for accessing services from remote computers. To ensure connection security between thin clients and remote computers, certificates of remote computers where desktop virtualization services are delivered may be required in order to verify the identify of remote computers. You could import security certificates of remote computers, and then push certificates remotely to multiple thin clients with the help of Atrust Device Manager.

Importing Certificates of Remote Computers

To import the certificate of a remote computer, please do the following:

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

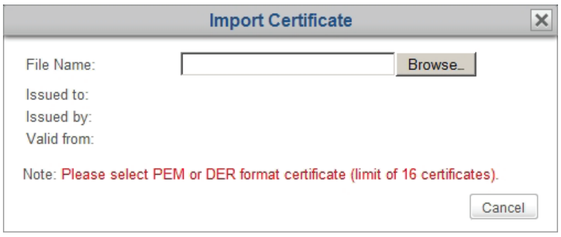


Issued to	Issued by	Expired on	Valid

NOTE

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

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



File Name:
Issued to:
Issued by:
Valid from:

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

NOTE

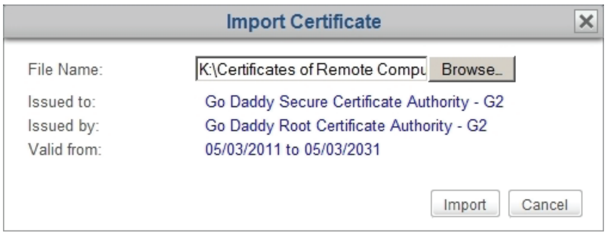
- Atrust Device Manager supports both **PEM** (Privacy Enhanced Mail) and **DER** (Distinguished Encoding Rules) format certificates.
- The upper limit of imported certificates is 16.

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

NOTE

- Atrust Device Manager will automatically perform file check to ensure there is no duplicate in the Certificate list.

6. Click **Import** to continue.



Import Certificate

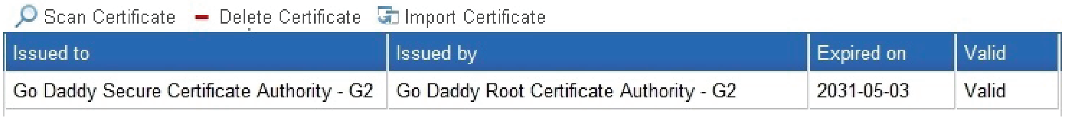
File Name: K:\Certificates of Remote Compu

Issued to: Go Daddy Secure Certificate Authority - G2

Issued by: Go Daddy Root Certificate Authority - G2

Valid from: 05/03/2011 to 05/03/2031

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



Issued to	Issued by	Expired on	Valid
Go Daddy Secure Certificate Authority - G2	Go Daddy Root Certificate Authority - G2	2031-05-03	Valid

NOTE

- While pushing certificates to thin clients, all certificates in the Certificate list will be imported to selected clients. For instructions on how to push certificates to clients, please refer to section "3.4.18 Pushing Certificates of Remote Computers to Clients" on page 89.

Deleting Certificates of Remote Computers

To delete the certificate of a remote computer, please do the following:

1. On **System** tab, click **Deployment** > **Certificate**.
2. The Certificate list appears in Management area.
3. Click to select the desired certificate.

NOTE

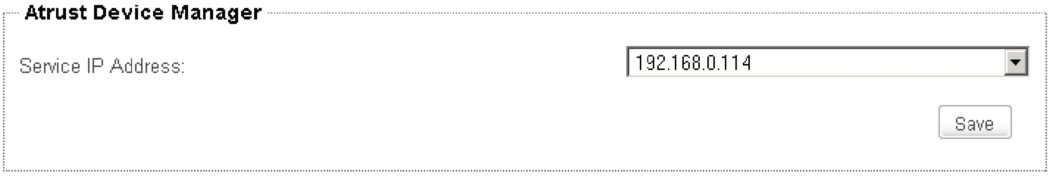
- To delete more than one certificate, Ctrl-click to select multiple entries.

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

3.2.10 Selecting the Service IP of Atrust Device Manager

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

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



Atrust Device Manager

Service IP Address: 192.168.0.114

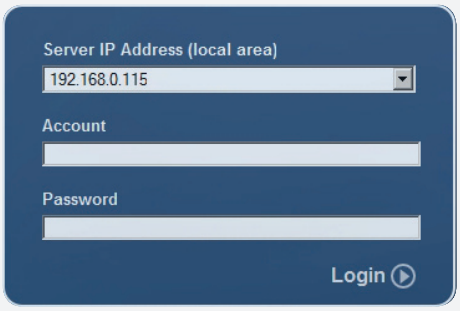
3. Click **Save** to apply.

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.

NOTE

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



Server IP Address (local area): 192.168.0.115

Account

Password

3.2.11 Configuring Auto-Logout for Atrust Device Manager

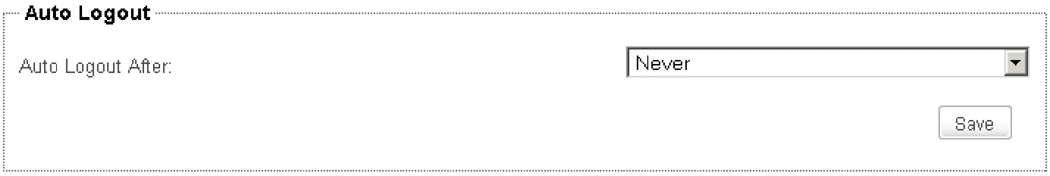
Atrust Device Manager allows you to configure its auto-logout to enhance the security of the management console. When configured, your session will be ended automatically when it's idle for a specific amount of time.

NOTE

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

To configure auto-logout for Atrust Device Manager, please do the following:

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



Auto Logout After: Never

3. Click **Save** to apply.

3.2.12 Enabling or Disabling Auto Registration

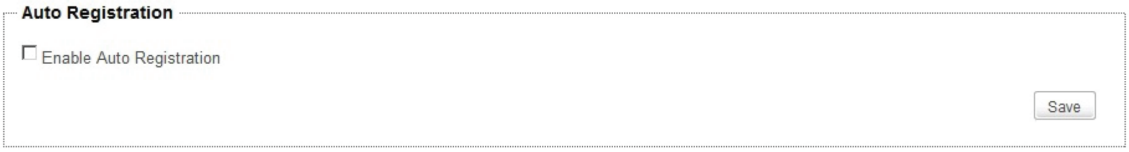
Auto Registration allows that thin clients automatically register with Atrust Device Manager when they are online and then become managed by Atrust Device Manager.

NOTE

- Please refer to appendix "A.3 Configuring Your DHCP or DNS Server for Auto Registration" on page 146 for more information.

To enable or disable Auto Registration, please do the following:

1. On Atrust Device Manager, click **System** > **System Settings** > **General Settings**.



□ Enable Auto Registration

2. In Auto Registration section, check or uncheck **Enable Auto Registration** to enable or disable Auto Registration.

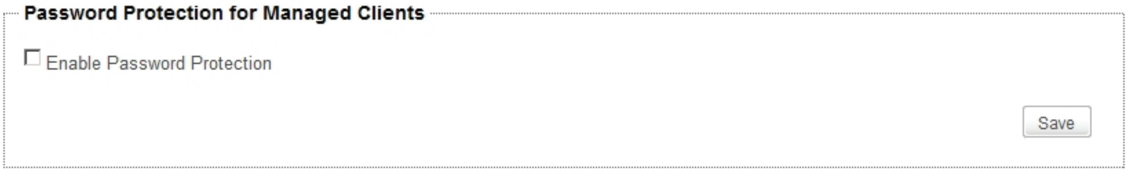
NOTE

- By default, Auto Registration is disabled.

3.2.13 Setting Password Protection for Managed Thin Clients

To set password protection for managed thin clients, please do the following:

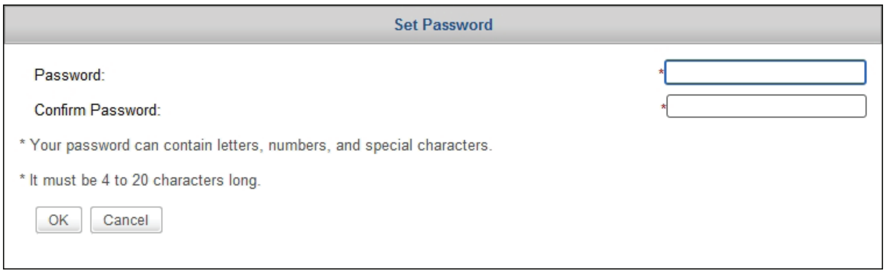
1. On Atrust Device Manager, click **System** > **System Settings** > **General Settings**.



Password Protection for Managed Clients

□ Enable Password Protection

2. In Password Protection for Managed Client section, click to check **Enable Password Protection**.
3. A window appears prompting for the password.



Set Password

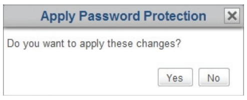
Password: *

Confirm Password: *

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

* It must be 4 to 20 characters long.

4. Type the desired password, and then click **OK** to confirm.
5. Click **Save** in that section to store the password.
6. If there is any existing managed thin client, a window appears prompting to apply the password. Click **Yes** to push the password to all managed clients.



Apply Password Protection

Do you want to apply these changes?

NOTE

- For newly added thin clients, that password will be automatically applied.

NOTE

- Please note thin clients may need new firmware to support password protection.

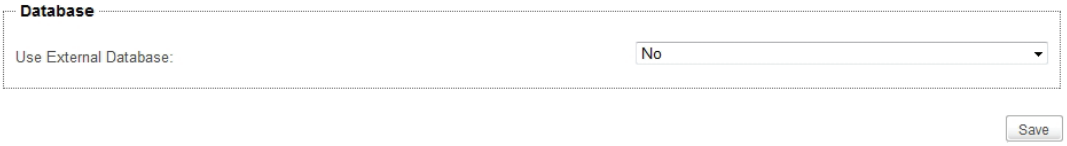
3.2.14 Configuring the Database Source of Atrust Device Manager

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

Using Local Management Database

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

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



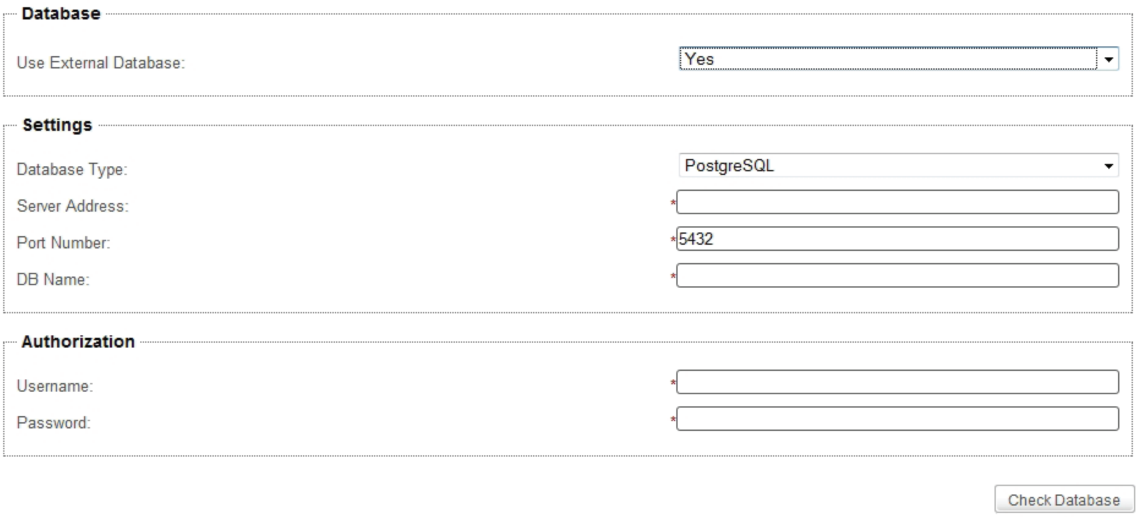
Database

Use External Database: 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.



Database

Use External Database: Yes

Settings

Database Type: PostgreSQL

Server Address: *

Port Number: * 5432

DB Name: *

Authorization

Username: *

Password: *

NOTE

- Four database management systems are supported: PostgreSQL, MySQL, MsSQL (Microsoft SQL Server), and Oracle (Oracle Database).
- Ensure that you have set up the desired database management system.

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

3.2.15 Selecting the Interface Language of Atrust Device Manager

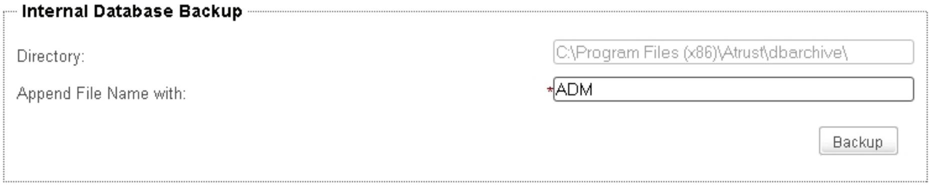
To select the interface language of your Atrust Device Manager, please do the following:

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.

3.2.16 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.



Internal Database Backup

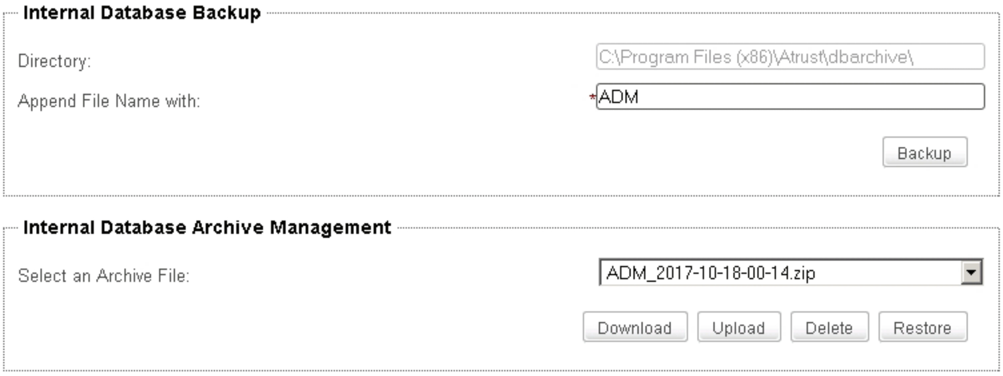
Directory: C:\Program Files (x86)\Atrust\dbarchive\

Append File Name with: *ADM

TIP

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

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



Internal Database Backup

Directory: C:\Program Files (x86)\Atrust\dbarchive\

Append File Name with: *ADM

Internal Database Archive Management

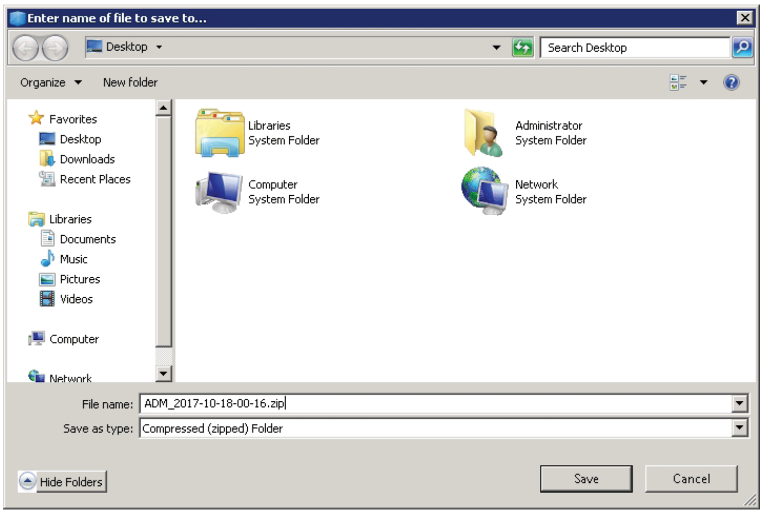
Select an Archive File: ADM_2017-10-18-00-14.zip

3.2.17 Managing Database Archive Files

Downloading a Database Archive File

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

1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click the Archive File drop-down menu to select the desired database archive file, and then click **Download**.
3. In the opened window, navigate to the desired location, and then click **Save** to store the file.



Enter name of file to save to...

File name: ADM_2017-10-18-00-16.zip

Save as type: Compressed (zipped) Folder

Uploading a Database Archive File

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

1. On **System** tab, click **Backup and Restore**.
2. In Database Archive Management section, click **Upload** to open the File Upload window.
3. Locate the desired database archive file, and then click **OK** to confirm.
4. The file is added to the Archive File drop-down menu.

Deleting a Database Archive File

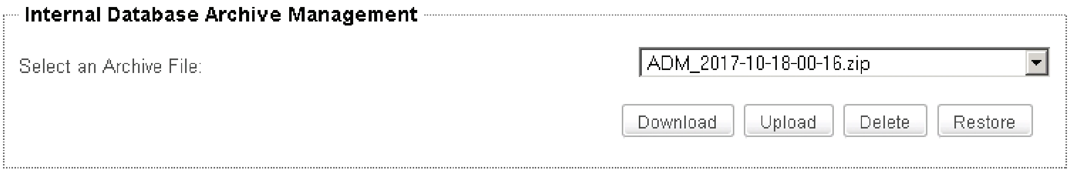
To delete a database archive file, please do the following:

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

3.2.18 Restoring a Database Archive File

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

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



Internal Database Archive Management

Select an Archive File: ADM_2017-10-18-00-16.zip

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

3.2.19 Managing P2T License Files

Atrust P2T Converter is also one of tools 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 tool 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 User's Manual 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 license and activate your P2T thin clients through Atrust Device Manager, first you need to import P2T license file(s) into it, preparing licenses for your P2T thin clients.

Importing P2T Lincense Files

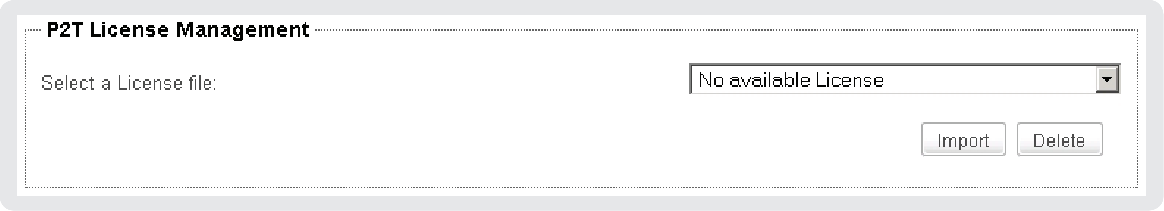
To import P2T license file(s) into Atrust Device Manager, please follow the steps below:

NOTE

- If you don't have any P2T license files, please contact us for information on how to get P2T licenses. You may need to provide Atrust Device Manager's UUID, which could be found at **Systems** > **P2T Licenses** > **UUID information**.

1. On **System** tab, click **P2T Licenses**.

2. Under the P2T License Management section, click **Import**.



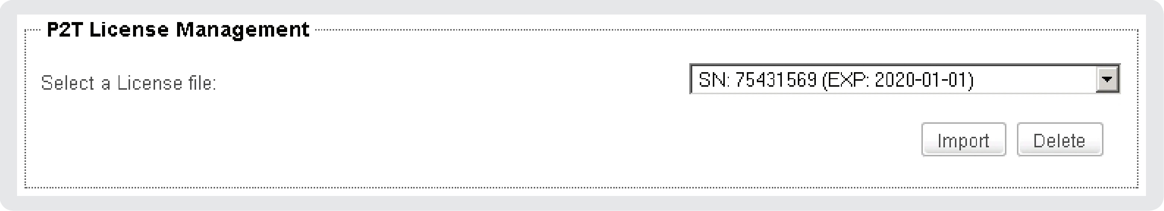
P2T License Management

Select a License file: No available License

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 **.lic**.

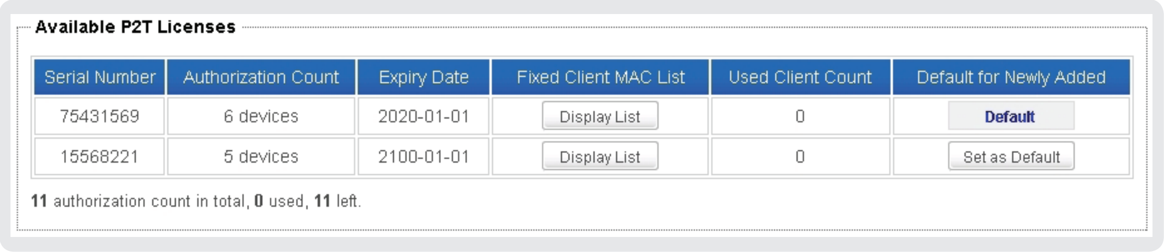
4. The license file is imported and available number of P2T licenses is shown under the Available P2T Licenses section.



P2T License Management

Select a License file: SN: 75431569 (EXP: 2020-01-01)

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



Available P2T Licenses

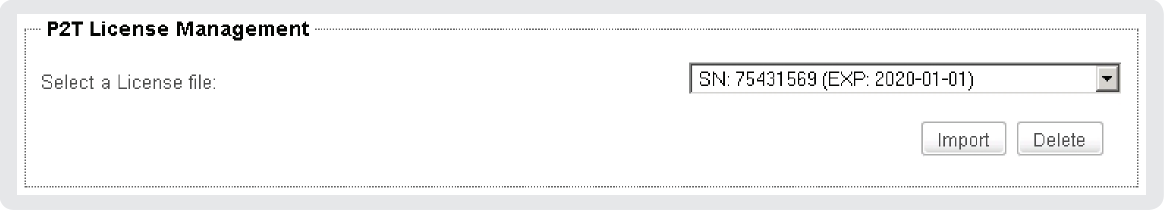
Serial Number	Authorization Count	Expiry Date	Fixed Client MAC List	Used Client Count	Default for Newly Added
75431569	6 devices	2020-01-01	Display List	0	**Default**
15568221	5 devices	2100-01-01	Display List	0	Set as Default

11 authorization count in total, **0** used, **11** left.

Deleting P2T Lincense Files

To delete P2T license file(s) from Atrust Device Manager, please follow the steps below:

1. On **System** tab, click **P2T Licenses**.
2. Under the P2T License Management section, click the drop-menu to select the desired P2T license file, and then click **Delete** to remove the file.



P2T License Management

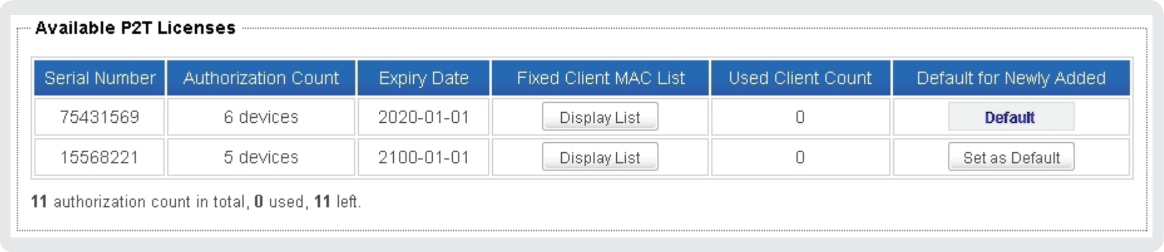
Select a License file: SN: 75431569 (EXP: 2020-01-01)

Setting the Default License Set

If more than one set of licenses is available, you will need to decide which one should be used currently (active license set) for newly added P2T thin clients.

To change the active license set, please do the following:

1. Under the Available P2T Licenses section, click **Set as Default** for the desired license set.

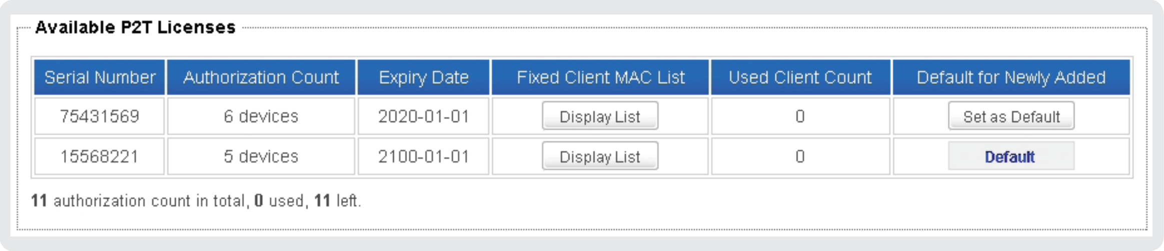


Available P2T Licenses

Serial Number	Authorization Count	Expiry Date	Fixed Client MAC List	Used Client Count	Default for Newly Added
75431569	6 devices	2020-01-01	Display List	0	**Default**
15568221	5 devices	2100-01-01	Display List	0	Set as Default

11 authorization count in total, **0** used, **11** left.

2. That license set will be changed to **Default**.



Available P2T Licenses

Serial Number	Authorization Count	Expiry Date	Fixed Client MAC List	Used Client Count	Default for Newly Added
75431569	6 devices	2020-01-01	Display List	0	Set as Default
15568221	5 devices	2100-01-01	Display List	0	**Default**

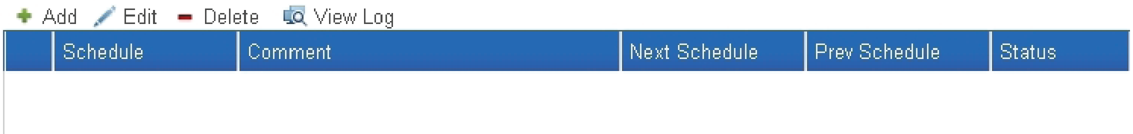
11 authorization count in total, **0** used, **11** left.

3.2.20 Scheduling Automatically Performed Tasks

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

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

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

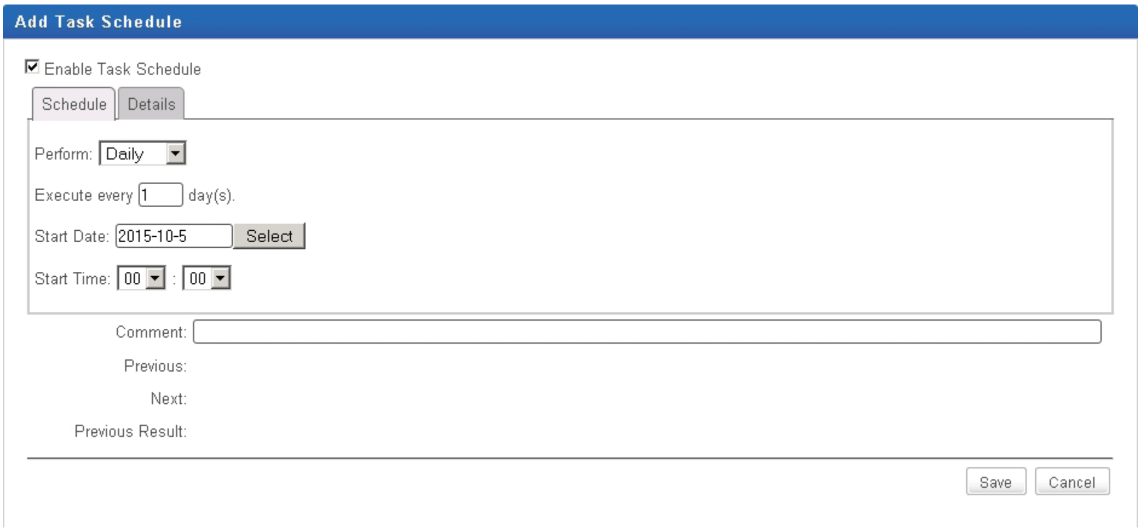


	Schedule	Comment	Next Schedule	Prev Schedule	Status

NOTE

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

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



Add Task Schedule

☑ Enable Task Schedule

Perform: Daily

Execute every 1 day(s).

Start Date: 2015-10-5

Start Time: 00 : 00

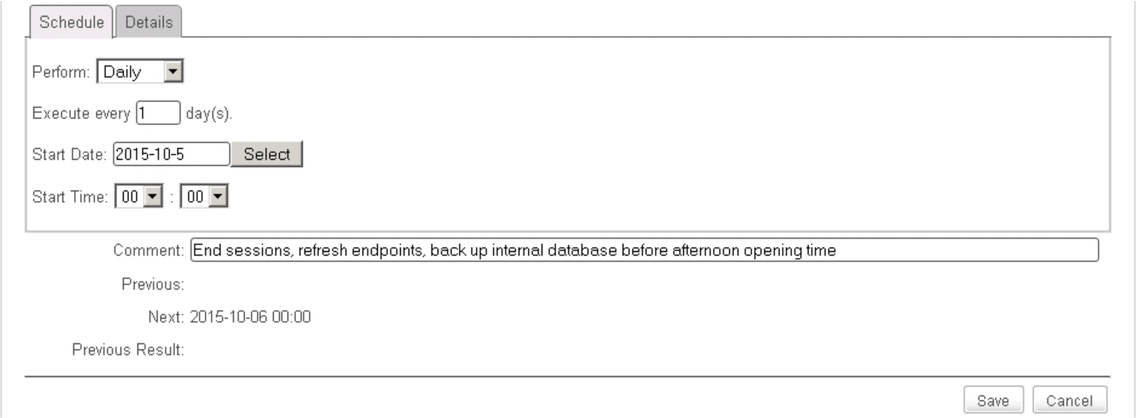
Comment:

Previous:

Next:

Previous Result:

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



Perform: Daily

Execute every 1 day(s).

Start Date: 2015-10-5

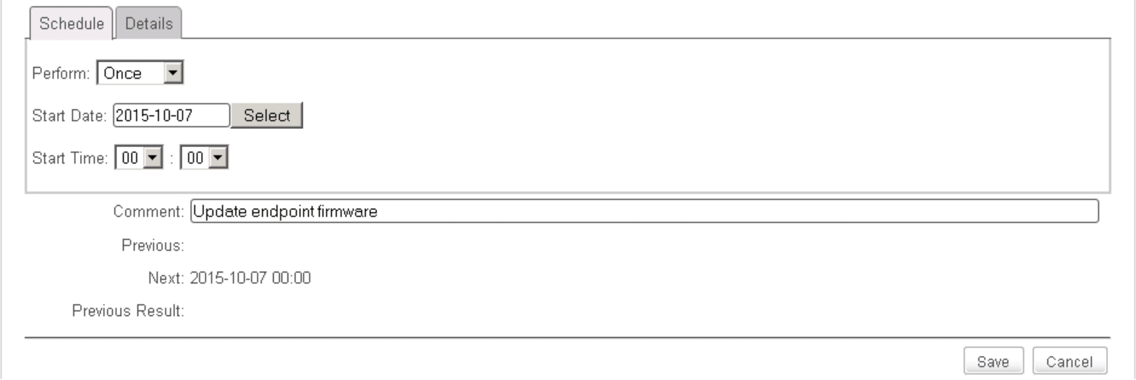
Start Time: 00 : 00

Comment: End sessions, refresh endpoints, back up internal database before afternoon opening time

Previous:

Next: 2015-10-06 00:00

Previous Result:



Perform: Once

Start Date: 2015-10-07

Start Time: 00 : 00

Comment: Update endpoint firmware

Previous:

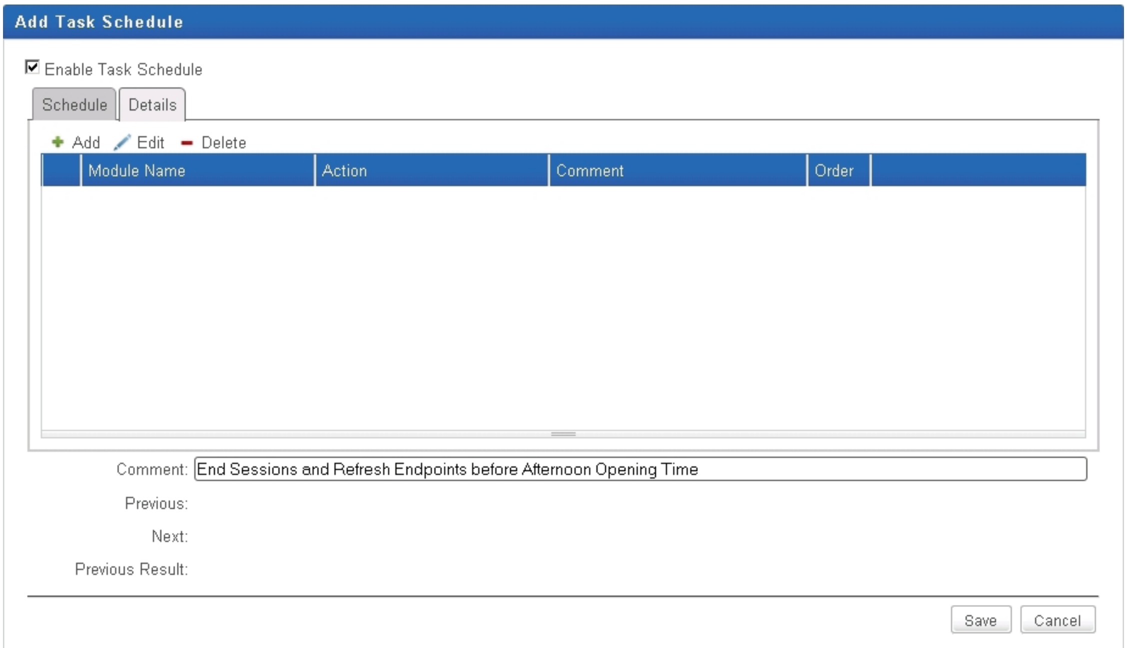
Next: 2015-10-07 00:00

Previous Result:

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

NOTE

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



Add Task Schedule

☑ Enable Task Schedule

Schedule | Details

+ Add / Edit – Delete

	Module Name	Action	Comment	Order

Comment: End Sessions and Refresh Endpoints before Afternoon Opening Time

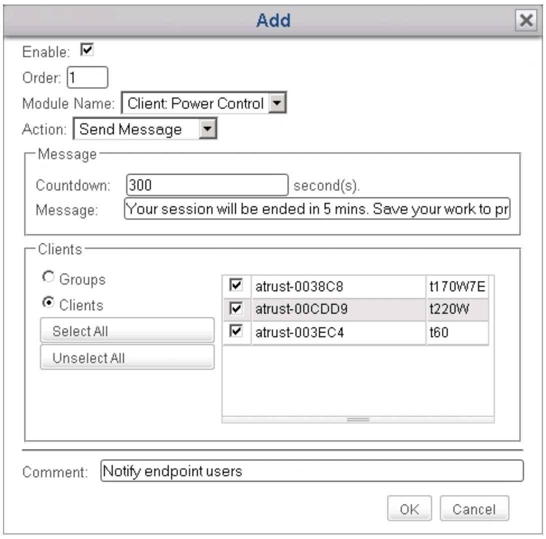
Previous:

Next:

Previous Result:

Save Cancel

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



Add

Enable: ☑

Order: 1

Module Name: Client: Power Control

Action: Send Message

Message

Countdown: 300 second(s).

Message: Your session will be ended in 5 mins. Save your work to pr

Clients

○ Groups

● Clients

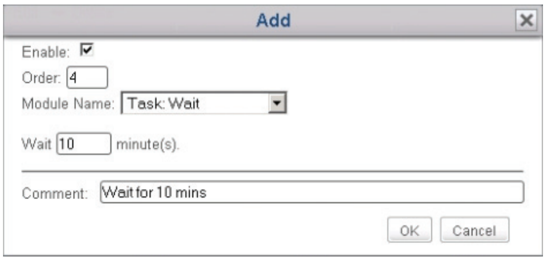
Select All

Unselect All

☑	atrust-0038C8	t170W7E
☑	atrust-00CDD9	t220W
☑	atrust-003EC4	t60

Comment: Notify endpoint users

OK Cancel



Add

Enable: ☑

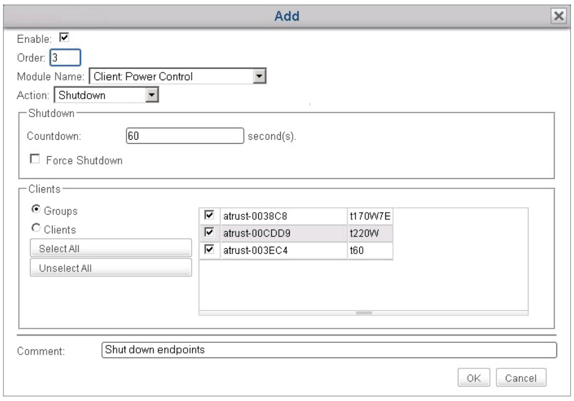
Order: 4

Module Name: Task: Wait

Wait 10 minute(s).

Comment: Wait for 10 mins

OK Cancel



Add

Enable: ☑

Order: 3

Module Name: Client: Power Control

Action: Shutdown

Shutdown

Countdown: 60 second(s).

□ Force Shutdown

Clients

● Groups

○ Clients

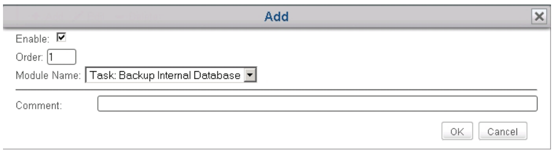
Select All

Unselect All

☑	atrust-0038C8	t170W7E
☑	atrust-00CDD9	t220W
☑	atrust-003EC4	t60

Comment: Shut down endpoints

OK Cancel



Add

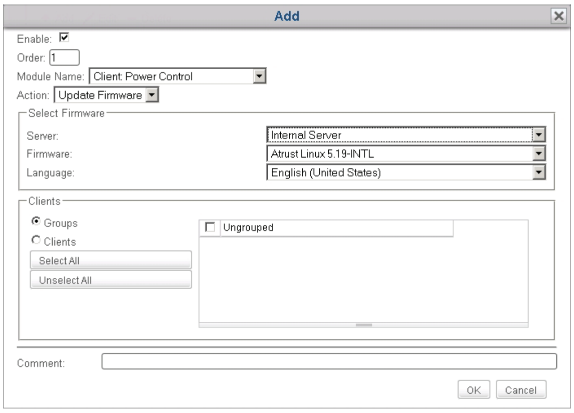
Enable: ☑

Order: 1

Module Name: Task: Backup Internal Database

Comment:

OK Cancel



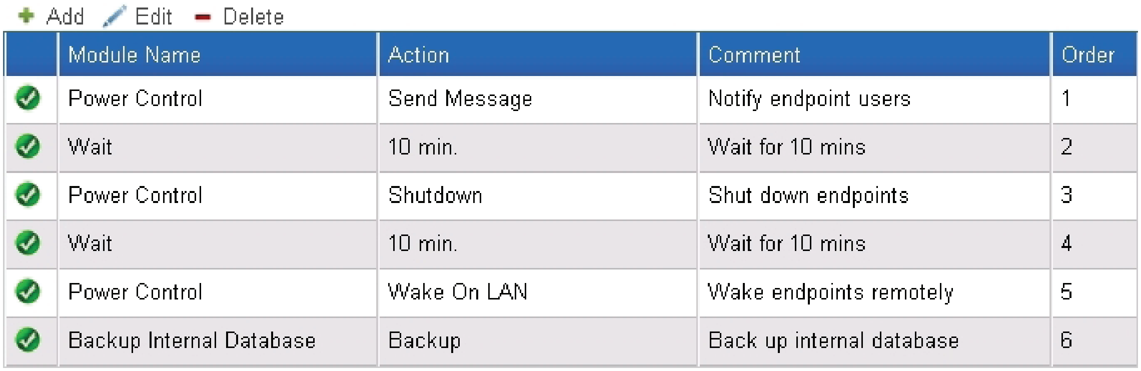
Enable: ☑
Order: 1
Module Name: Client: Power Control
Action: Update Firmware

Select Firmware
Server: Internal Server
Firmware: Atrust Linux 5.19-INTL
Language: English (United States)

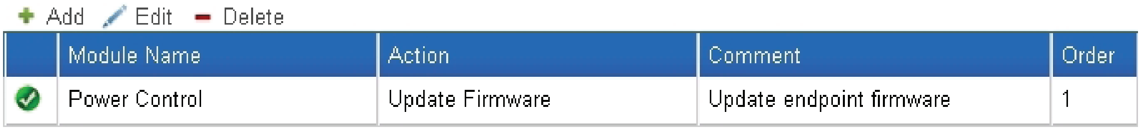
Clients
● Groups
○ Clients
Select All
Unselect All
□ Ungrouped

Comment:

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

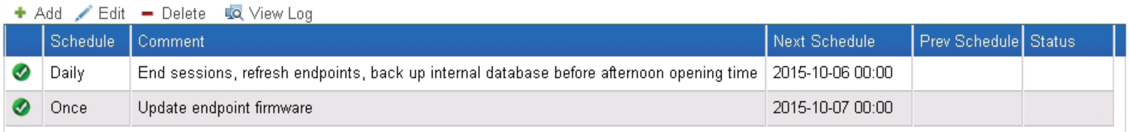


	Module Name	Action	Comment	Order
✓	Power Control	Send Message	Notify endpoint users	1
✓	Wait	10 min.	Wait for 10 mins	2
✓	Power Control	Shutdown	Shut down endpoints	3
✓	Wait	10 min.	Wait for 10 mins	4
✓	Power Control	Wake On LAN	Wake endpoints remotely	5
✓	Backup Internal Database	Backup	Back up internal database	6



	Module Name	Action	Comment	Order
✓	Power Control	Update Firmware	Update endpoint firmware	1

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



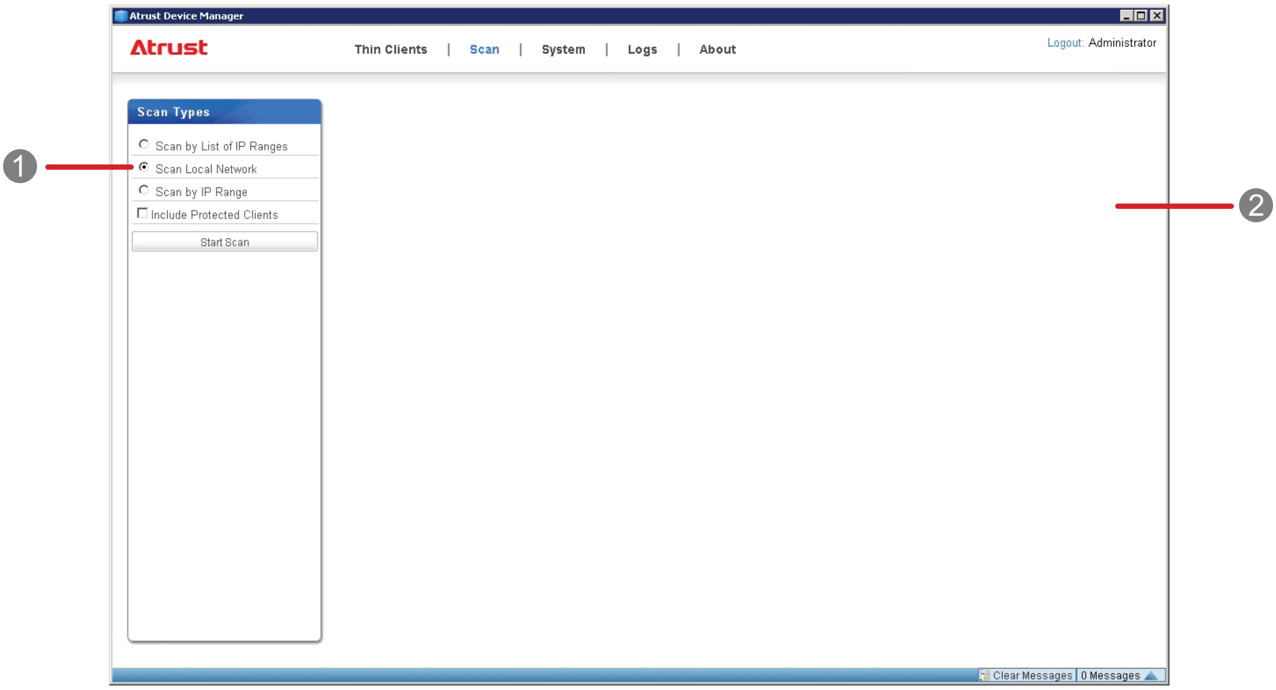
	Schedule	Comment	Next Schedule	Prev Schedule	Status
✓	Daily	End sessions, refresh endpoints, back up internal database before afternoon opening time	2015-10-06 00:00		
✓	Once	Update endpoint firmware	2015-10-07 00:00		

3.3 Adding Clients into a Managed Group

3.3.1 Scan Tab Overview

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

Scan Tab Overview


Atrust Device Manager
Atrust
Thin Clients | Scan | System | Logs | About
Logout: Administrator
Scan Types
○ Scan by List of IP Ranges
● Scan Local Network
○ Scan by IP Range
□ Include Protected Clients
Start Scan
Clear Messages | 0 Messages
1
2

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	54
2	Discovering clients in a specified range of IP addresses	3.3.5	55
3	Discovering clients using predefined IP range lists	3.3.6 3.3.7	56 57

3.3.3 Client Detection and Management

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

To look for a thin client over your local network, you can use different client detection options available under the **Scan** tab. 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 zero clients that are not managed by the current Atrust Device Manager instance, 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 console. 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	Almost all thin client models	• Clients are connected to the local network • Clients are powered up	Manual Scan	3.3.4 3.3.5 3.3.6	54 55 56
Zero Client	t100LZ t160LZ t200LZ t210LZ	• 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	62

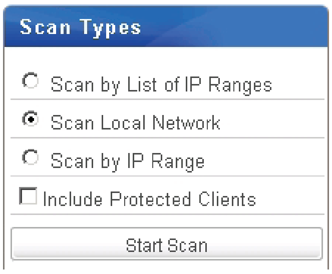
NOTE

- If the computer where an Atrust Device Manager is installed connects to a local network, then the Atrust Device Manager is connected to the local network.
- After adding clients into a managed group under your Atrust Device Manager, you can start remote management of clients. For details on how to manage your clients remotely, please refer to section "3.4 Managing All Your Clients" on page 60.

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:

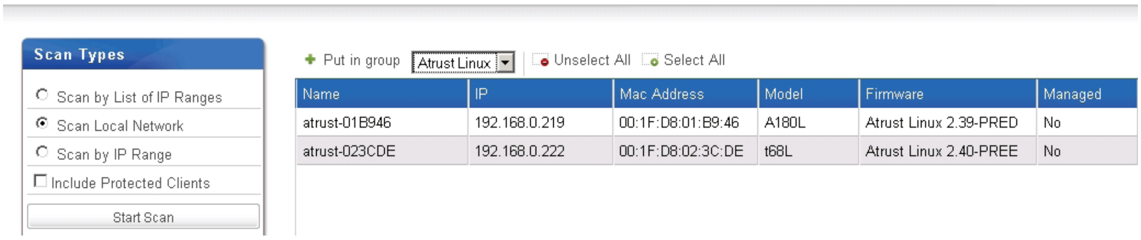
1. On **Scan** tab, click to check **Scan Local Network**.



Scan Types

○ Scan by List of IP Ranges
● Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

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



Scan Types

○ Scan by List of IP Ranges
● Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

Name	IP	Mac Address	Model	Firmware	Managed
atrust-01B946	192.168.0.219	00:1F:D8:01:B9:46	A180L	Atrust Linux 2.39-PRED	No
atrust-023CDE	192.168.0.222	00:1F:D8:02:3C:DE	t68L	Atrust Linux 2.40-PREE	No

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

NOTE

- The default client group is **Ungrouped**. You can change the group of a client at a later time. To create new client groups, please refer to section "3.4.4 Creating Client Groups" on page 64.
- 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.

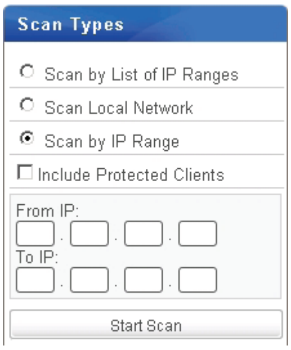
NOTE

- 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:

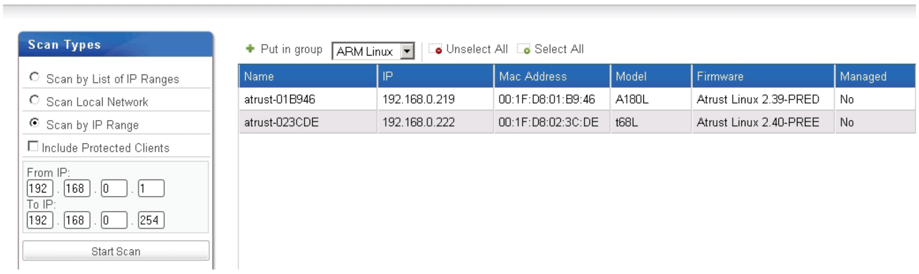
1. On **Scan** tab, click to check **Scan by IP Ranges**.
2. The IP range fields appear.



○ Scan by List of IP Ranges
○ Scan Local Network
● Scan by IP Range
□ Include Protected Clients

From IP: [ ] . [ ] . [ ] . [ ]
To IP: [ ] . [ ] . [ ] . [ ]

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



○ Scan by List of IP Ranges
○ Scan Local Network
● Scan by IP Range
□ Include Protected Clients

From IP: 192 . 168 . 0 . 1
To IP: 192 . 168 . 0 . 254

Put in group: ARM Linux

Name	IP	Mac Address	Model	Firmware	Managed
atrust-01B946	192.168.0.219	00:1F:D8:01:B9:46	A180L	Atrust Linux 2.39-PRED	No
atrust-023CDE	192.168.0.222	00:1F:D8:02:3C:DE	t68L	Atrust Linux 2.40-PREE	No

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 64.
- 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.

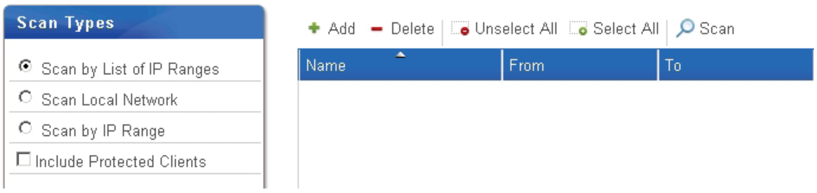
3.3.6 Creating and Managing an IP Range List

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.

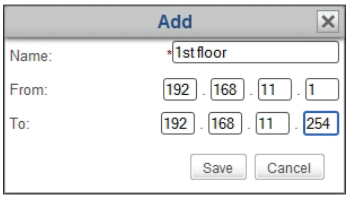


Scan Types

● Scan by List of IP Ranges
○ Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

Name	From	To

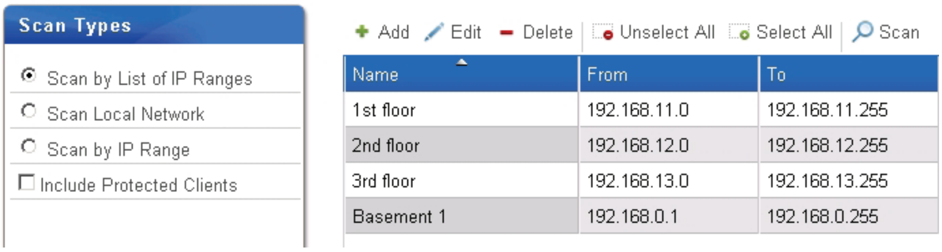
3. The Add window appears.
4. Type in the name for this entry of IP range, and specify the desired IP range using **From** and **To** fields.



Add

Name: *1st floor
From: 192 . 168 . 11 . 1
To: 192 . 168 . 11 . 254

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



Scan Types

● Scan by List of IP Ranges
○ Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

Name	From	To
1st floor	192.168.11.0	192.168.11.255
2nd floor	192.168.12.0	192.168.12.255
3rd floor	192.168.13.0	192.168.13.255
Basement 1	192.168.0.1	192.168.0.255

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.

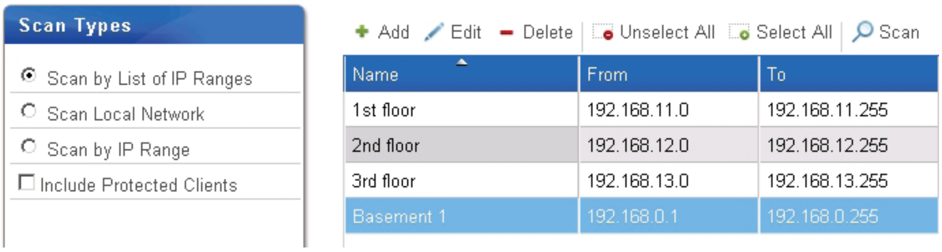
3.3.7 Discovering Clients using a Predefined IP Range List

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 56 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.



Scan Types

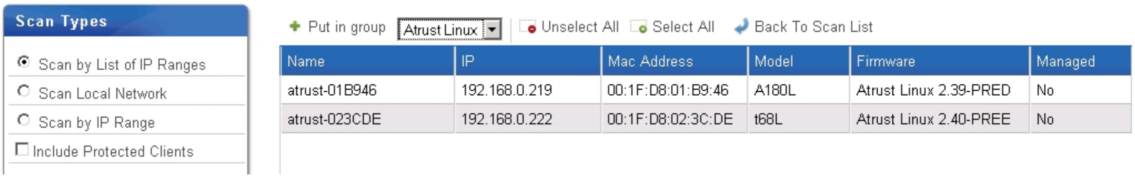
● Scan by List of IP Ranges
○ Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

Name	From	To
1st floor	192.168.11.0	192.168.11.255
2nd floor	192.168.12.0	192.168.12.255
3rd floor	192.168.13.0	192.168.13.255
Basement 1	192.168.0.1	192.168.0.255

NOTE

- To select more than one IP range, Ctrl-click to select multiple ranges.

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



Scan Types

● Scan by List of IP Ranges
○ Scan Local Network
○ Scan by IP Range
□ Include Protected Clients

Name	IP	Mac Address	Model	Firmware	Managed
atrust-01B946	192.168.0.219	00:1F:D8:01:B9:46	A180L	Atrust Linux 2.39-PRED	No
atrust-023CDE	192.168.0.222	00:1F:D8:02:3C:DE	t68L	Atrust Linux 2.40-PREE	No

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 64.
- 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.

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.

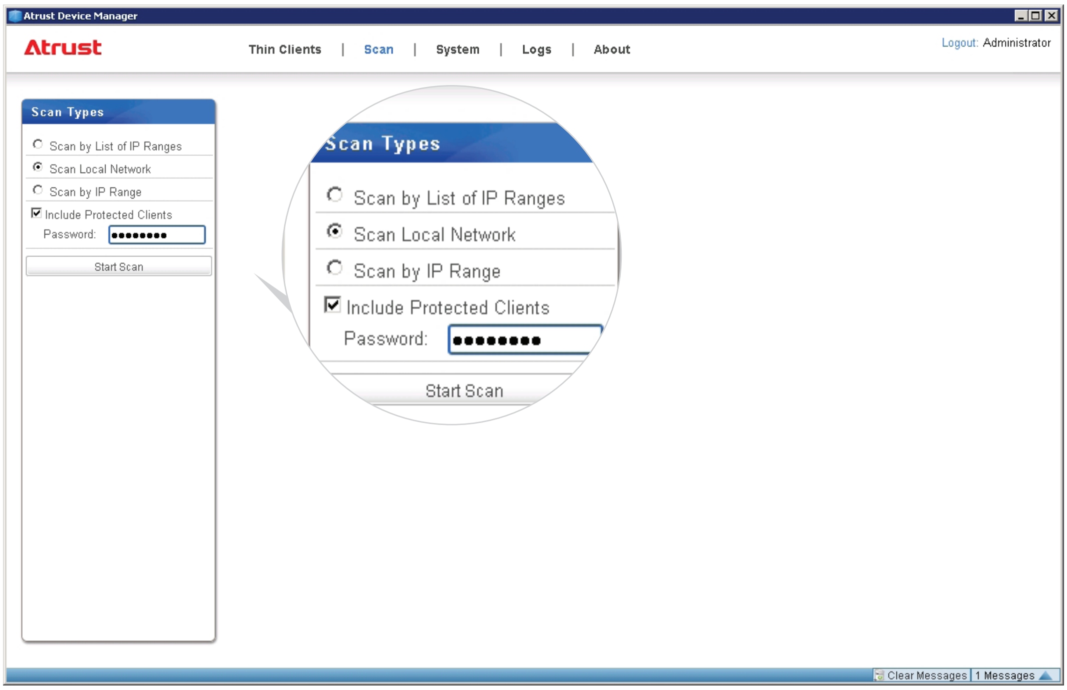
3.3.8 Discovering Thin Clients Including Those Password-Protected

To discover thin clients including those password-protected by another instance of Atrust Device Manager, please do the following:

NOTE

- To password-protect managed thin clients, please refer to "3.2.13 Setting Password Protection for Managed Thin Clients" on page 42.

1. On Atrust Device Manager, click **Scan**.
2. Select the desired discovery method, check **Include Protected Clients**, and then type the administrative password for thin clients.



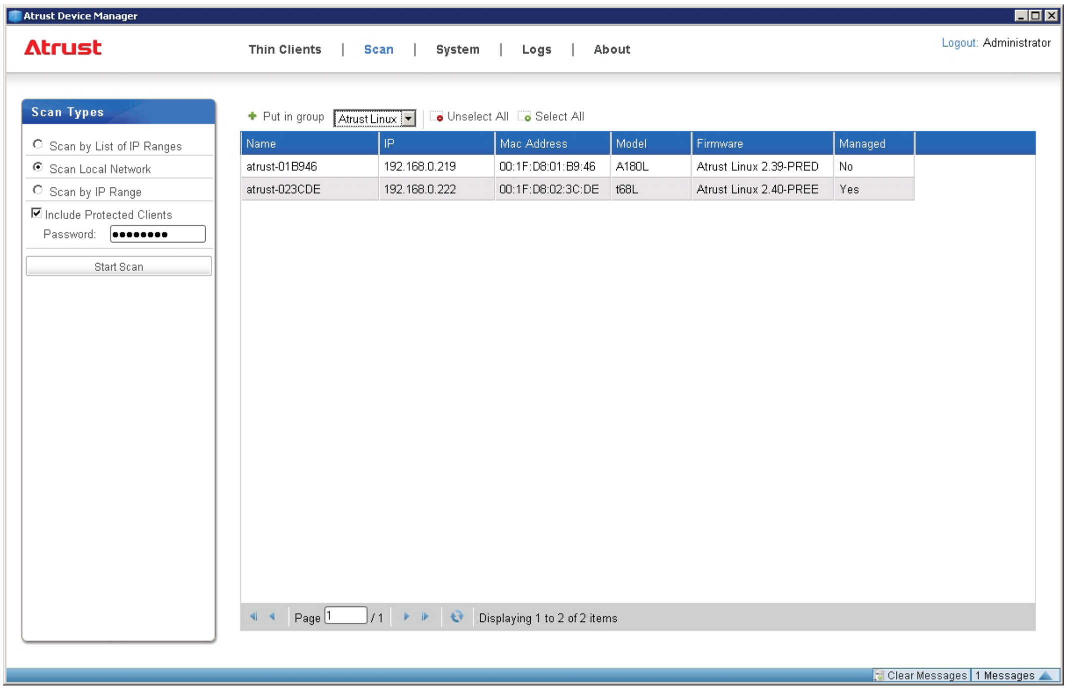
Scan Types
○ Scan by List of IP Ranges
● Scan Local Network
○ Scan by IP Range
☑ Include Protected Clients
Password: ●●●●●●●●

Atrust Device Manager
Atrust
Thin Clients | Scan | System | Logs | About
Logout: Administrator
Start Scan
Clear Messages | 1 Messages

3. Click **Start Scan** to discover thin clients.

4. The following thin clients will be listed:

    - Thin clients managed by another Atrust Device Manager and with the typed password
    - Thin clients managed by another Atrust Device Manager and not password-protected
    - Thin clients not managed by any Atrust Device Manager



○ Scan by List of IP Ranges
● Scan Local Network
○ Scan by IP Range
☑ Include Protected Clients
Password: ●●●●●●●●●

Put in group: Atrust Linux

Name	IP	Mac Address	Model	Firmware	Managed
atrust-01B946	192.168.0.219	00:1F:D8:01:B9:46	A180L	Atrust Linux 2.39-PRED	No
atrust-023CDE	192.168.0.222	00:1F:D8:02:3C:DE	t68L	Atrust Linux 2.40-PREE	Yes

Page 1 / 1

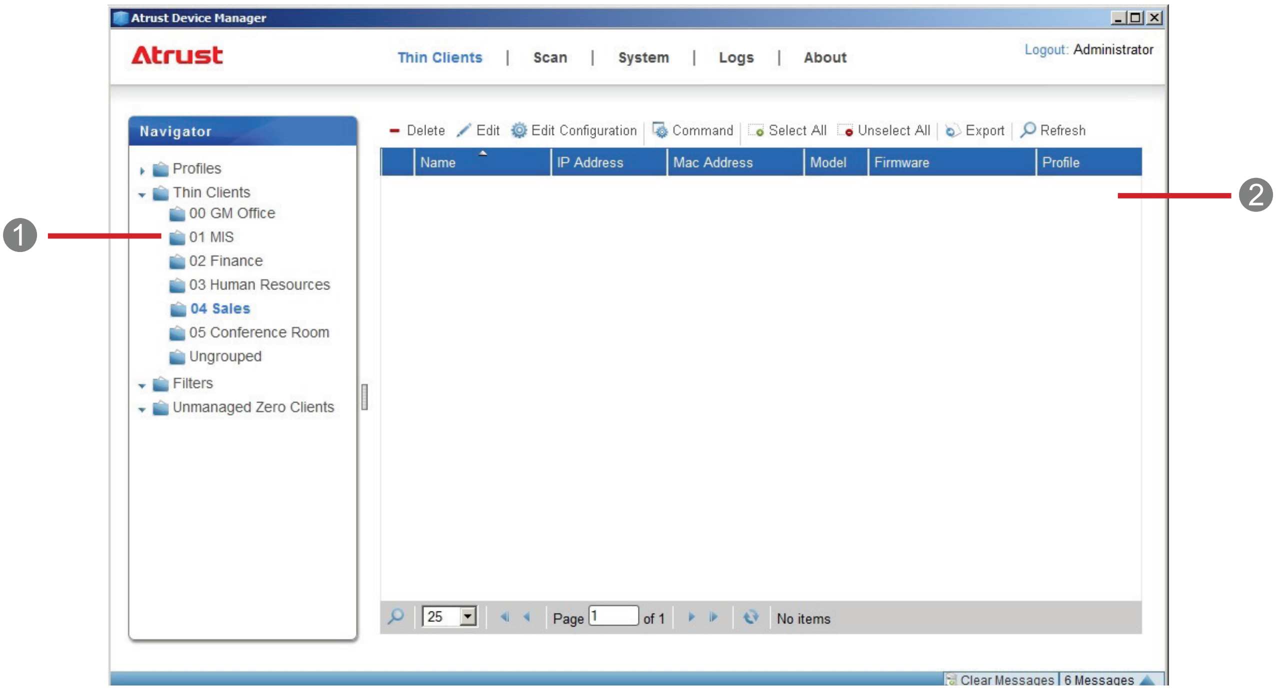
Displaying 1 to 2 of 2 items

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	62
2	Creating client groups	3.4.4	64
3	Managing client groups	3.4.5	65
4	Managing clients in a group	3.4.6 3.4.7	66 67
5	Creating setting profile groups	3.4.10	71
6	Managing setting profile groups	3.4.11	72
7	Creating client setting profiles	3.4.12	73
8	Managing client setting profiles	3.4.13	76
9	Using individualized client settings	3.4.14	79
10	Using hybrid client settings	3.4.15	80
11	Pushing settings to clients through your local network	3.4.16	82
12	Pulling settings from clients through your local network	3.4.17	86
13	Pushing certificates of remote computers to clients	3.4.18	89
14	Sending messages to clients	3.4.19	90
15	Editing or viewing basic information about a client	3.4.20	91
16	Rebooting clients through your local network	3.4.21	92
17	Shutting down clients through your local network	3.4.22	95
18	Waking clients through your local network	3.4.23	99
19	Updating client firmware	3.4.24	102
20	Installing/Uninstalling software packages	3.4.25	105
21	Taking client snapshots	3.4.26	107
22	Restoring client snapshots	3.4.27	108
23	Assisting a client user remotely	3.4.28	109
24	Monitoring a client remotely	3.4.28	109
25	Controlling a client remotely	3.4.28	109
26	Exporting client data	3.4.29	111
27	Digging out profiles or managed clients with Quick Search	3.4.30	112
28	Digging out managed clients with filters	3.4.31	113
29	Managing your client filters	3.4.32	115

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 53.
- For Atrust Device Manager 2.00 or earlier versions, you need to turn off Windows Firewall of your computer where the Atrust Device Manager console is installed in order to manage zero clients.
- Atrust recommends using a version of Atrust Device Manager later than version 2.00 for client management. Please refer to section "2.3 Upgrading Atrust Device Manager" on page 15 for ***important*** instructions.

1. On **Thin Clients** tab, click **Unmanaged Zero Clients**.
2. 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.

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

6. 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 "3.2.6 Managing Zero Client Image Files" on page 29.
- 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 64.
- 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.

7. 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.

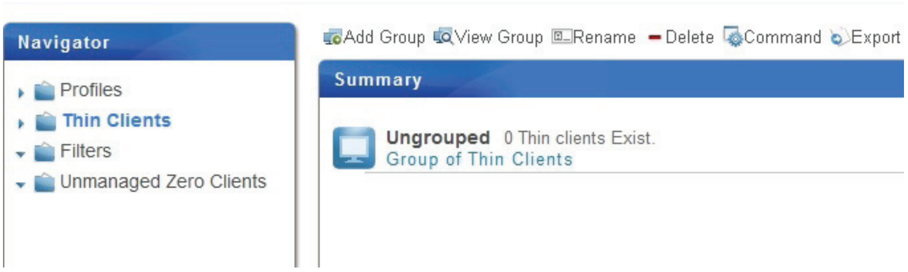
3.4.4 Creating Client Groups

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

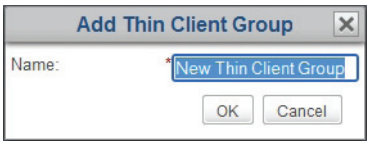
> **NOTE**
>
> - The default client group is **Ungrouped**. You can change a client's group if needed.

To create a client group, please do the following:

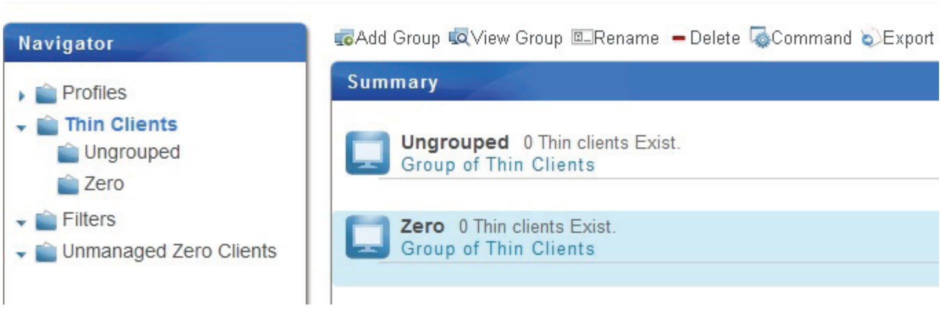
1. On **Thin Clients** tab, click **Thin Clients** in Navigation area.
2. Click **Add Group** on the top of the Management area.



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

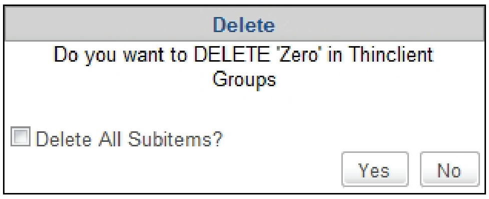
To rename a client group, please do the following:

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.



Delete

Do you want to DELETE 'Zero' in Thinclient Groups

□ Delete All Subitems?

- 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.

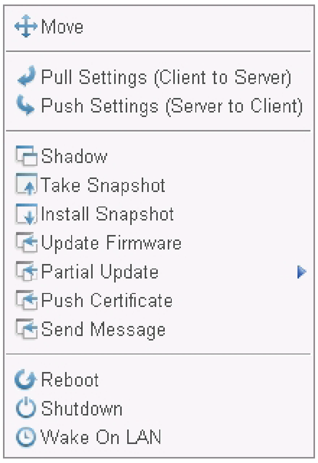
> **NOTE**
>
> - Removing a client from your Atrust Device Manager will release the client from the management of Atrust Device Manager. If the removed is a zero client then that client will become unbootable due to the lack of an operating system downloaded from and provided by the governing Atrust 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:

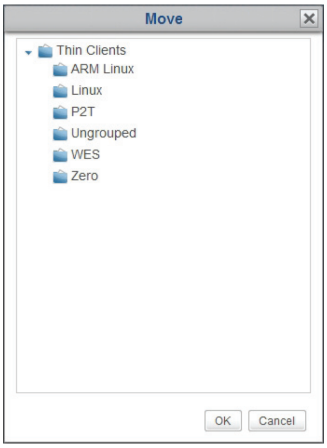
1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. Click to select the desired client, and then click **Command** on the top of the Client list to open the Command menu.



NOTE

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

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



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

3.4.7 Deleting Clients from a Group

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

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

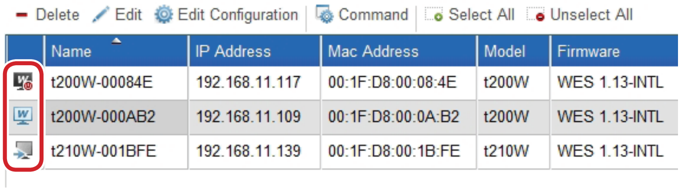
> **NOTE**
>
> - To select more than one client, Ctrl-click or use **Select All** to select multiple clients.

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

> **NOTE**
>
> - Removing a client from your Atrust Device Manager will release the client from the management of Atrust Device Manager. If the removed is a zero client then that client will become unbootable due to the lack of an operating 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 or a filter, a client status icon is placed in front of each client to indicate the current state of the client.



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

NOTE

- With filters, you can access and manage a specific set of clients quickly on Atrust Device Manager. For more information on filters, please refer to section "3.4.31 Digging Out Clients with Filters" on page 113.

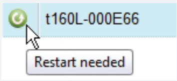
The status icon changes according to different states of a client. Six types of icons are available:

Understanding Client Status Icons

State	Icon	Description
Online	L W Z P	Indicates that the client is turned on at the moment.
Offline	L W Z P	Indicates that the client is turned off at the moment.
Reboot needed	↻	Indicates that you need to reboot the client for a configuration change to take effect.
Modified		Indicates that a client configuration change has been made on Atrust Device Manager and you need to push the change to the client.
Pushed		Indicates that Atrust Device Manager has pushed a configuration change to the client (also see NOTE below).
Unknown	?	Indicates that the previously managed client is not under the management now.

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, Windows Embedded-based thin client, or a Zero client.
- A tooltip pops up as shown below if you hover your mouse pointer over an icon.



- icon indicates that Atrust Device Manager has tried to push a configuration change to the client no matter it's successful or not. A popup message would let you know if that task succeeds or fails. Your thin client should also move to the next state and show another status icon if that task is done on the client side.

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 all-in-one, mobile, t-series zero / thin clients can meet a wide range of forms and needs. However, To get your client device ready for use in your IT infrastructure, you might need to customize client settings to meet the specific needs in your desktop virtualization plan.

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

NOTE

- The available ***tabs*** and ***setting items*** may vary, depending on: the ***client model***, ***firmware version***, and the used ***operating system***. For more details, please see chapter 4 "Configuring Client Settings" on page 123.

Remote and Local Management of Client Settings

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

NOTE

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

Some client settings are only available locally on clients. You can configure those settings locally through the Atrust Client Setup console. For a detailed list of client settings that are only locally available, please refer to section "4.2 Client Settings at a Glance" on page 125.

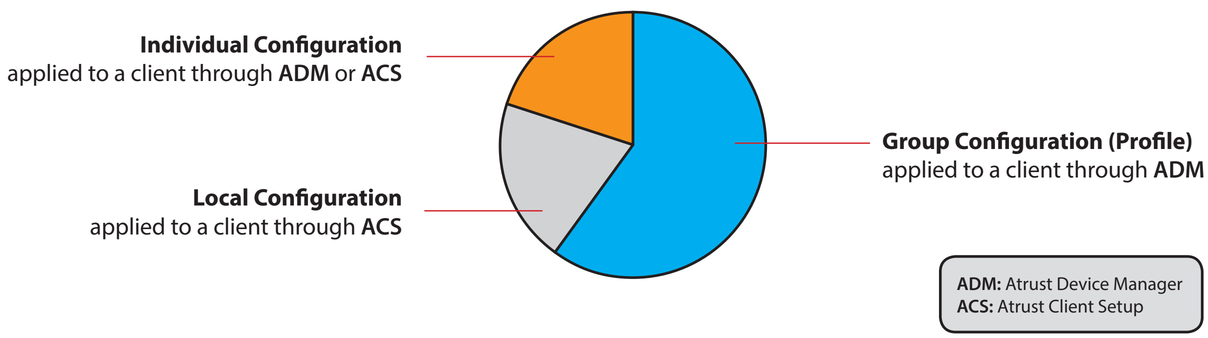
Group Configuration and Individual Configuration

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	Console	Section	Page
Local	Local configuration	Atrust Client Setup (ACS)	4.2 4.5	125 135
	Individual configuration	Atrust Client Setup (ACS)	4.2 4.5	125 135
Remote	Group configuration	Atrust Device Manager (ADM)	3.4.12	73
	Individual configuration	Atrust Device Manager (ADM)	3.4.14	79

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

Locking the Setting Values

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

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

3.4.10 Creating Setting Profile Groups

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

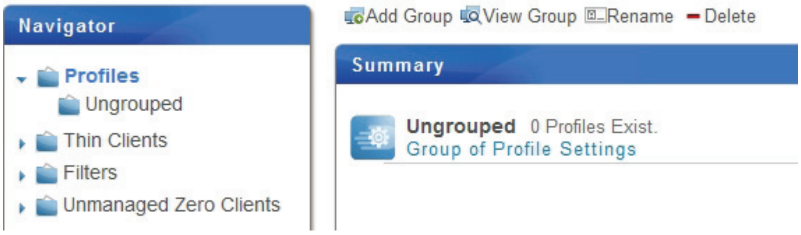
A setting profile group is a set of profiles grouped together for ease of management.

NOTE

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

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

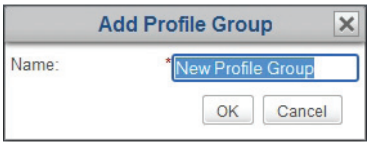
1. On **Thin Clients** tab, click **Profiles**.
2. The Profile Group list appears.



NOTE

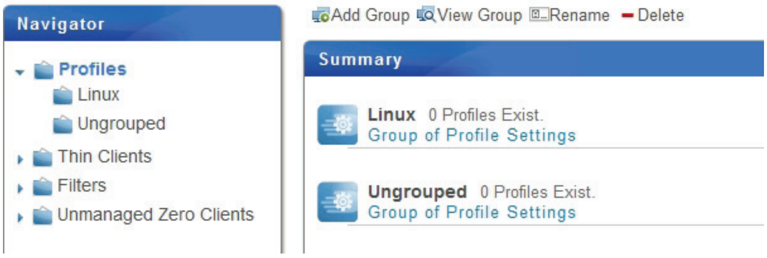
- **Ungrouped** is the system default group.

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



Name: * New Profile Group

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

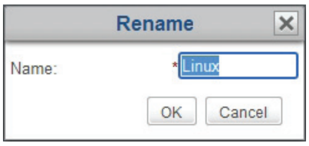


3.4.11 Managing Setting Profile Groups

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.

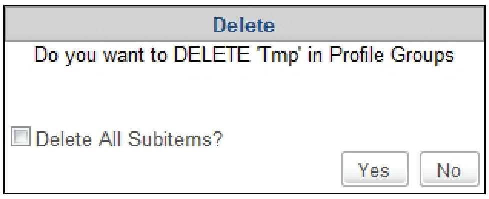


4. Type in the new name for the profile group, and then click **OK** to confirm.

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.



Do you want to DELETE 'Tmp' in Profile Groups

- 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 of client settings shared by a set of clients. Deleting a setting profile will change client settings of the corresponding clients.

3.4.12 Creating Client Setting Profiles

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

> **NOTE**
>
> - To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 69.

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

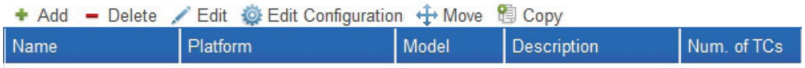
STEP 1: Create a set of shared client settings

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.

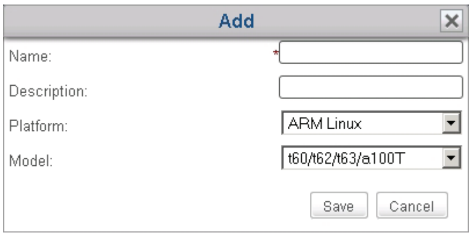
> **NOTE**
>
> - You need to select the profile group to which the new profile belongs first. You can use the system default (**Ungrouped**), and change the group at a later time if necessary. For detailed instructions on how to create a profile group, please refer to section "3.4.10 Creating Setting Profile Groups" on page 71.

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



Name	Platform	Model	Description	Num. of TCs

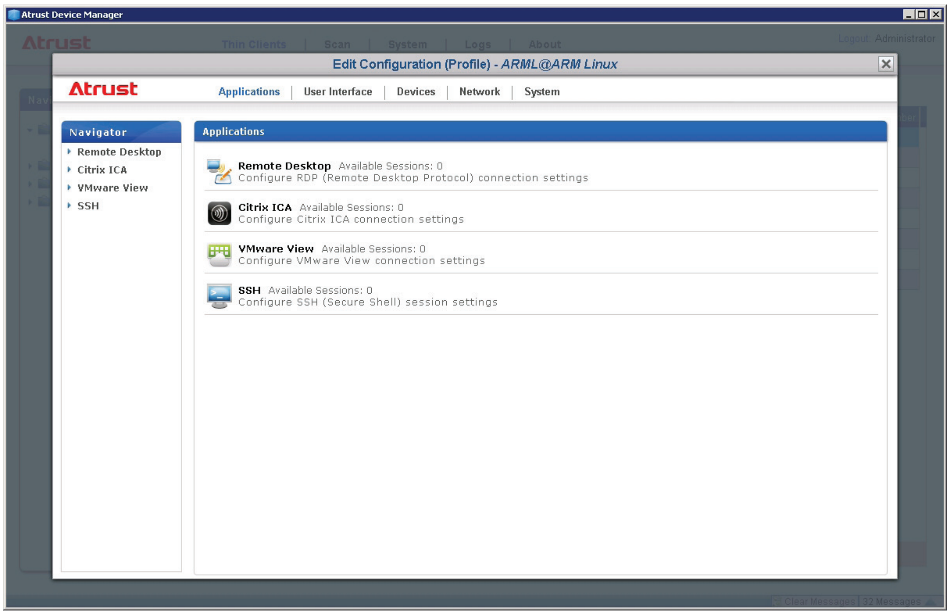
3. The Add window appears prompting for the name, description, applicable platform, and models.



Name: *
Description:
Platform: ARM Linux
Model: t60/t62/t63/a100T

> **NOTE**
>
> - A field marked with an asterisk is the required field.

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



Edit Configuration (Profile) - *ARML@ARM Linux*

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

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

NOTE

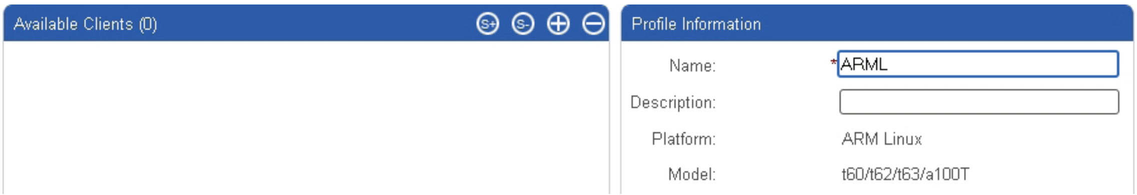
- The Edit Configuration window for the profile (group configuration) is just like a remote version of Atrust Client Setup on a client. You can simply edit client settings for this setting profile through this window. For detailed instructions on how to configure client settings, please refer to "Configuring Client Settings" on page 123.

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.

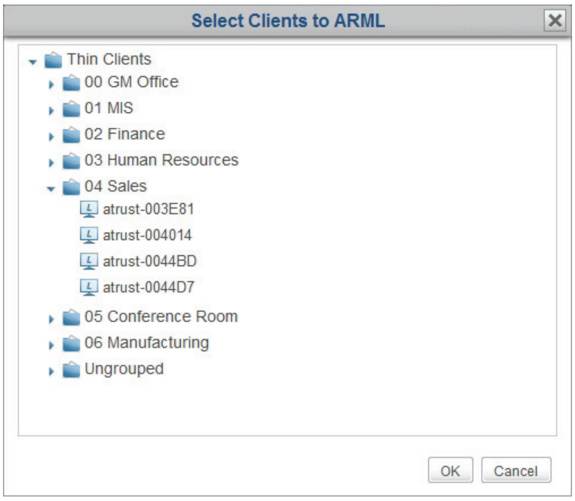


Name: * ARML
Description:
Platform: ARM Linux
Model: t60/t62/t63/a100T

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 expand the tree and click to select the desired client group or individual clients.

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



NOTE

- The tree view of client groups and individual clients corresponds exactly to client groups and individual clients established under **Thin Clients** tab. For information on how to create client groups and add clients to a group, please refer to "3.4.4 Creating Client Groups" on page 64 and "3.3.3 Client Detection and Management" on page 53 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 82.

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

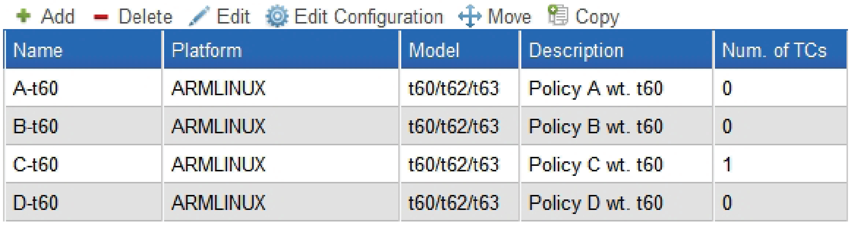
- Only a well defined setting profile is actually used for remote configuration of multiple clients. If the applicable scope of a setting profile is not specified, the profile (group configuration) doesn't affect any client.
- From now on, we will call a client configuration set up by applying a shared 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	Platform	Model	Description	Num. of TCs
A-t60	ARMLINUX	t60/t62/t63	Policy A wt. t60	0
B-t60	ARMLINUX	t60/t62/t63	Policy B wt. t60	0
C-t60	ARMLINUX	t60/t62/t63	Policy C wt. t60	1
D-t60	ARMLINUX	t60/t62/t63	Policy D wt. t60	0

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

- To adjust client settings, change desired settings directly in the opened Edit Configuration window.
- To adjust profile information, make changes in the Profile Information pane, and then click Save to apply.

> **NOTE**
>
> - For detailed instructions on the adjustment of client settings or profile information, please refer to section "3.4.12 Creating Client Setting Profiles" on page 73.

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

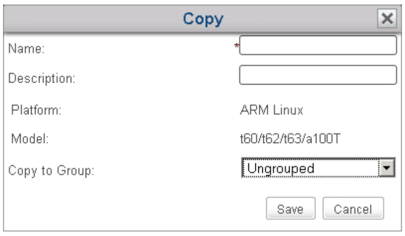
Button	Description
S+	Click to select all clients in the client list.
S-	Click to unselect all clients in the client list.
⊕	Click to add new clients.
⊖	Click to remove the selected clients.

Copying a Setting Profile

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

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

4. The Copy window appears prompting for the name, description, and profile group.



Name: *

Description:

Platform: ARM Linux

Model: t60/t62/t63/a100T

Copy to Group: Ungrouped

NOTE

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

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

NOTE

- The following steps are similar to those for creating a new setting profile. More information, including both screenshots and notes, can be found in section "3.4.12 Creating Client Setting Profiles" on page 73.

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

NOTE

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

10. Click to select the newly created profile, and then click **Edit** on the top of the Profile list.
11. Both the Profile Information and Available Clients panes appear in Management area.
12. Click ⊕ at the right top of the Available Clients pane.
13. The Select Clients window appears. A tree view of client groups and individual clients is provided in the window for specifying the applicable scope of this setting profile.
14. Click on arrows to expand the tree and click to select the desired client group or clients.

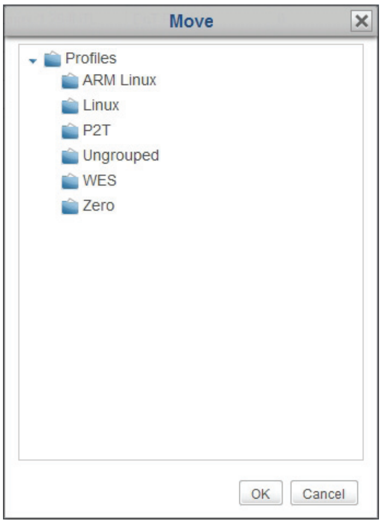
    - To select all clients under a client group, click to select the client group.
    - To select multiple clients under a client group, Ctrl-click to select the desired clients.

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

Moving a Setting Profile

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

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

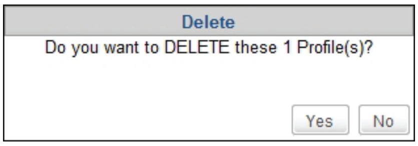


5. Click to select the desired profile group, and then click **OK** to confirm.
6. The selected setting profile is moved to the desired profile group.

Deleting a Setting Profile

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

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


Delete

Do you want to DELETE these 1 Profile(s)?

5. Click **Yes** to confirm.

NOTE

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

3.4.14 Using Individualized Client Settings

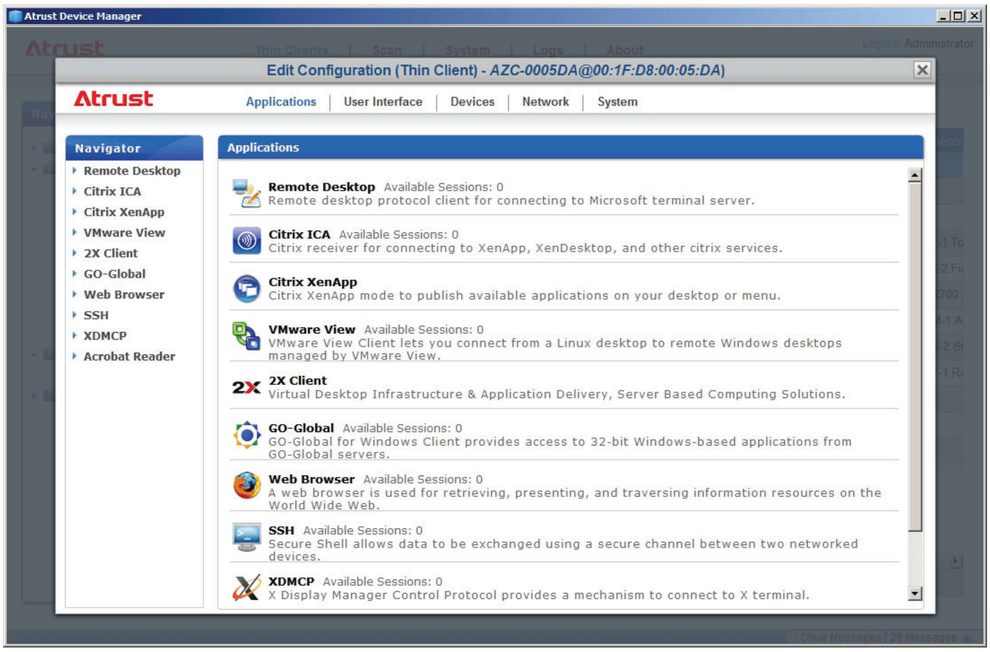
An individual configuration is a set of client settings applied only to a single client.

NOTE

- To have a basic understanding of client configuration, please refer to section “3.4.9 Client Settings” on page 69.
- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it’s recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section “3.4.17 Pulling Client Settings through Your Local Network” on page 86.

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.



Edit Configuration (Thin Client) - *AZC-0005DA@00:1F:D8:00:05:DA*

Remote Desktop Available Sessions: 0
Remote desktop protocol client for connecting to Microsoft terminal server.

Citrix ICA Available Sessions: 0
Citrix receiver for connecting to XenApp, XenDesktop, and other citrix services.

Citrix XenApp
Citrix XenApp mode to publish available applications on your desktop or menu.

VMware View Available Sessions: 0
VMware View Client lets you connect from a Linux desktop to remote Windows desktops managed by VMware View.

2X Client
Virtual Desktop Infrastructure & Application Delivery, Server Based Computing Solutions.

GO-Global Available Sessions: 0
GO-Global for Windows Client provides access to 32-bit Windows-based applications from GO-Global servers.

Web Browser Available Sessions: 0
A web browser is used for retrieving, presenting, and traversing information resources on the World Wide Web.

SSH Available Sessions: 0
Secure Shell allows data to be exchanged using a secure channel between two networked devices.

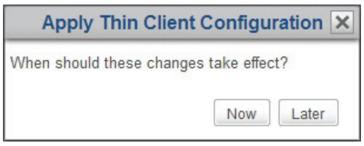
XDMCP Available Sessions: 0
X Display Manager Control Protocol provides a mechanism to connect to X terminal.

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 80 for more details).
- For detailed instructions on how to configure specific client settings, please refer to chapter 4 "Configuring Client Settings" on page 123.

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


Apply Thin Client Configuration

When should these changes take effect?

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 69.

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 73.

STEP 2: Apply an individual configuration to the client

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

NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 86.

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 79.

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 69 and chapter 4 "Configuring Client Settings" on page 123 for more details.

Pushing Settings to a Client

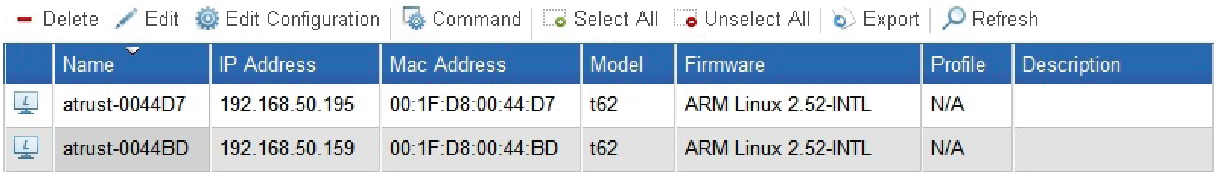
To push settings to a client, please do the following:

NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 86.

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.



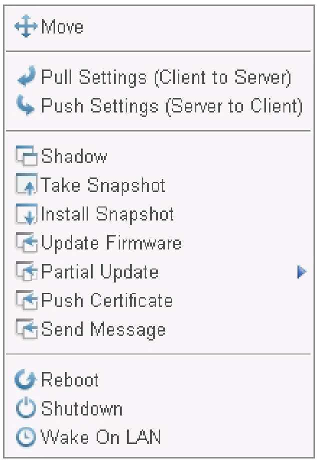
	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

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

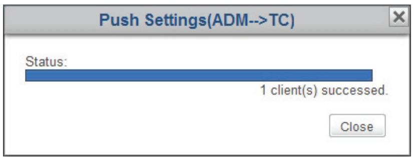
NOTE

- 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 68.

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.


Push Settings(ADM-->TC)

Status:

1 client(s) successed.

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

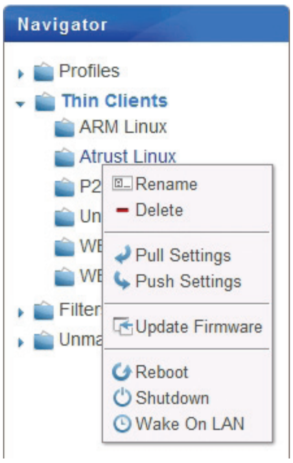
Pushing Settings to a Client Group

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

NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 86.

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 68.

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

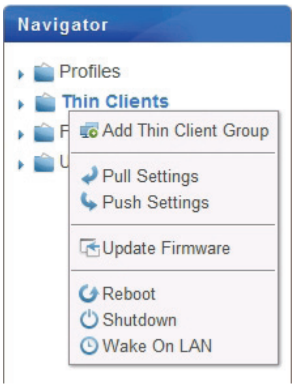
Pushing Settings to All Client Groups

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

NOTE

- To ensure that your Atrust Device Manager is in sync with the setting values on managed clients, it's recommended to ***pull client settings from all managed clients*** for Atrust Device Manager ***before*** editing individualized client settings. For detailed instructions on how to pull client settings from managed clients, please refer to section "3.4.17 Pulling Client Settings through Your Local Network" on page 86.

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 68.

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

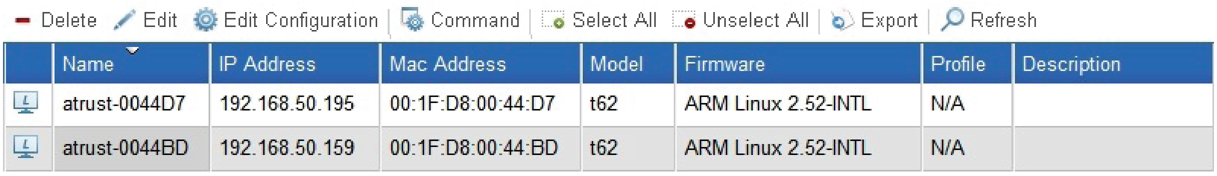
The **Pull Settings** feature enables you to retrieve settings from a client and store in Atrust Device Manager, which help you sync up the client configuration in Atrust Device Manager with the one set up locally on a client.

> **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 69 and chapter 4 "Configuring Client Settings" on page 123 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.

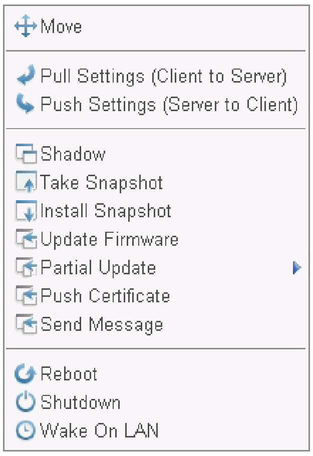


	Name	IP Address	Mac Address	Model	Firmware	Profile	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

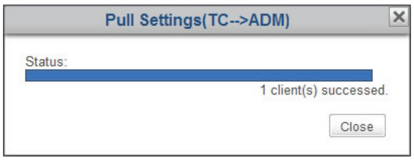
3. Click to select the desired client, and then click **Command** on the top of the Client list.

> **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 68.

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.



Pull Settings(TC-->ADM)

Status:

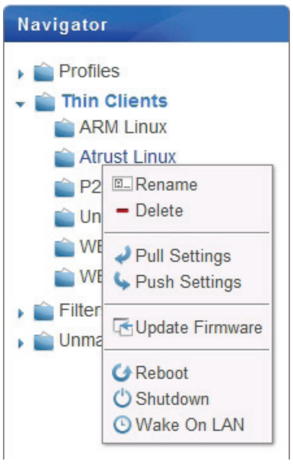
1 client(s) successed.

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

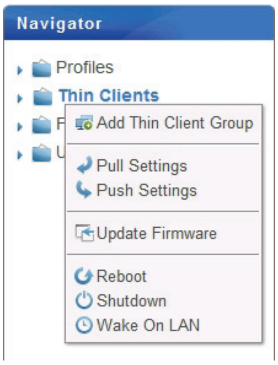
- Ensure that clients in the selected group are all powered up. Otherwise you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 68.

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

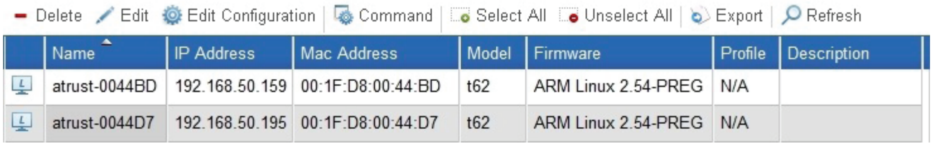
- Ensure that all clients are powered up. Otherwise, you may fail to pull settings from some clients. You can remotely know the current status of a client through the Status icon in front of the client. For information on the Status icons, please refer to section "3.4.8 Understanding Client Status Icons" on page 68.

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

3.4.18 Pushing Certificates of Remote Computers to Clients

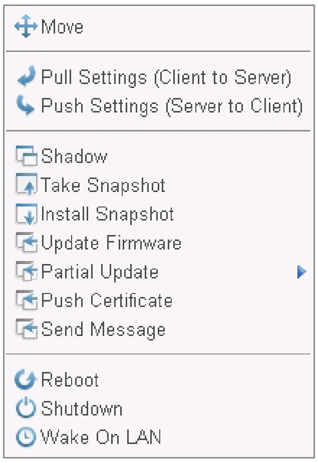
To push certificates of remote computers to a thin client, please do the following:

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.

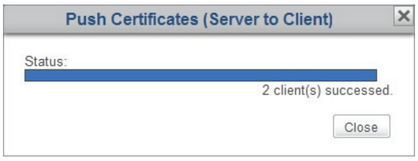


Name	IP Address	Mac Address	Model	Firmware	Profile	Description
atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.54-PREG	N/A	
atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.54-PREG	N/A	

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 **Push Certificate**.
6. A window appears prompting for confirmation.
7. Click **OK** to confirm.
8. The Push Certificates window appears showing the progress and result of pushing certificates.



Status:

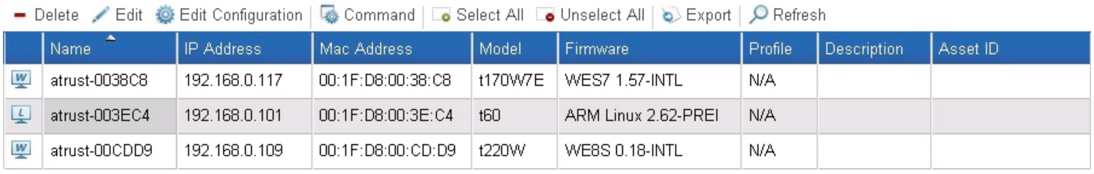
2 client(s) successed.

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

3.4.19 Sending Messages to Clients

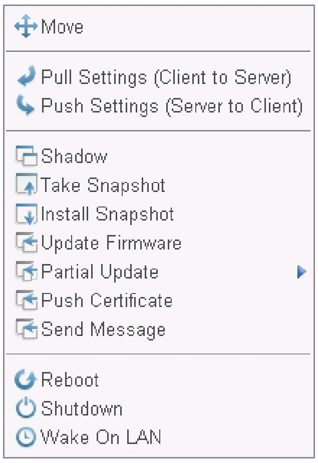
To send a message to the managed client(s), please do the following:

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

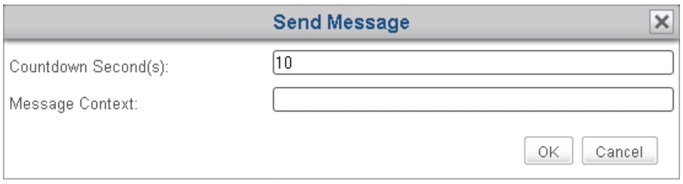


	Name	IP Address	Mac Address	Model	Firmware	Profile	Description	Asset ID
W	atrust-0038C8	192.168.0.117	00:1F:D8:00:38:C8	t170W7E	WES7 1.57-INTL	N/A		
L	atrust-003EC4	192.168.0.101	00:1F:D8:00:3E:C4	t60	ARM Linux 2.62-PREI	N/A		
W	atrust-00CDD9	192.168.0.109	00:1F:D8:00:CD:D9	t220W	WE8S 0.18-INTL	N/A		

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



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


Send Message

Countdown Second(s): 10

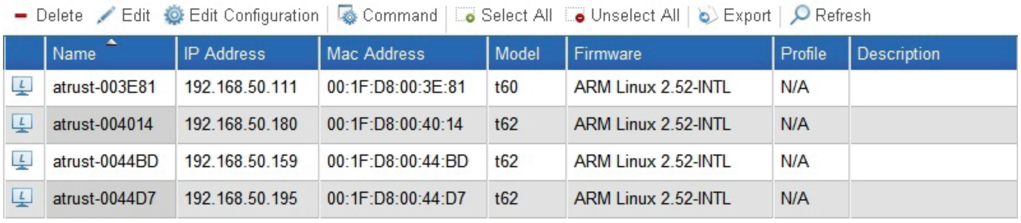
Message Context:

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

3.4.20 Editing or Viewing the Basic Information about a Client

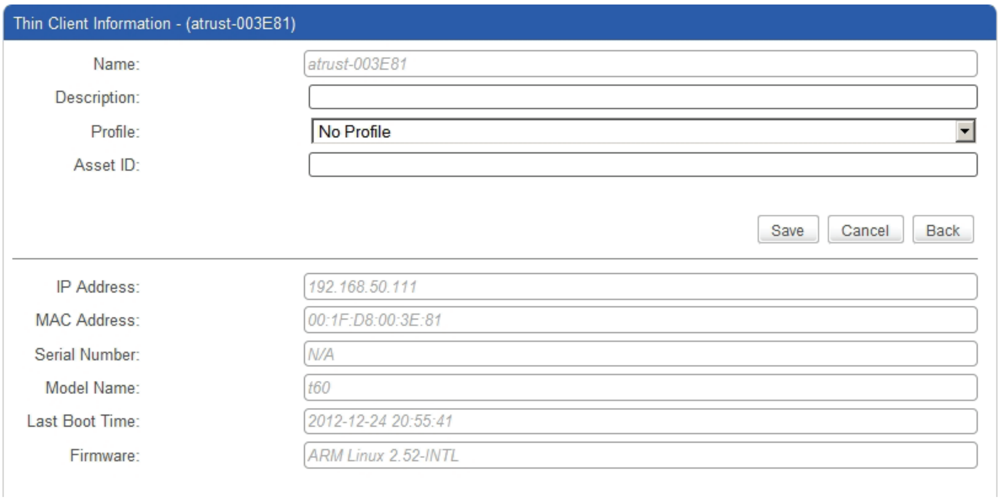
To edit or view the basic information about a client, please do the following:

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



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

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



Thin Client Information - (atrust-003E81)

Name: atrust-003E81
Description:
Profile: No Profile
Asset ID:

IP Address: 192.168.50.111
MAC Address: 00:1F:D8:00:3E:81
Serial Number: N/A
Model Name: t60
Last Boot Time: 2012-12-24 20:55:41
Firmware: ARM Linux 2.52-INTL

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

   - To adjust the name, comment, profile (group configuration), Asset ID for the client, or type in the new data, and then click **Save** to apply.

   NOTE

   - When selecting a profile (group configuration) from the drop-down menu, you add the client into the applicable scope of the selected profile.

   - After viewing the basic information, click **Back** to return to the Client list.

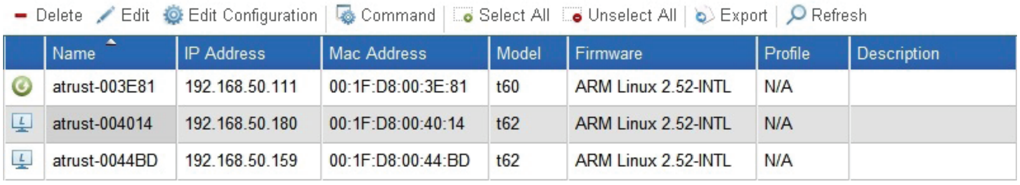
3.4.21 Rebooting Clients through Your Local Network

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

Rebooting a Client through Your Local Network

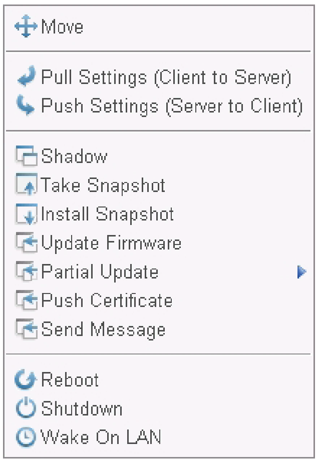
To restart a client through your local network, please do the following:

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



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

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



4. Click to select **Reboot**.

NOTE

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

WARNING

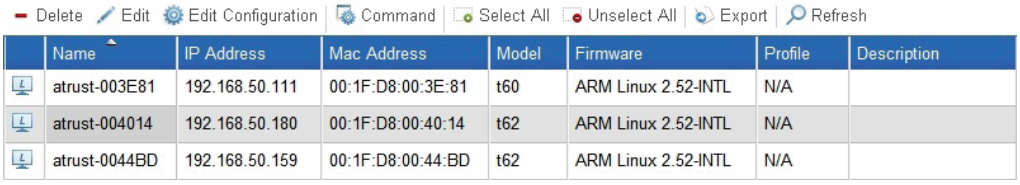
- Ensure that no important tasks are performed on the selected clients.

5. On the selected client, a warning message appears to notify the user of the planned reboot and allow the user to cancel the action if necessary.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

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



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

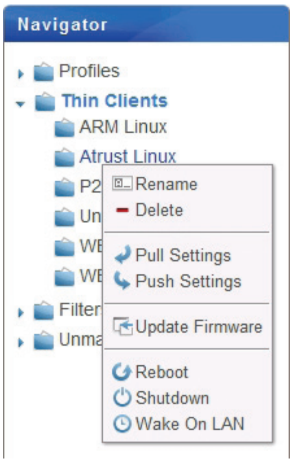
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

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.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

5. After completion, the Status icons will indicate clients of this group are on-line again.

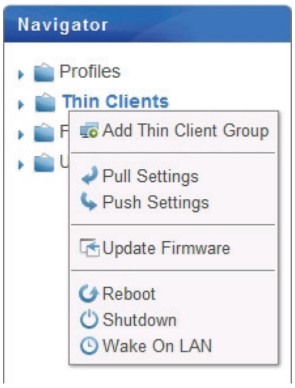
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

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.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

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

NOTE

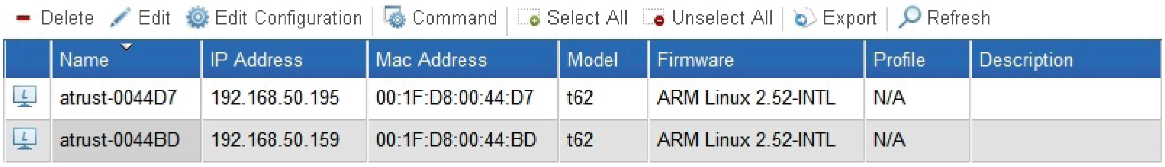
- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

3.4.22 Shutting Down Clients through Your Local Network

Shutting Down a Client through Your Local Network

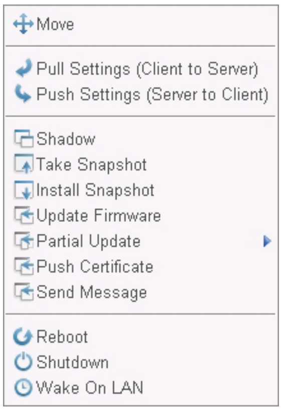
To shut down a client through your local network, please do the following:

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



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

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



4. Click to select **Shutdown**.

NOTE

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

WARNING

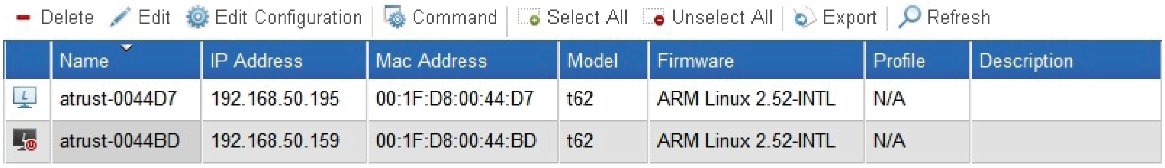
- Ensure that no important tasks are performed on the selected clients.

5. On the selected client, a warning message appears to notify the user of the planned shutdown and allow the user to cancel the action if necessary.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

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



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

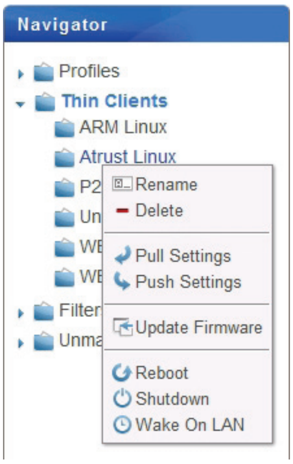
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

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.

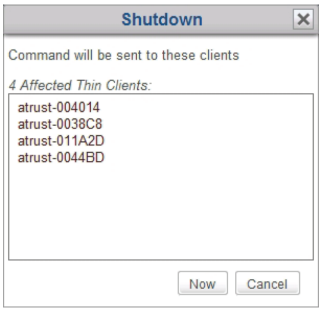


3. Click to select **Shutdown**.

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.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

7. After completion, the Status icons will indicate clients of this group are off-line.

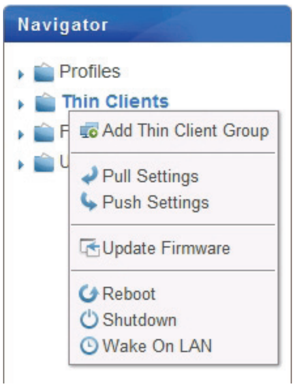
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

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.

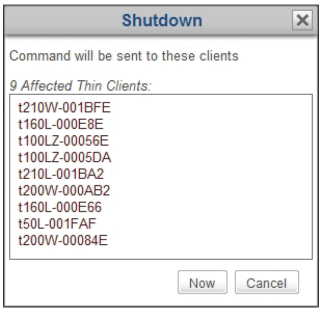


2. Click to select **Shutdown**.

WARNING

- Ensure that no important tasks are performed on clients.

3. The Shutdown window appears prompting for confirmation.



Command will be sent to these clients

9 Affected Thin Clients:

t210W-001BFE
t160L-000E8E
t100LZ-00056E
t100LZ-0005DA
t210L-001BA2
t200W-000AB2
t160L-000E66
t50L-001FAF
t200W-00084E

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.

NOTE

- You can customize the default behaviors on Atrust Device Manager. For details, please refer to "A.4 Customizing Remote Reboot and Shutdown of Thin Clients" on page 151.

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 68.

3.4.23 Waking Clients through Your Local Network

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

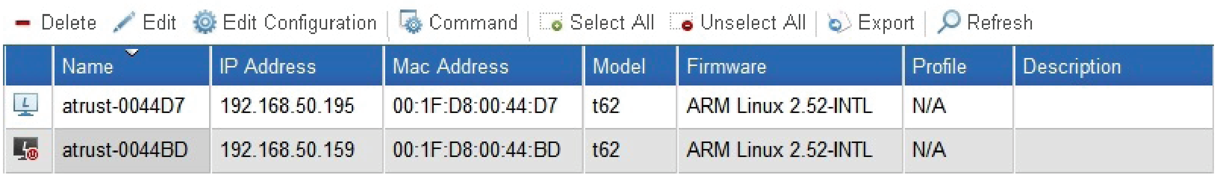
NOTE

- t50 does not support the **Wake On LAN** feature.

Waking a Client through Your Local Network

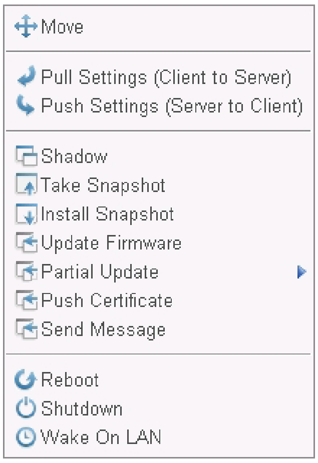
To wake a client through your local network, please do the following:

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	Description
	atrust-0044D7	192.168.50.195	00:1F:D8:00:44:D7	t62	ARM Linux 2.52-INTL	N/A	
	atrust-0044BD	192.168.50.159	00:1F:D8:00:44:BD	t62	ARM Linux 2.52-INTL	N/A	

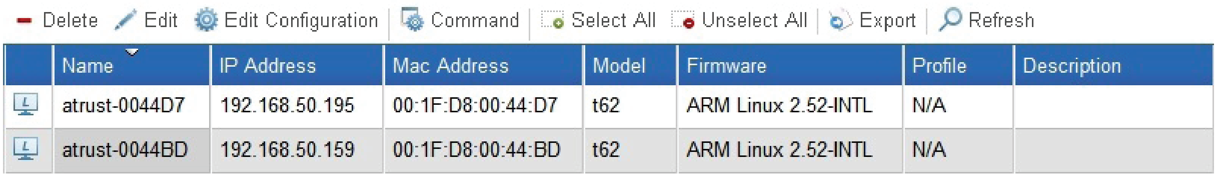
3. Click to select the desired client, and then click **Command** to open the Command menu.



NOTE

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

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



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

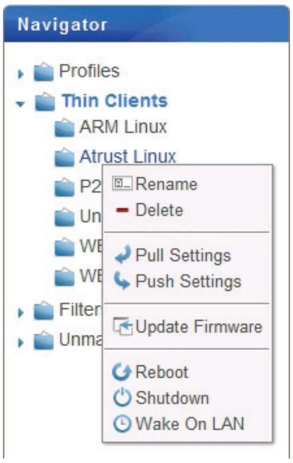
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

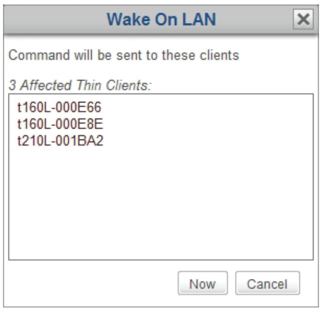
Waking a Client Group through Your Local Network

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.



Command will be sent to these clients

3 Affected Thin Clients:

t160L-000E66
t160L-000E8E
t210L-001BA2

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.

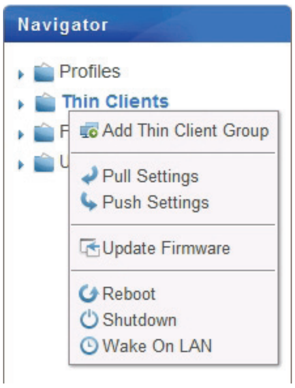
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

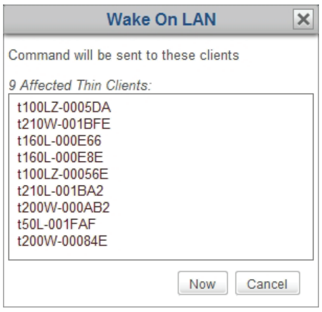
Waking All Client Groups through Your Local Network

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**.



Command will be sent to these clients

9 Affected Thin Clients:

t100LZ-0005DA
t210W-001BFE
t160L-000E66
t160L-000E8E
t100LZ-00056E
t210L-001BA2
t200W-000AB2
t50L-001FAF
t200W-00084E

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 68.

3.4.24 Updating Client Firmware

The **Update Firmware** feature enables your to update the firmware for your client through the network.

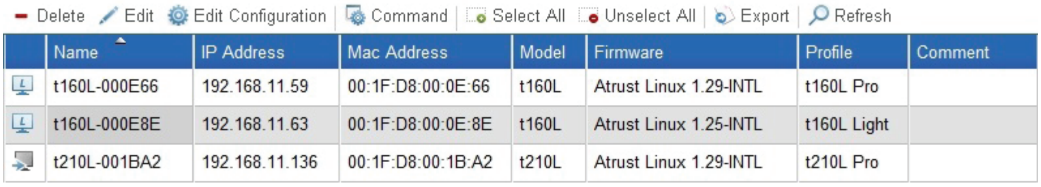
Updating Firmware for a Client through the Network

To update the firmware for a client through the network, 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.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Comment
	t160L-000E66	192.168.11.59	00:1F:D8:00:0E:66	t160L	Atrust Linux 1.29-INTL	t160L Pro	
	t160L-000E8E	192.168.11.63	00:1F:D8:00:0E:8E	t160L	Atrust Linux 1.25-INTL	t160L Light	
	t210L-001BA2	192.168.11.136	00:1F:D8:00:1B:A2	t210L	Atrust Linux 1.29-INTL	t210L Pro	

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

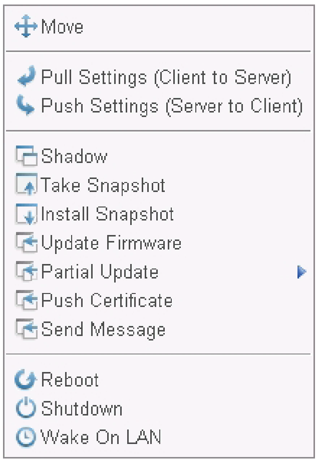
NOTE

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

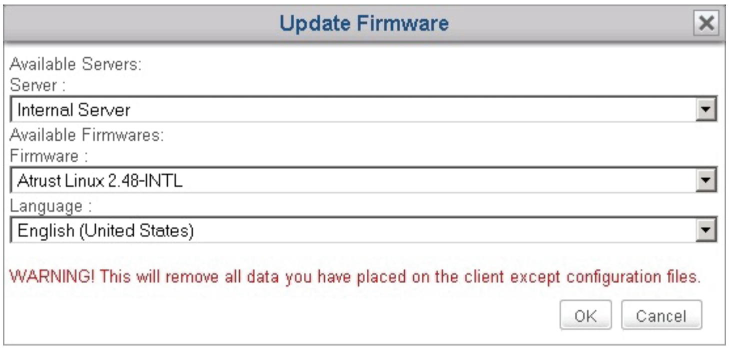
WARNING

- 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 server where to get firmware files, firmware version, and system language.



Update Firmware

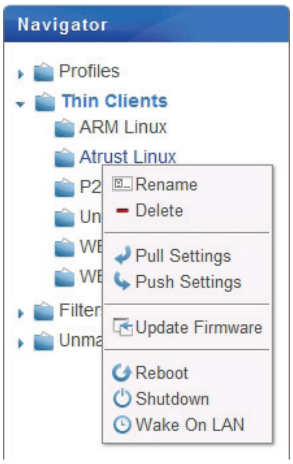
Available Servers:
Server : Internal Server
Available Firmwares:
Firmware : Atrust Linux 2.48-INTL
Language : English (United States)

WARNING! This will remove all data you have placed on the client except configuration files.

7. Click drop-down menus to select the desired server, 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.

Updating Firmware for a Client Group through the Network

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



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

WARNING

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

4. The Update Firmware window appears prompting you to select the server, model, firmware version, and system language. Click **OK** to continue.
5. On the opened window, check the Client list, and then click **Now** to confirm.

6. On each applicable 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.
7. After completion, the Status icons will indicate clients of this group are on-line again.

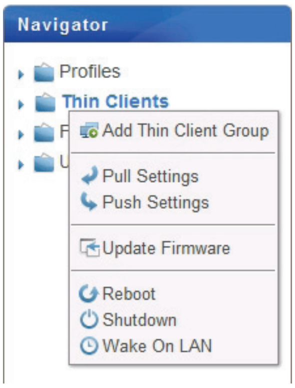
NOTE

- For information on the meanings of the Status icons, please refer to "3.4.8 Understanding Client Status Icons" on page 68.

Updating Firmware for All Client Groups through the Network

To update the firmware for all client groups through the network, please do the following:

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



2. Click to select **Update Firmware**.

WARNING

- Ensure that no important tasks are performed on clients.

3. The Update Firmware window appears prompting you to select the server, model, firmware version, and system language. Click **OK** to continue.
4. On the opened window, check the Client list, and then click **Now** to confirm.
5. On each applicable 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 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 68.

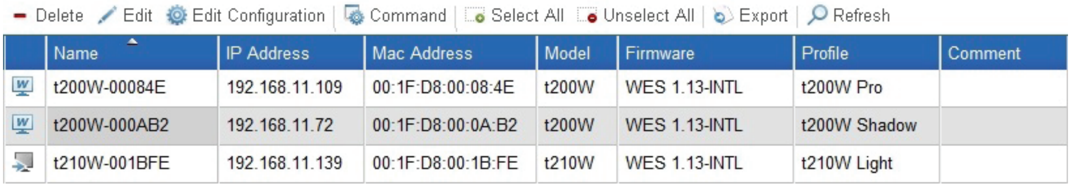
3.4.25 Installing and Uninstalling Software Packages

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

NOTE

- Installing additional software packages is allowed only for Windows Embedded-based thin 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.

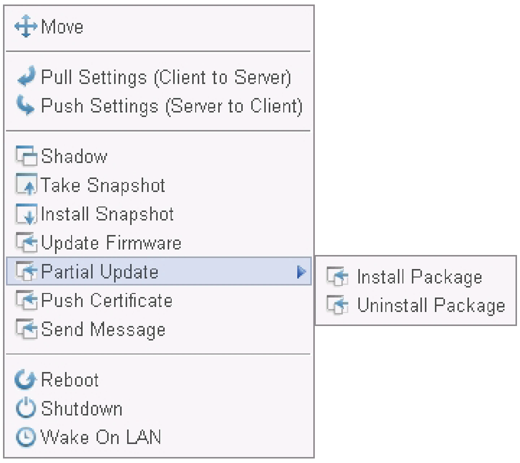
NOTE

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

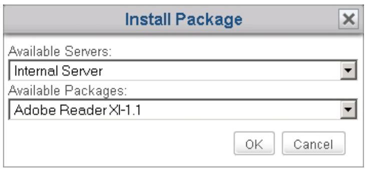
WARNING

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

4. The Command menu appears.
5. Click **Partial Update**, and then click to select **Install Package** or **Uninstall Package**.



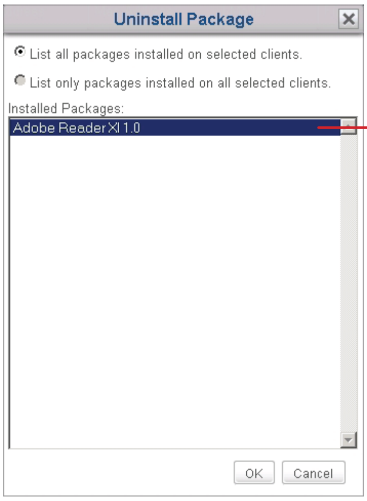
6. On the opened window, select the desired software package to install or uninstall, and then click **OK**.



Install Package

Available Servers: Internal Server

Available Packages: Adobe Reader XI-1.1



Uninstall Package

● List all packages installed on selected clients.

○ List only packages installed on all selected clients.

Installed Packages: Adobe Reader XI 1.0

Highlight a package to select it

7. 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. More than one reboot is required to complete the task.

TIP

- To check remotely if the installation is completed, select the client, and then click **Edit** to view the basic information about a client. For more details, refer to section "3.4.20 Editing or Viewing the Basic Information about a Client" on page 91.

3.4.26 Taking Client Snapshots

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

NOTE

- Atrust t-series zero clients download their operating system while connecting to the local network. Therefore, there is no need to take any local system copy. Atrust t-series zero clients include t100LZ, t160LZ, t200LZ, t210LZ etc.
- Only Windows Embedded-based thin clients support this feature.

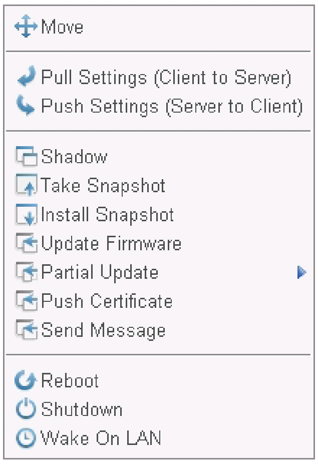
To take a system snapshot for a client, please do the following:

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.

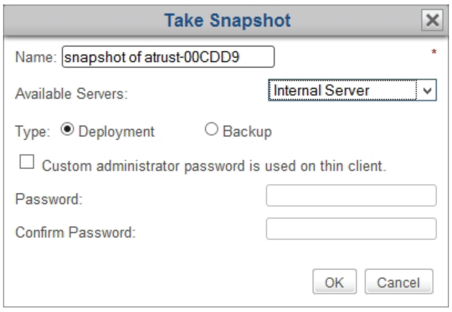
NOTE

- 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 select where to store the snapshot, choose its type, and provide its name.



Name: snapshot of atrust-00CDD9 *

Available Servers: Internal Server

Type: ● Deployment ○ Backup

□ Custom administrator password is used on thin client.

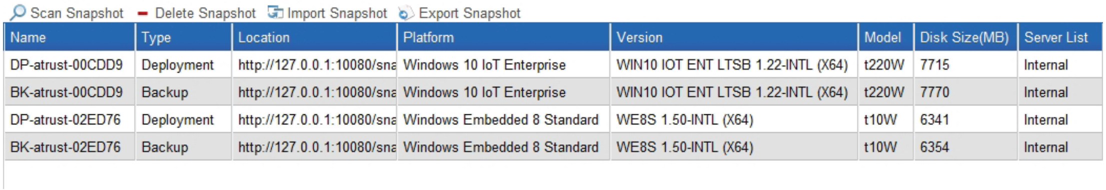
Password:

Confirm Password:

NOTE

- If you change the default password of the built-in administrator account for the target thin client and want to keep that new password in its snapshot, please check **Custom administrator password is used on thin client** and then provide the new password.

7. Provide the required information, choose the desired options, 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.



Name	Type	Location	Platform	Version	Model	Disk Size(MB)	Server List
DP-atrust-00CDD9	Deployment	http://127.0.0.1:10080/sna	Windows 10 IoT Enterprise	WIN10 IOT ENT LTSB 1.22-INTL (X64)	t220W	7715	Internal
BK-atrust-00CDD9	Backup	http://127.0.0.1:10080/sna	Windows 10 IoT Enterprise	WIN10 IOT ENT LTSB 1.22-INTL (X64)	t220W	7770	Internal
DP-atrust-02ED76	Deployment	http://127.0.0.1:10080/sna	Windows Embedded 8 Standard	WE8S 1.50-INTL (X64)	t10W	6341	Internal
BK-atrust-02ED76	Backup	http://127.0.0.1:10080/sna	Windows Embedded 8 Standard	WE8S 1.50-INTL (X64)	t10W	6354	Internal

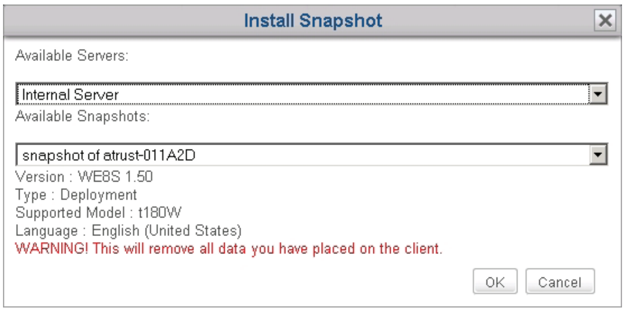
NOTE

- To access the Snapshot list, click **System** tab, and then click **Deployment** > **Snapshot**.
- Refer to section "3.2.8 Managing Client Snapshots" on page 35 for instructions on how to manage your snapshots.

3.4.27 Restoring Client Snapshots

To restore a system copy of a client, please do the following:

1. On **Thin Clients** tab, click **Thin Clients** to expand the Client Group tree, and then click the client group to which the desired client belongs.
2. The Client list appears.
3. Click to select the desired client, and then click **Command** on the top of the Client list.
4. The Command menu appears.
5. Click to select **Install Snapshot**.
6. The Install Snapshot window appears prompting you to select a server and snapshot.



Install Snapshot

Available Servers:

Internal Server

Available Snapshots:

snapshot of atrust-011A2D

Version : WE8S 1.50
Type : Deployment
Supported Model : t180W
Language : English (United States)
WARNING! This will remove all data you have placed on the client.

7. Click the drop-down menus to select the desired server and snapshot, and then click **OK** to confirm.
8. On the selected client, a warning message appears to notify the user of the planned reboot and allow the user to cancel the action if necessary.
9. After completion, the client is restored to the desired state.

3.4.28 Assisting a Client User Remotely

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

NOTE

- Atrust t50 doesn't support the **Shadow** feature.

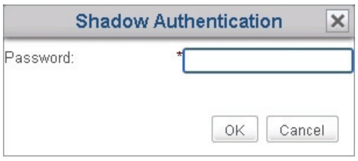
To remotely assist a client user, please do the following:

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 Shadow Authentication window appears prompting you for the Shadow password.

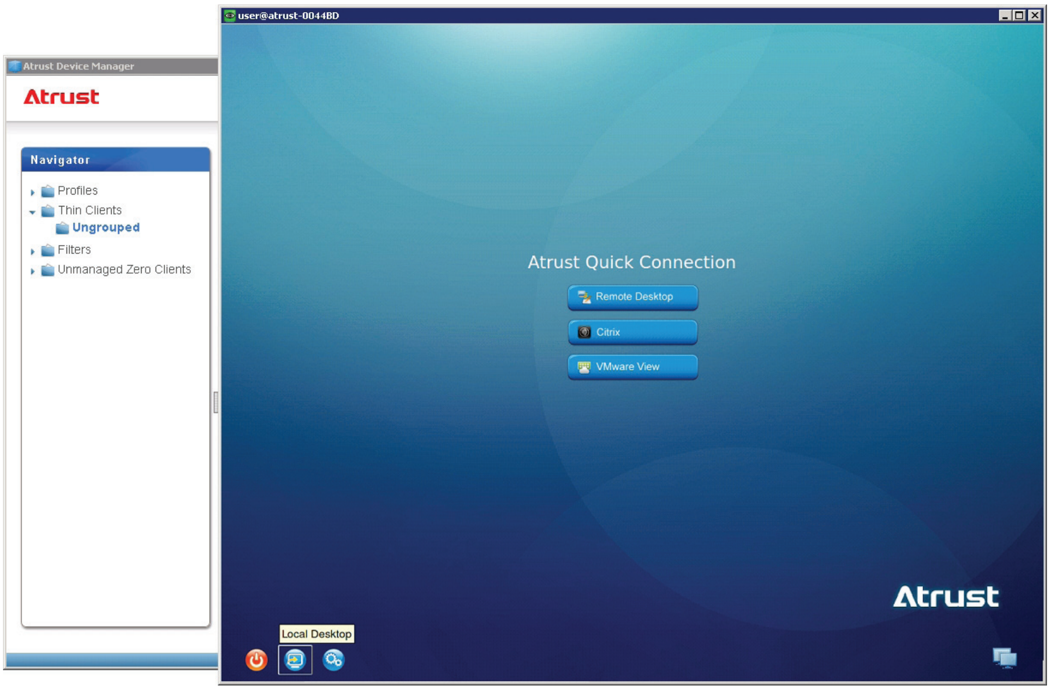


Shadow Authentication

Password: *

7. Type in your Shadow password, and then click **OK** to confirm.

8. A window pops up with the desktop screen of the selected client.



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

NOTE

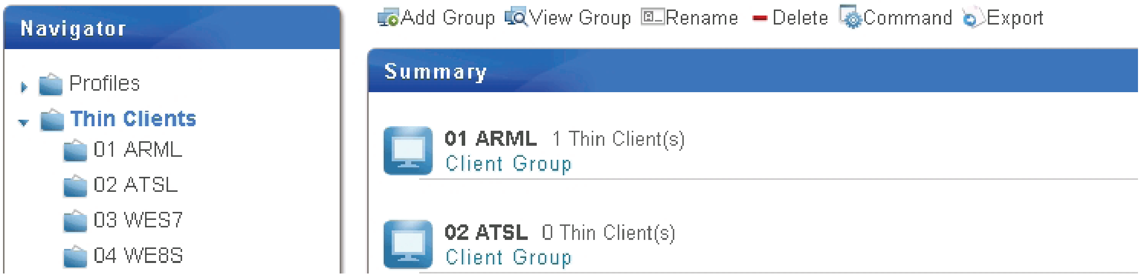
- The user of the client could also control the system with the local keyboard and mouse.

3.4.29 Exporting Client Data

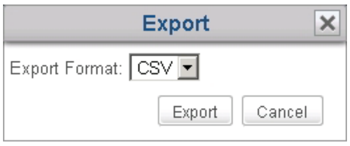
The **Export** feature available on the top of the Client Group list or the Client list allows you export an inventory of managed clients.

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

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

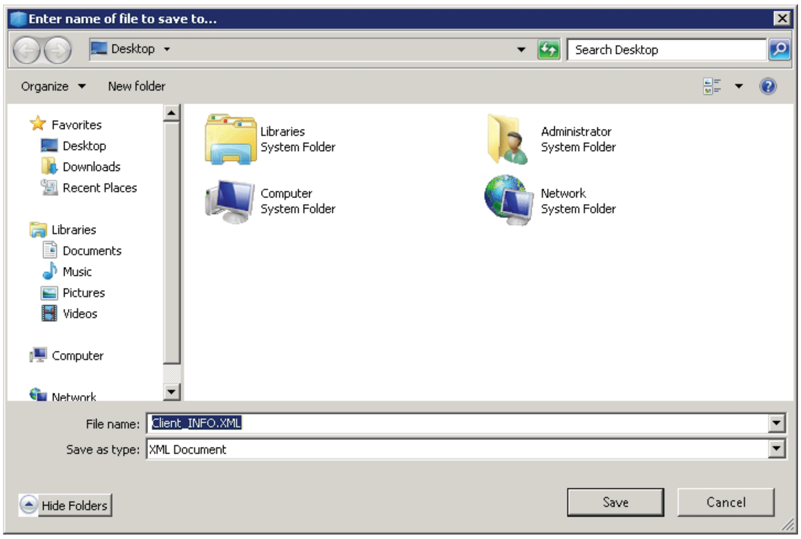


3. A window appears prompting you to select the Export format: **CSV** or **XML**.



Export Format: CSV

4. Click the drop-down menu to select the desired format, and then click **Export**.
5. On the opened window, click to select the desired option, and then click **Save** to confirm.



File name: Client_INFO.XML
Save as type: XML Document

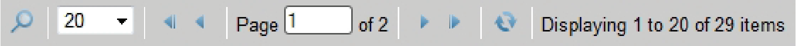
3.4.30 Digging Out Profiles, Clients, or Event Logs with Quick Search

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

> **NOTE**
>
> - Event logs will be introduced on section "3.5.1 Logs Tab Overview" on page 116.
> - You can also use filters to find out the desired clients within the managed clients. For details, please refer to section "3.4.31 Digging Out Clients with Filters" on page 113.

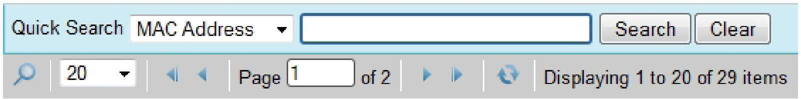
To dig out the desired profile, client, or event log on a Profile, Client, Zero Client, Event Log list, please do the following:

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 .



Displaying 1 to 20 of 29 items

4. The Quick Search bar appears.


Quick Search: MAC Address

Displaying 1 to 20 of 29 items

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.

3.4.31 Digging Out Clients with Filters

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

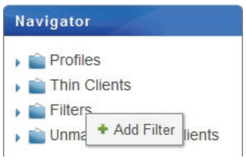
NOTE

- You can also use Quick Search to dig out clients within managed clients and unmanaged zero clients. For details, please refer to "3.4.30 Digging Out Profiles, Clients, or Event Logs with Quick Search" on page 112.

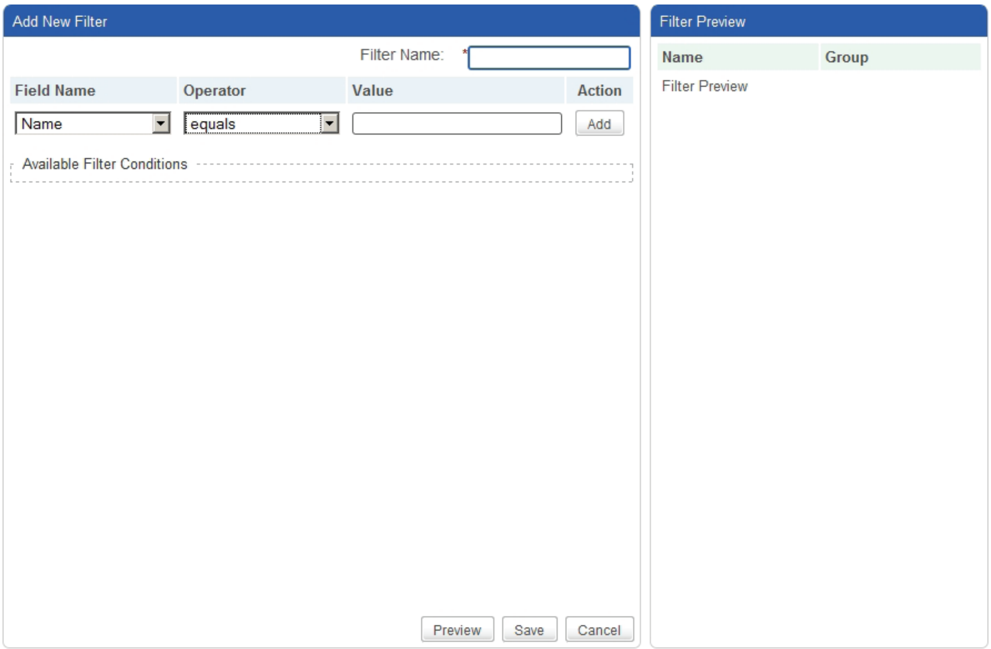
Adding a Filter

To add a filter, please do the following:

1. On **Thin Clients** tab, right click on the **Filters** in Navigation area.
2. A popup menu appears.



3. Click to select **Add Filter**.
4. The Add New Filter and Filter Preview panes appear in Management area.



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

NOTE

- Most information about a client, which can be used as filter conditions, are available in the Thin Client Information pane. To access Thin Client Information pane, please refer to section "3.4.20 Editing or Viewing the Basic Information about a Client" on page 91 for detailed instructions.

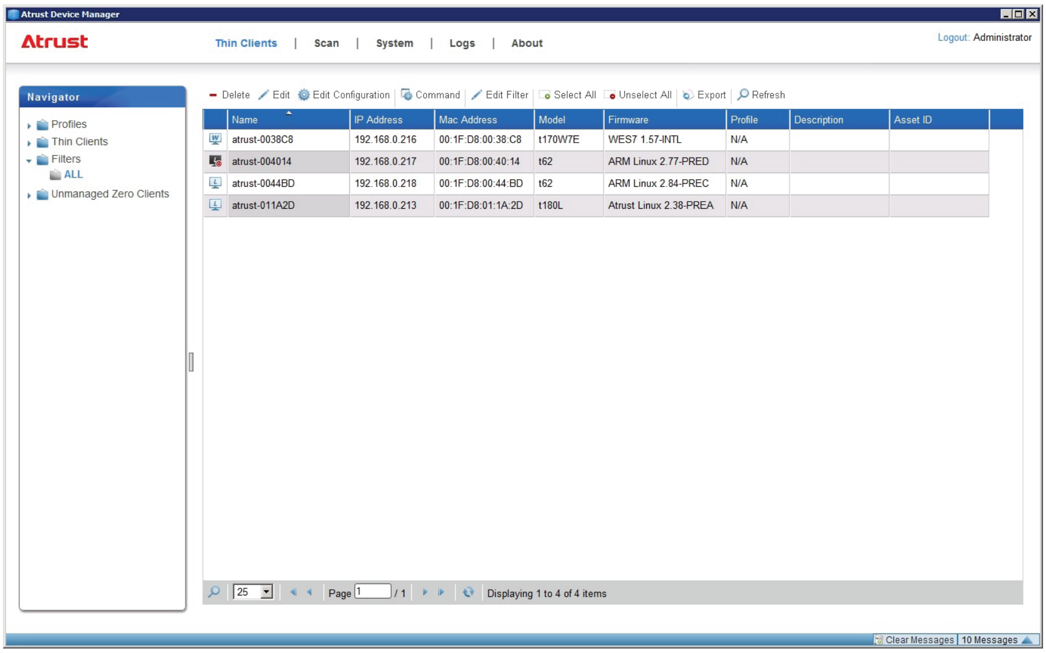
7. Click **Add** to add a condition to a filter.
8. Repeat steps 5 through 7 to add a new condition.
9. Click **Preview** to view the result of a filter. The result is displayed in the Filter Preview pane.
10. Click **Save** to create the filter.

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.



Name	IP Address	Mac Address	Model	Firmware	Profile	Description	Asset ID
atrust-0038C8	192.168.0.216	00:1F:D8:00:38:C8	t170W7E	WES7 1.57-INTL	N/A		
atrust-004014	192.168.0.217	00:1F:D8:00:40:14	t62	ARM Linux 2.77-PRED	N/A		
atrust-0044BD	192.168.0.218	00:1F:D8:00:44:BD	t62	ARM Linux 2.84-PREC	N/A		
atrust-011A2D	192.168.0.213	00:1F:D8:01:1A:2D	t180L	Atrust Linux 2.38-PREA	N/A		

25

Displaying 1 to 4 of 4 items

TIP

- You can then manage clients directly through the Client list.

3.4.32 Managing Your Filters

Deleting a Filter

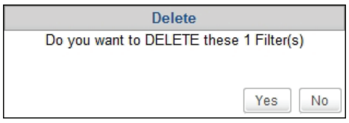
To delete a filter, please do the following:

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

NOTE

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

4. The Delete window appears prompting for confirmation.



Delete

Do you want to DELETE these 1 Filter(s)

5. Click **Yes** to confirm.

Adjusting a Filter

To adjust a filter, please do the following:

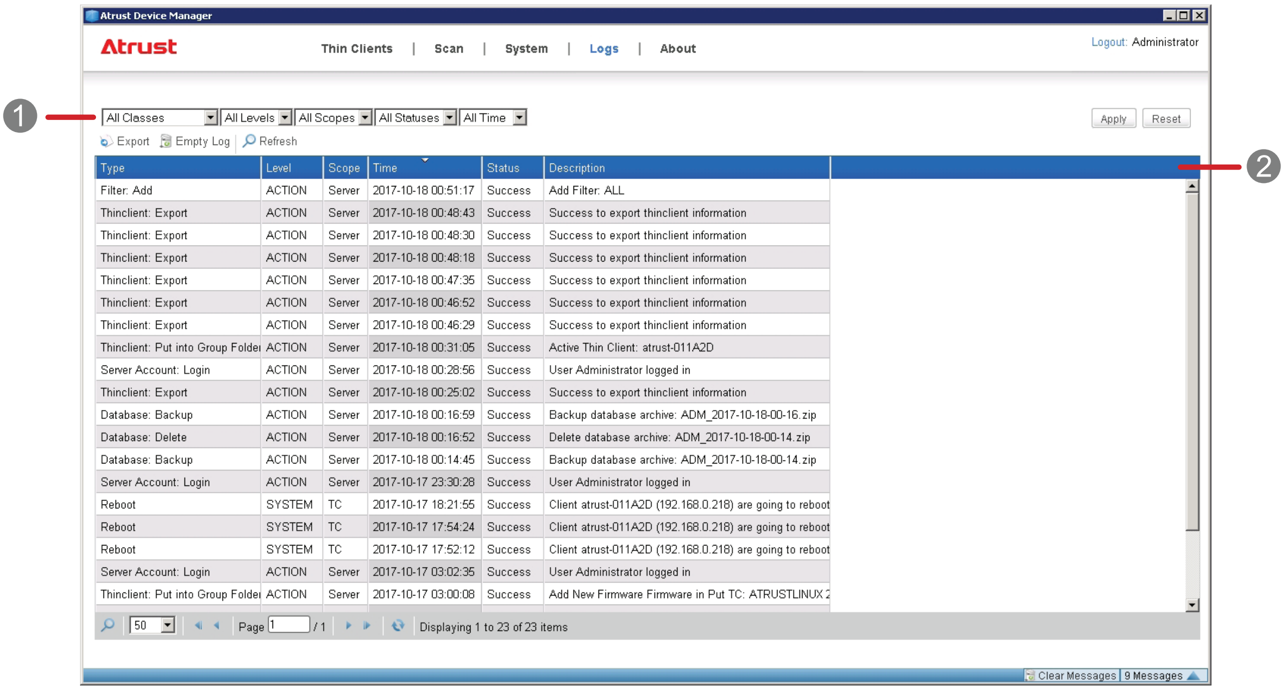
1. On **Thin Clients** tab, click **Filters** in Navigation area.
2. The Filter list appears in Management area.
3. Click to select the desired filter, and then click **Edit** on the top of the Filter list.
4. The Filter Condition List and Filter Preview panes appear in Management area.
5. Adjust conditions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



Type	Level	Scope	Time	Status	Description
Filter: Add	ACTION	Server	2017-10-18 00:51:17	Success	Add Filter: ALL
Thinclient: Export	ACTION	Server	2017-10-18 00:48:43	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:48:30	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:48:18	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:47:35	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:46:52	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:46:29	Success	Success to export thinclient information
Thinclient: Put into Group Folde	ACTION	Server	2017-10-18 00:31:05	Success	Active Thin Client: atrust-011A2D
Server Account: Login	ACTION	Server	2017-10-18 00:28:56	Success	User Administrator logged in
Thinclient: Export	ACTION	Server	2017-10-18 00:25:02	Success	Success to export thinclient information
Database: Backup	ACTION	Server	2017-10-18 00:16:59	Success	Backup database archive: ADM_2017-10-18-00-16.zip
Database: Delete	ACTION	Server	2017-10-18 00:16:52	Success	Delete database archive: ADM_2017-10-18-00-14.zip
Database: Backup	ACTION	Server	2017-10-18 00:14:45	Success	Backup database archive: ADM_2017-10-18-00-14.zip
Server Account: Login	ACTION	Server	2017-10-17 23:30:28	Success	User Administrator logged in
Reboot	SYSTEM	TC	2017-10-17 18:21:55	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Reboot	SYSTEM	TC	2017-10-17 17:54:24	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Reboot	SYSTEM	TC	2017-10-17 17:52:12	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Server Account: Login	ACTION	Server	2017-10-17 03:02:35	Success	User Administrator logged in
Thinclient: Put into Group Folde	ACTION	Server	2017-10-17 03:00:08	Success	Add New Firmware Firmware in Put TC: ATRUSTLINUX 2

Displaying 1 to 23 of 23 items

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.

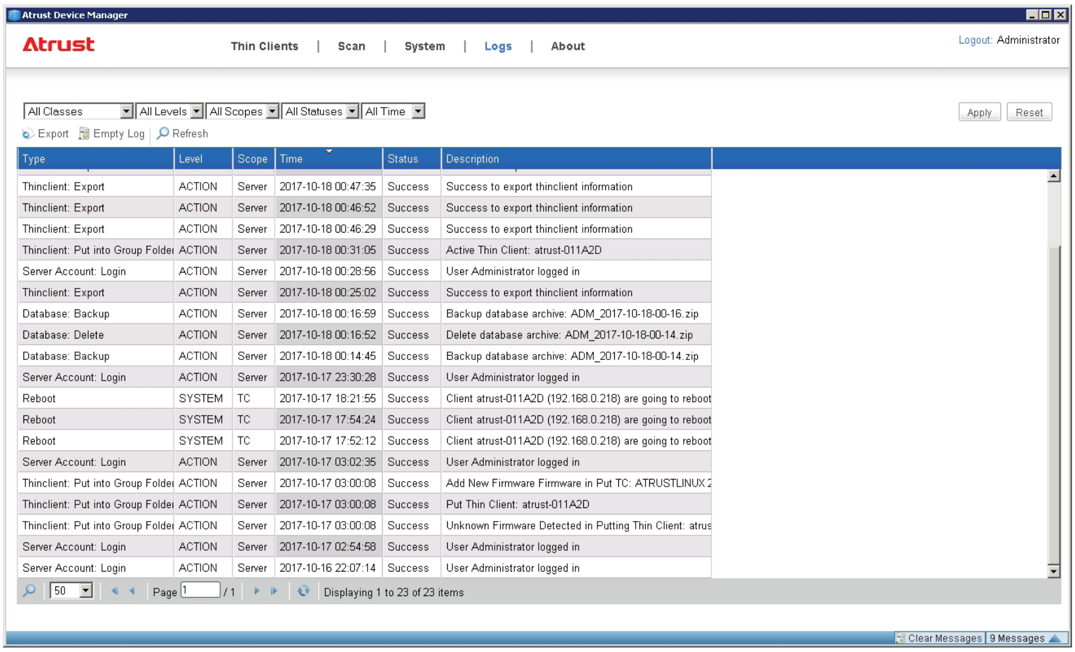
3.5.2 Available Tasks at a Glance

No.	Available Task	Section	Page
1	Viewing your event logs	3.5.3	117
2	Exporting your event logs	3.5.4	118
3	Emptying your event logs	3.5.5	118

3.5.3 Viewing Event Logs

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

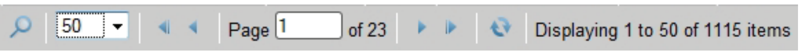
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.



Type	Level	Scope	Time	Status	Description
Thinclient: Export	ACTION	Server	2017-10-18 00:47:35	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:46:52	Success	Success to export thinclient information
Thinclient: Export	ACTION	Server	2017-10-18 00:46:29	Success	Success to export thinclient information
Thinclient: Put into Group Folder	ACTION	Server	2017-10-18 00:31:05	Success	Active Thin Client: atrust-011A2D
Server Account: Login	ACTION	Server	2017-10-18 00:28:56	Success	User Administrator logged in
Thinclient: Export	ACTION	Server	2017-10-18 00:25:02	Success	Success to export thinclient information
Database: Backup	ACTION	Server	2017-10-18 00:16:59	Success	Backup database archive: ADM_2017-10-18-00-16.zip
Database: Delete	ACTION	Server	2017-10-18 00:16:52	Success	Delete database archive: ADM_2017-10-18-00-14.zip
Database: Backup	ACTION	Server	2017-10-18 00:14:45	Success	Backup database archive: ADM_2017-10-18-00-14.zip
Server Account: Login	ACTION	Server	2017-10-17 23:30:28	Success	User Administrator logged in
Reboot	SYSTEM	TC	2017-10-17 18:21:55	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Reboot	SYSTEM	TC	2017-10-17 17:54:24	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Reboot	SYSTEM	TC	2017-10-17 17:52:12	Success	Client atrust-011A2D (192.168.0.218) are going to reboot
Server Account: Login	ACTION	Server	2017-10-17 03:02:35	Success	User Administrator logged in
Thinclient: Put into Group Folder	ACTION	Server	2017-10-17 03:00:08	Success	Add New Firmware Firmware in Put TC: ATRUSTLINUX 2
Thinclient: Put into Group Folder	ACTION	Server	2017-10-17 03:00:08	Success	Put Thin Client: atrust-011A2D
Thinclient: Put into Group Folder	ACTION	Server	2017-10-17 03:00:08	Success	Unknown Firmware Detected in Putting Thin Client: atrus
Server Account: Login	ACTION	Server	2017-10-17 02:54:58	Success	User Administrator logged in
Server Account: Login	ACTION	Server	2017-10-16 22:07:14	Success	User Administrator logged in

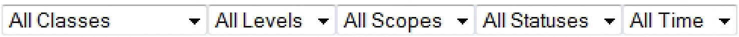
50 Page 1 / 1 Displaying 1 to 23 of 23 items

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



Displaying 1 to 50 of 1115 items

- 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:

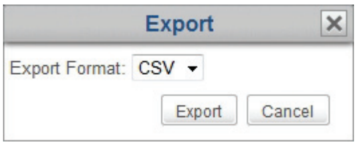
1. On Atrust Device Manager, click **Logs** tab.
2. The Log list appears.

- 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.



Export Format: CSV

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

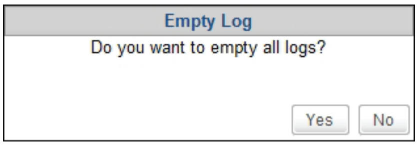
- You cannot partially delete log entries.

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.



Empty Log

Do you want to empty all logs?

5. Click **Yes** to confirm.
6. All log entries are deleted from Atrust Device Manager.

NOTE

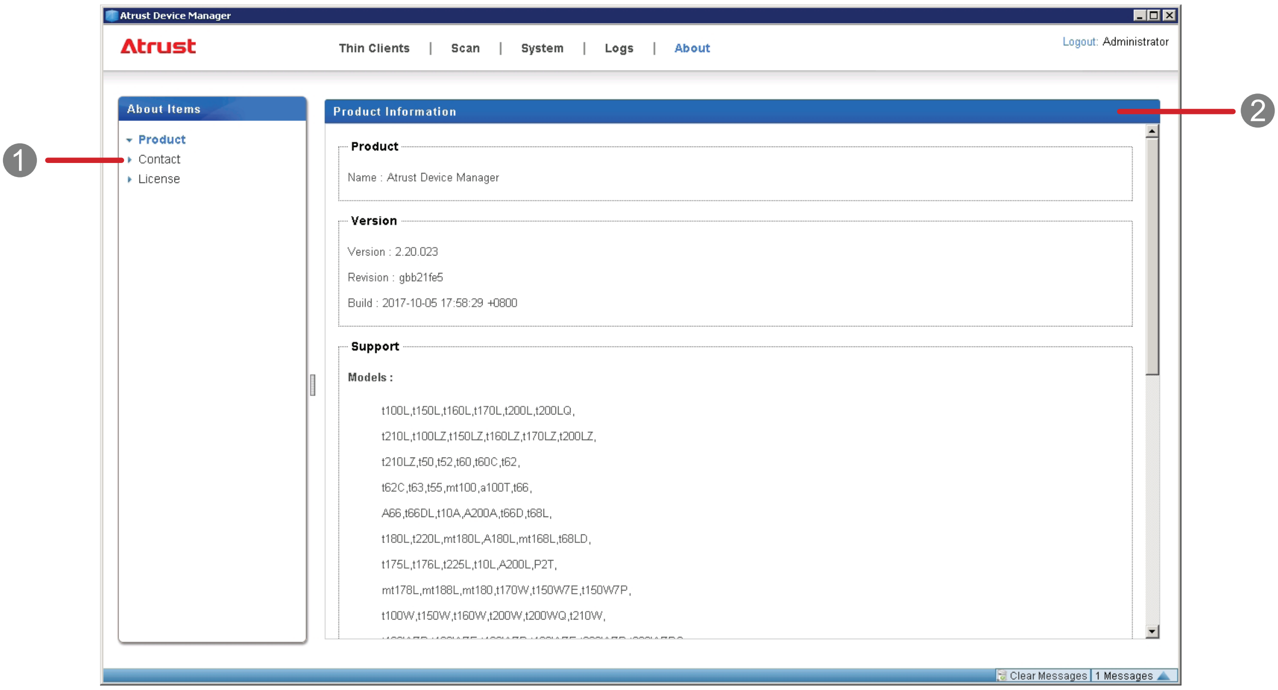
- A new log entry about emptying log will be added to the Log list.

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



Product

Name : Atrust Device Manager

Version

Version : 2.20.023

Revision : gbb21fe5

Build : 2017-10-05 17:58:29 +0800

Support

Models :

t100L,t150L,t160L,t170L,t200L,t200LQ,

t210L,t100LZ,t150LZ,t160LZ,t170LZ,t200LZ,

t210LZ,t50,t52,t60,t60C,t62,

t62C,t63,t55,mt100,a100T,t66,

A66,t66DL,t10A,A200A,t66D,t68L,

t180L,t220L,mt180L,A180L,mt168L,t68LD,

t175L,t176L,t225L,t10L,A200L,P2T,

mt178L,mt188L,mt180,t170W,t150W7E,t150W7P,

t100W,t150W,t160W,t200W,t200WQ,t210W,

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	121
2	Viewing Atrust contact information	3.6.4	121
3	Viewing Atrust Software License Agreement	3.6.5	121

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

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 all-in-one, mobile, t-series thin / zero clients can meet a wide range of desktop virtualization forms and needs. To get your client device ready for use in your IT infrastructure, you might need to customize client settings to meet the specific needs in your desktop virtualization plan.

4.2 Client Settings at a Glance

The following table provides brief descriptions of client setting items.

NOTE

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

Tab	Setting	Icon	Description
Applications	Remote Desktop		Click to configure RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for Remote Desktop sessions.
	Citrix ICA		Click to configure Citrix ICA (Independent Computing Architecture) connection settings and create shortcuts on the local desktop and START menu for ICA sessions.
	Citrix XenApp		Click to configure Citrix XenApp connection settings and create a Start menu folder and/or desktop folder for accessing application delivery services.
	VMware View		Click to configure VMware View connection settings and create shortcuts on the local desktop and START menu for View sessions.
	GO-Global		Click to configure GO-Global Client connection settings and create shortcuts on the local desktop and START menu for accessing application delivery services.
	Web Browser		Click to configure general (for Windows Embedded-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 shortcuts on the local desktop and START menu for SSH sessions.
	Parallels 2X Client	Parallels	Click to configure RAS (Remote Application Server) / RDP (Remote Desktop Protocol) connection settings and create shortcuts on the local desktop and START menu for RAS / RDP sessions.
	XDMCP		Click to configure XDMCP (X Display Manager Control Protocol) connection settings and create shortcuts on the local desktop and START menu 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 device.
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.
	Host Name *		Click to change the host name of your client device.
	Wireless *		Click to configure your wireless network settings and create a wireless connection.
	Proxy		Click to configure proxy settings for Web-based access to services. The settings available here are only applicable to services that use Web-based access, such as (Microsoft) Remote Web Access and (Citrix) Web Logon connection types.

Tab	Setting	Icon	Description
System	Time and Date (Time Zone)	7	Click to configure date and time settings.
	Password		Click to configure your password settings.
	Firmware Update *		Click to update firmware through the network. This feature is only applicable when this client is managed by the Atrust Device Manager console.
	Snapshot		Click to take a snapshot (system copy at a specific point of time) for your client device, which you can use for mass deployment, system backup, and recovery.
	Appliance Mode		Click to enable/disable the Appliance mode to allow/disallow the automatic RDP / ICA / View session. In Appliance mode, the client starts up with the desired RDP / ICA / View session and shuts down when the user logs out (also see NOTE below).
	Auto Setup		Click to enable Auto Setup to allow the client to get its preset configuration on startup and enter the desired user environment automatically.
	Quick Connection		Click to enable/disable the Quick Connection mode after system startup.
	Miscellaneous		Click to change the host name of your client device.
	Terminal	>_	Click to enable/disable the execution of the text-based (command-line) functions.
	FBWF		Click to configure FBWF (File-Based Write Filter) settings. As a file-based write filter, FBWF will intercept all write attempts to a protected volume and redirect those attempts to a RAM cache. After restart, all changes are discarded.
	UWF		Click to configure UWF (Unified Write Filter) settings. As a sector-based write filter, UWF will intercept all write attempts to a protected volume and redirect those attempts to a RAM cache. All system changes only affect the session where the changes are made. After restart, all changes are discarded.
	Error Report	!	Click to collect event logs and launch the screen capturing program for error reporting.
	Certificate Manager		Click to import or manage certificates for remote computers.
	Advanced		Click to configure advanced settings such as Auto Registration.
	System Information	i	Click to view detailed system, network, and license (only for P2T thin clients) information.

NOTE

- Appliance mode might allow more options when the user logs out, depending on the firmware version of your thin client.

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

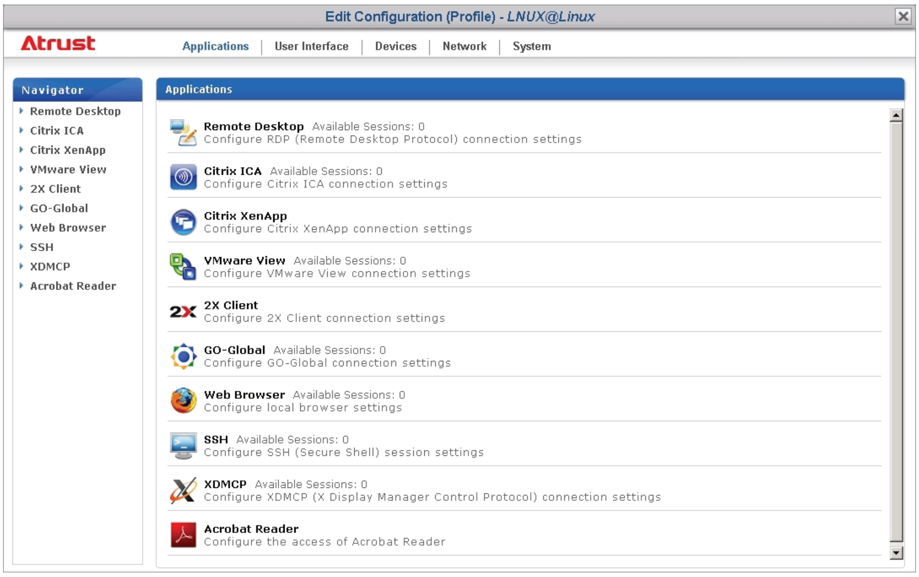
- In this section, we will focus on the editing or adjusting of a profile (group configuration) in greater detail. For general instructions on how to create a profile (group configuration) or on how to open the Edit Configuration window for profile, please refer to section "3.4.12 Creating Client Setting Profiles" on page 73.
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 69.
- 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 132.

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.

Example: Edit Configuration (Profile) Window

Linux-based: All



Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

Citrix XenApp
Configure Citrix XenApp connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

2X Client
Configure 2X Client connection settings

GO-Global Available Sessions: 0
Configure GO-Global connection settings

Web Browser Available Sessions: 0
Configure local browser settings

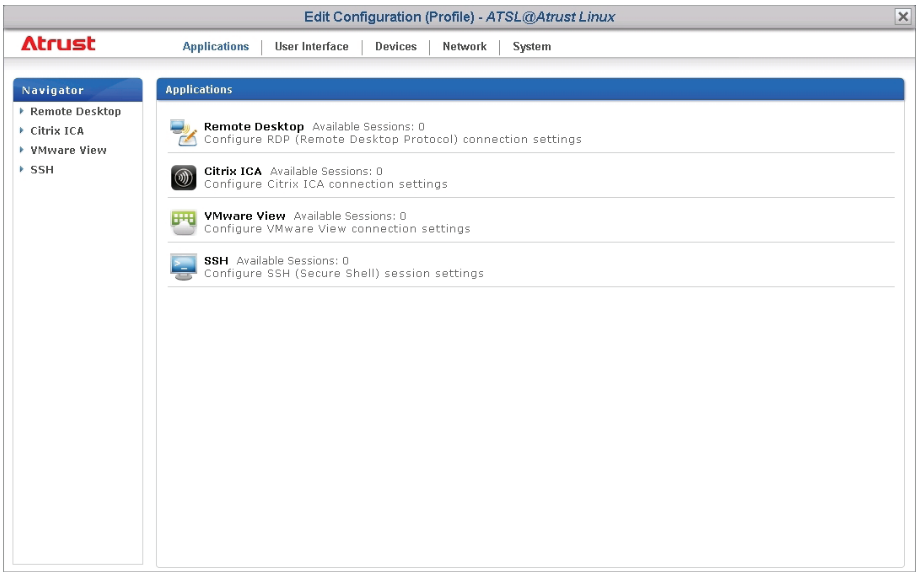
SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

XDMCP Available Sessions: 0
Configure XDMCP (X Display Manager Control Protocol) connection settings

Acrobat Reader
Configure the access of Acrobat Reader

Example: Edit Configuration (Profile) Window

Atrust Linux-based t68L / t68LD / t180L / t220L



Edit Configuration (Profile) - *ATSL@Atrust Linux*

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

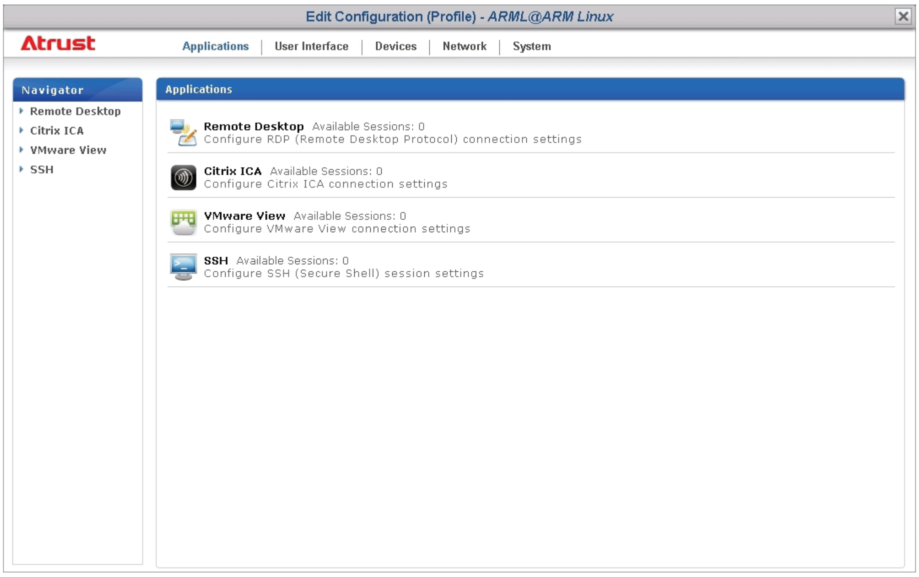
Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

Example: Edit Configuration (Profile) Window

ARM Linux-based t60 / t62 / t63 / a100T



Edit Configuration (Profile) - *ARML@ARM Linux*

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

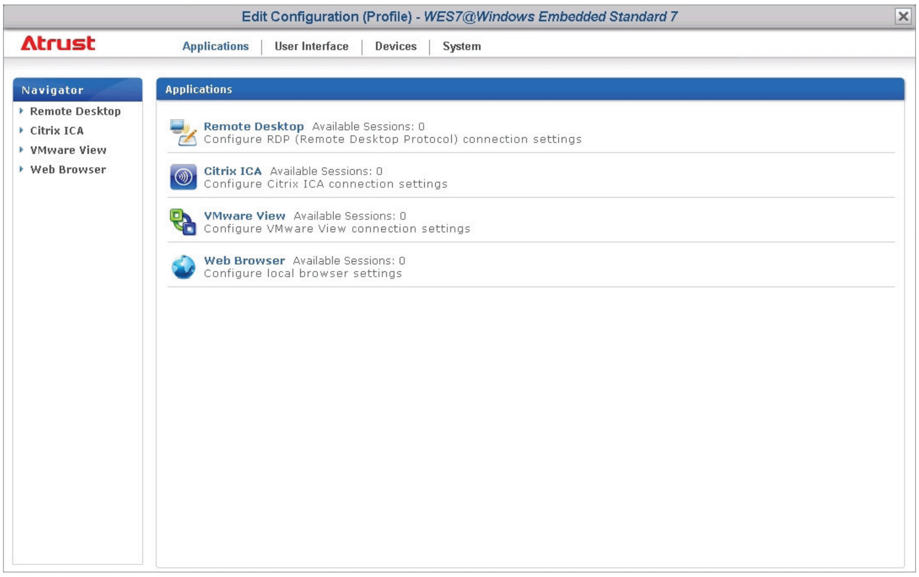
Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

Example: Edit Configuration (Profile) Window

Windows Embedded-based (Windows Embedded Standard 7) t160W7 / t170W7 / t200W7 / t210W7



Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

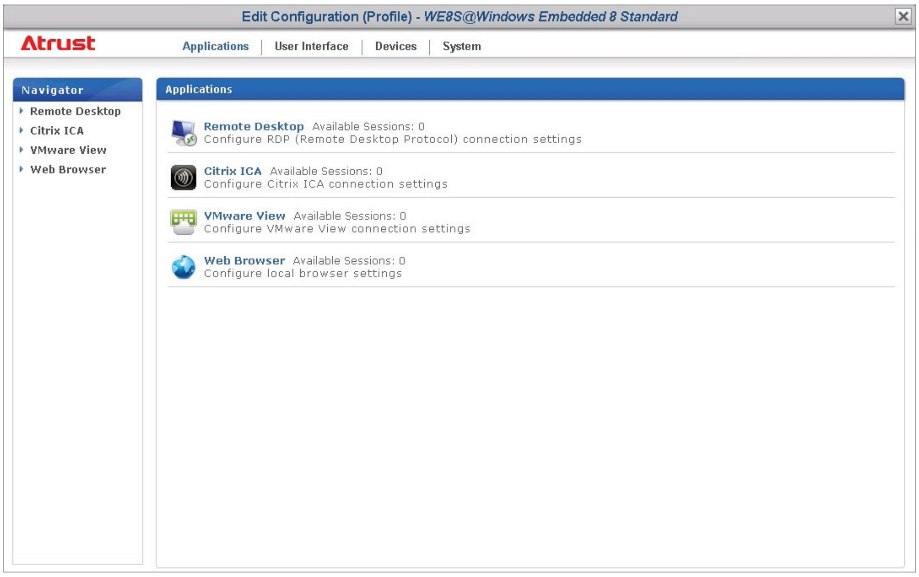
Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

Web Browser Available Sessions: 0
Configure local browser settings

Example: Edit Configuration (Profile) Window

Windows Embedded-based (Windows Embedded 8 Standard) t68W / mt168W / mt180W / t180W / t220W / A180W



Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

Web Browser Available Sessions: 0
Configure local browser settings

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 activate the item.

NOTE

- The gray globe icon will become blue 🌐 when you click to activate the item.
- 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.

NOTE

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

4.4 Editing or Adjusting an Individual Configuration

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

NOTE

- In this section, we will focus on the editing/adjusting of an individual configuration in greater detail. For general instructions on how to create an individual configuration or on how to open the Edit Configuration window for a client, please refer to section "3.4.14 Using Individualized Client Settings" on page 79.

NOTE

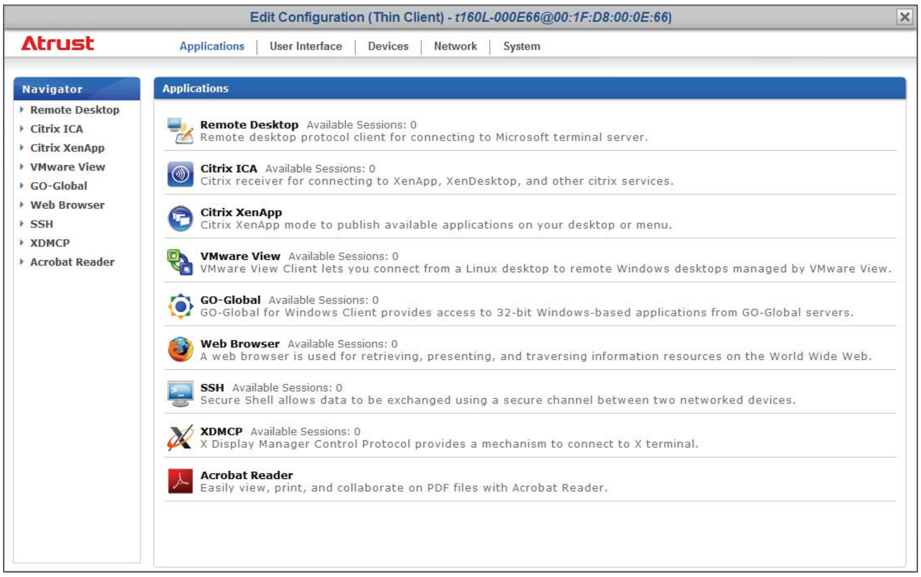
- To have a basic understanding of client configuration, please refer to section "3.4.9 Client Settings" on page 69.
- Please note that, although the Edit Configuration window for a profile (group configuration) looks almost the same as the Edit Configuration window for a client (individual configuration), 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.

Example: Edit Configuration (Thin Client) Window

Linux-based: t160L


Edit Configuration (Thin Client) - t160L-000E66@00:1F:D8:00:0E:66)
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Remote Desktop
Citrix ICA
Citrix XenApp
VMware View
GO-Global
Web Browser
SSH
XDMCP
Acrobat Reader
Applications

Remote Desktop Available Sessions: 0
Remote desktop protocol client for connecting to Microsoft terminal server.

Citrix ICA Available Sessions: 0
Citrix receiver for connecting to XenApp, XenDesktop, and other citrix services.

Citrix XenApp
Citrix XenApp mode to publish available applications on your desktop or menu.

VMware View Available Sessions: 0
VMware View Client lets you connect from a Linux desktop to remote Windows desktops managed by VMware View.

GO-Global Available Sessions: 0
GO-Global for Windows Client provides access to 32-bit Windows-based applications from GO-Global servers.

Web Browser Available Sessions: 0
A web browser is used for retrieving, presenting, and traversing information resources on the World Wide Web.

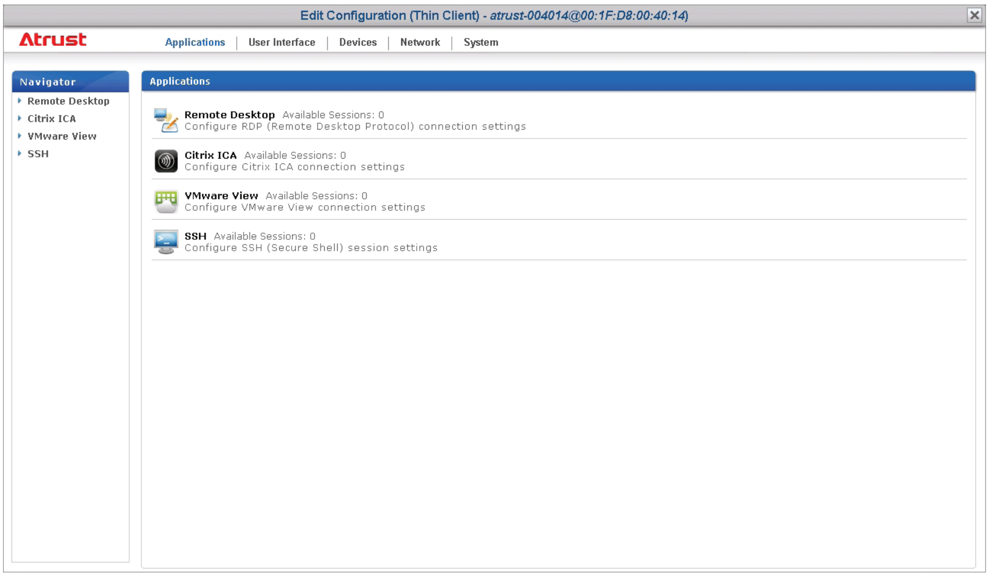
SSH Available Sessions: 0
Secure Shell allows data to be exchanged using a secure channel between two networked devices.

XDMCP Available Sessions: 0
X Display Manager Control Protocol provides a mechanism to connect to X terminal.

Acrobat Reader
Easily view, print, and collaborate on PDF files with Acrobat Reader.

Example: Edit Configuration (Thin Client) Window

ARM Linux-based: t62


Edit Configuration (Thin Client) - atrust-004014@00:1F:D8:00:40:14)
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Remote Desktop
Citrix ICA
VMware View
SSH
Applications

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

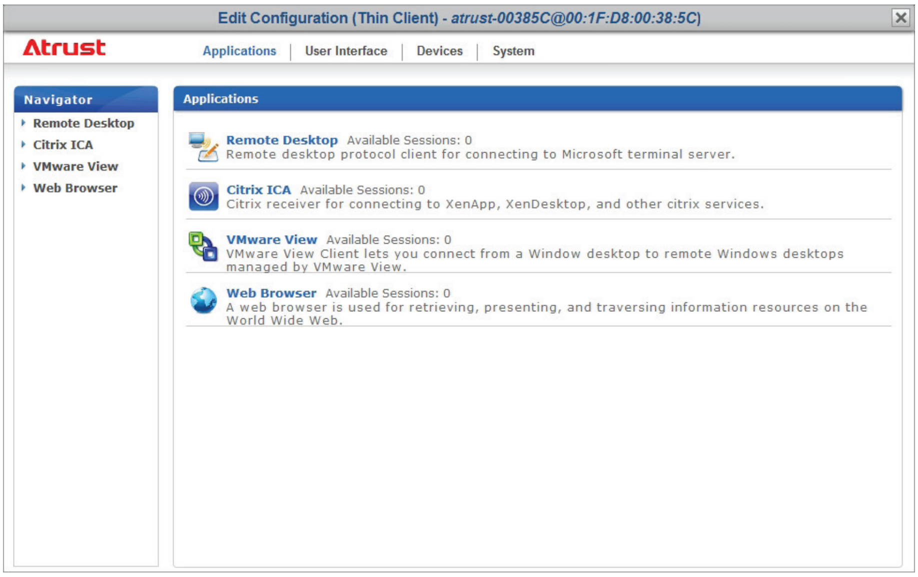
Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

Example: Edit Configuration (Thin Client) Window

Windows Embedded-based: t170


Edit Configuration (Thin Client) - atrust-00385C@00:1F:D8:00:38:5C)
Atrust
Applications | User Interface | Devices | System
Navigator
Remote Desktop
Citrix ICA
VMware View
Web Browser
Applications

Remote Desktop Available Sessions: 0
Remote desktop protocol client for connecting to Microsoft terminal server.

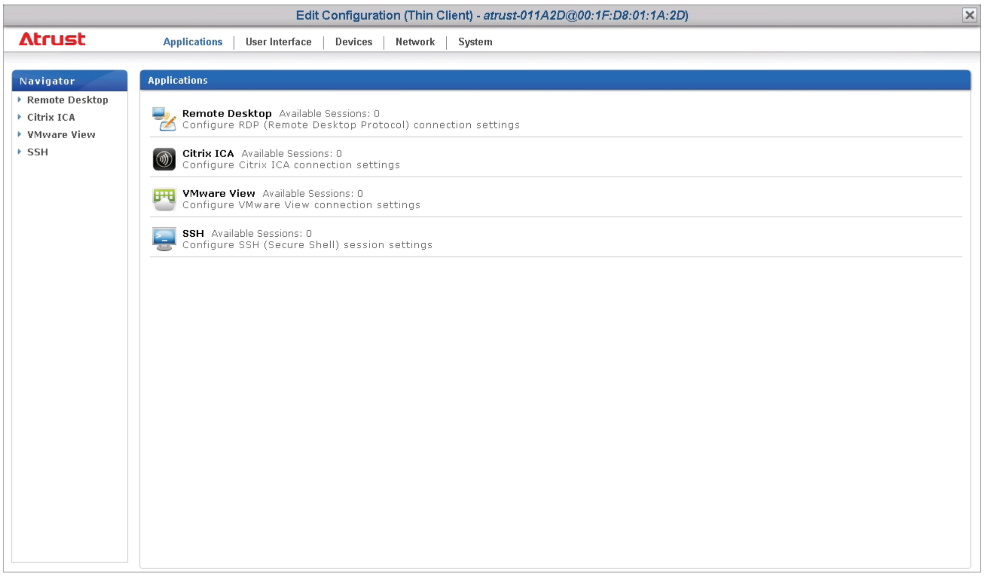
Citrix ICA Available Sessions: 0
Citrix receiver for connecting to XenApp, XenDesktop, and other citrix services.

VMware View Available Sessions: 0
VMware View Client lets you connect from a Window desktop to remote Windows desktops managed by VMware View.

Web Browser Available Sessions: 0
A web browser is used for retrieving, presenting, and traversing information resources on the World Wide Web.

Example: Edit Configuration (Thin Client) Window

Atrust Linux-based: t180L


Edit Configuration (Thin Client) - atrust-011A2D@00:1F:D8:01:1A:2D)
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Remote Desktop
Citrix ICA
VMware View
SSH
Applications

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

2. Click on the icon of the desired setting.
3. Click **Add** to add up an entry for that setting if necessary.
4. On the detailed setting page(s), choose or type in the desired setting values.

NOTE

- Click on the gray lock 🔓 icon located close to a setting item to lock its value. The gray lock will become orange 🔒 and secured. When a lock icon becomes orange and secured, the corresponding setting value is locked on the client and cannot be changed locally through Atrust Client Setup.
- If the lock icon of a setting value is blue 🔒, this setting value comes from the group configuration (profile). You can only change the value by modifying / removing the group configuration (profile) or applying a new one.
- If you apply a group configuration to a client, all related settings will also be shown in the Edit Configuration window for that client.

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

NOTE

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

4.5 Configuring Client Settings with Atrust Client Setup

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

NOTE

- For the list of client settings only locally accessible on clients, please refer to section “4.2 Client Settings at a Glance” on page 125.
- To have a basic understanding of client configuration, please refer to section “3.4.9 Client Settings” on page 69.

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

Appendices

A.1 Using a Custom Wallpaper on Clients via Atrust Device Manager

The Scenario where Applicable

This appendix provides instructions on how to use a custom wallpaper on thin clients via Atrust Device Manager.

Atrust Device Manager: v2.20.xxx / v2.08.041 or later.

NOTE

- Please note thin clients may need new firmware to support the custom wallpaper.

Getting Wallpaper Images Files Ready for Use

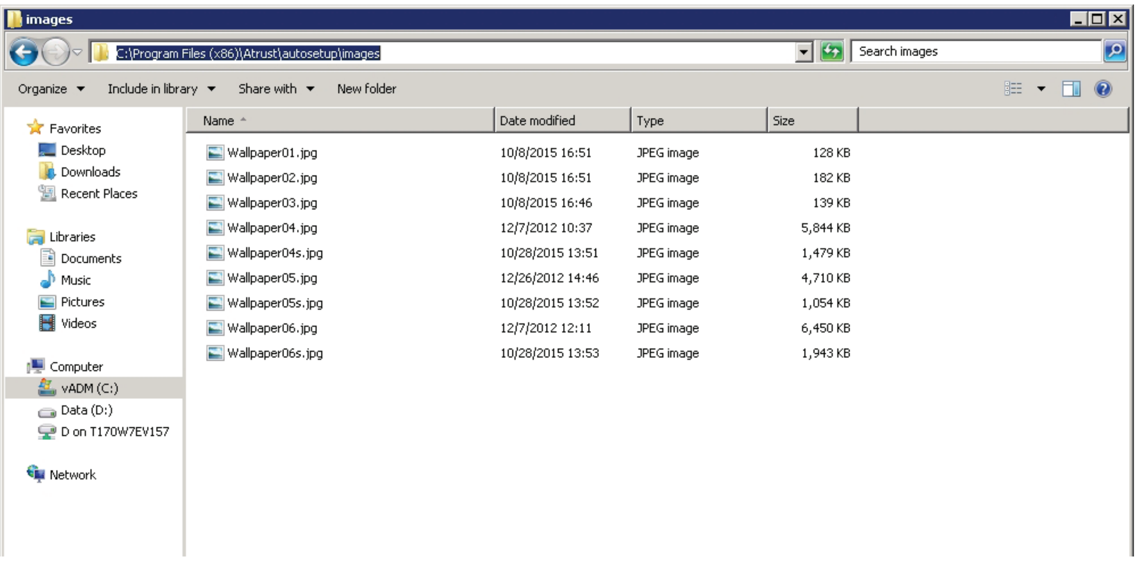
Please do the following to get wallpaper image files ready for use:

1. On the computer where Atrust Device Manager is installed, find the path: **C:\\Program Files (x86)\Atrust\autosetup\images**.

NOTE

- This is the default path. It might be different if you choose another path while installing Atrust Device Manager.

2. Put your wallpaper images under this path.



Name	Date modified	Type	Size
Wallpaper01.jpg	10/8/2015 16:51	JPEG image	128 KB
Wallpaper02.jpg	10/8/2015 16:51	JPEG image	182 KB
Wallpaper03.jpg	10/8/2015 16:46	JPEG image	139 KB
Wallpaper04.jpg	12/7/2012 10:37	JPEG image	5,844 KB
Wallpaper04s.jpg	10/28/2015 13:51	JPEG image	1,479 KB
Wallpaper05.jpg	12/26/2012 14:46	JPEG image	4,710 KB
Wallpaper05s.jpg	10/28/2015 13:52	JPEG image	1,054 KB
Wallpaper06.jpg	12/7/2012 12:11	JPEG image	6,450 KB
Wallpaper06s.jpg	10/28/2015 13:53	JPEG image	1,943 KB

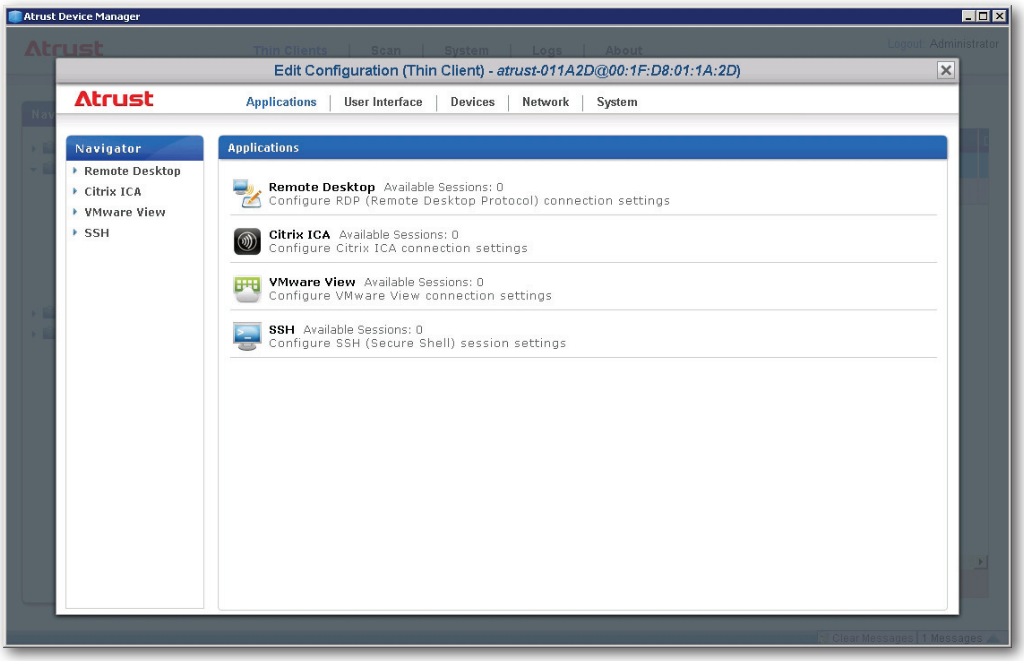
NOTE

- **Supported Wallpaper Formats:** JPG, JPEG, BMP, and PNG.
- **Wallpaper Size Limit:** 5 MB.

Enabling the Custom Wallpaper

To enable the custom wallpaper for your thin clients via Atrust Device Manager, please do the following:

1. Launch Atrust Device Manager.
2. 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.
3. The Client list appears in Management area.
4. Click to select the desired client, and then click **Edit Configuration**. The Edit Configuration window for that client appears.


Atrust Device Manager
Edit Configuration (Thin Client) - *atrust-011A2D@00:1F:D8:01:1A:2D)*
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Remote Desktop
Citrix ICA
VMware View
SSH
Applications

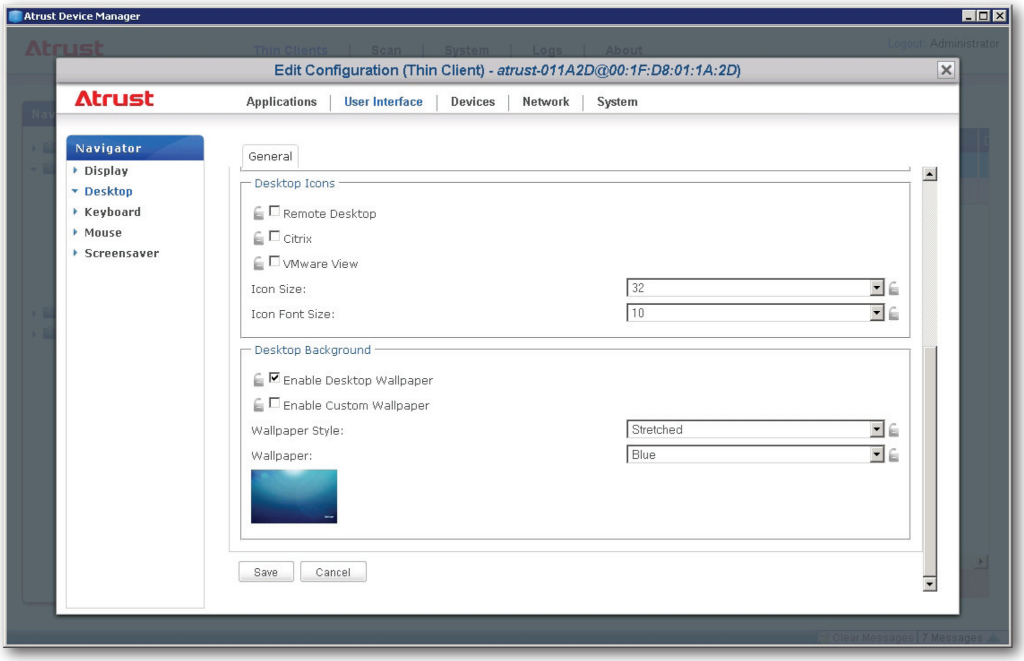
Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

5. Click **User Interface** > **Desktop**, and then scroll down to find the Desktop Background section.


Atrust Device Manager
Edit Configuration (Thin Client) - *atrust-011A2D@00:1F:D8:01:1A:2D)*
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Display
Desktop
Keyboard
Mouse
Screensaver
General
Save
Cancel

Desktop Icons

□ Remote Desktop

□ Citrix

□ VMware View

Icon Size: 32

Icon Font Size: 10

Desktop Background

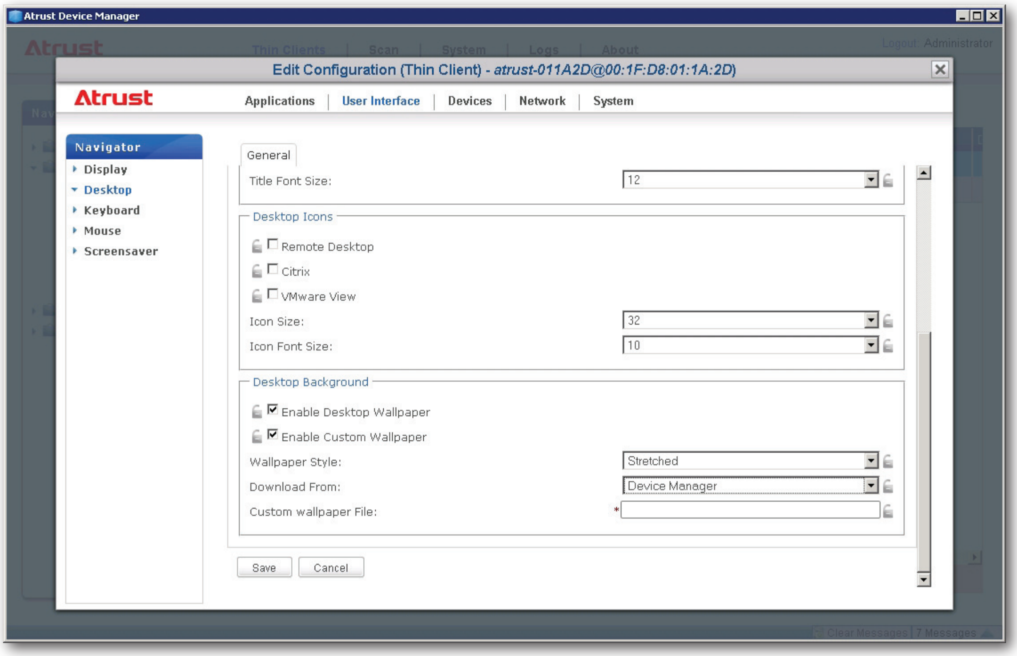
☑ Enable Desktop Wallpaper

□ Enable Custom Wallpaper

Wallpaper Style: Stretched

Wallpaper: Blue

6. Check **Enable Custom Wallpaper**, and then select **Device Manager** to get the wallpaper image file from Atrust Device Manager.


Atrust Device Manager
Edit Configuration (Thin Client) - atrust-011A2D@00:1F:D8:01:1A:2D)
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Display
Desktop
Keyboard
Mouse
Screensaver
General
Save
Cancel

Title Font Size: 12

Desktop Icons

☐ Remote Desktop

☐ Citrix

☐ VMware View

Icon Size: 32

Icon Font Size: 10

Desktop Background

☑ Enable Desktop Wallpaper

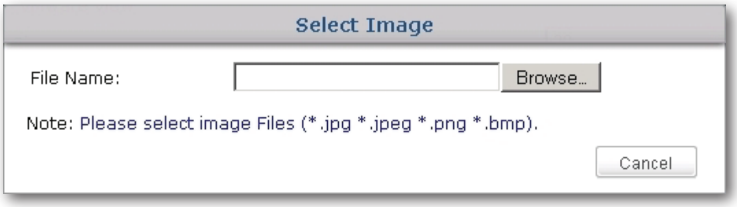
☑ Enable Custom Wallpaper

Wallpaper Style: Stretched

Download From: Device Manager

Custom wallpaper File: *

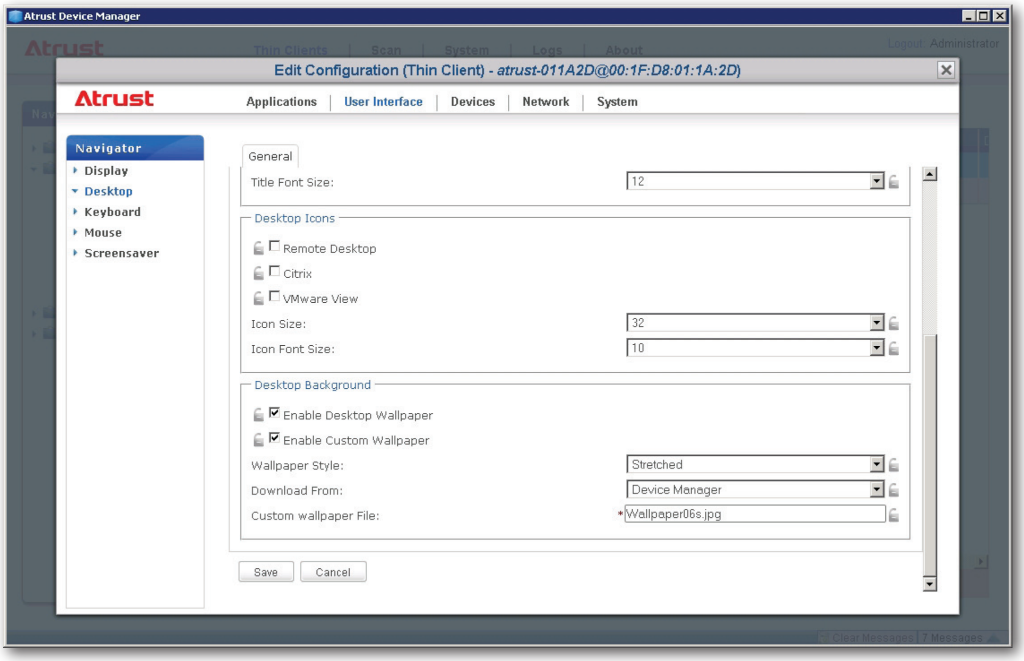
7. Click the Custom Wallpaper File field. On the opened window, click **Browse** to locate and select the desired wallpaper.



File Name:

Note: Please select image Files (*.jpg *.jpeg *.png *.bmp).

8. The file name of the selected image file appears in that field.


Atrust Device Manager
Edit Configuration (Thin Client) - atrust-011A2D@00:1F:D8:01:1A:2D)
Atrust
Applications | User Interface | Devices | Network | System
Navigator
Display
Desktop
Keyboard
Mouse
Screensaver
General
Save
Cancel

Title Font Size: 12

Desktop Icons

☐ Remote Desktop

☐ Citrix

☐ VMware View

Icon Size: 32

Icon Font Size: 10

Desktop Background

☑ Enable Desktop Wallpaper

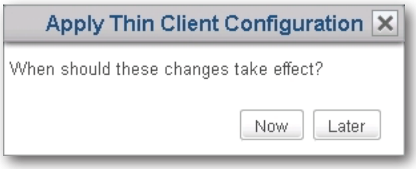
☑ Enable Custom Wallpaper

Wallpaper Style: Stretched

Download From: Device Manager

Custom wallpaper File: * Wallpaper06s.jpg

9. Click **Save** to confirm. A window appears prompting to apply the configuration.



Apply Thin Client Configuration

When should these changes take effect?

10. Click **Now** to apply immediately, and follow the on-screen instructions to complete the task. A restart to the thin client is required.

NOTE

- If **Later** is selected, then you need to push settings to the client later for the change to take effect.

TIP

- Through the similar steps, you can also edit a profile on Atrust Device Manager and apply configuration to a group of thin clients.

A.2 Using Images as Screensaver on Clients via Atrust Device Manager

The Scenario where Applicable

This appendix provides instructions on how to use images as screensaver on thin clients via Atrust Device Manager.

Atrust Device Manager: v2.20.xxx / v2.08.054 or later.

NOTE

- Please note thin clients may need new firmware to support this feature.

Getting Screensaver Images Files Ready for Use

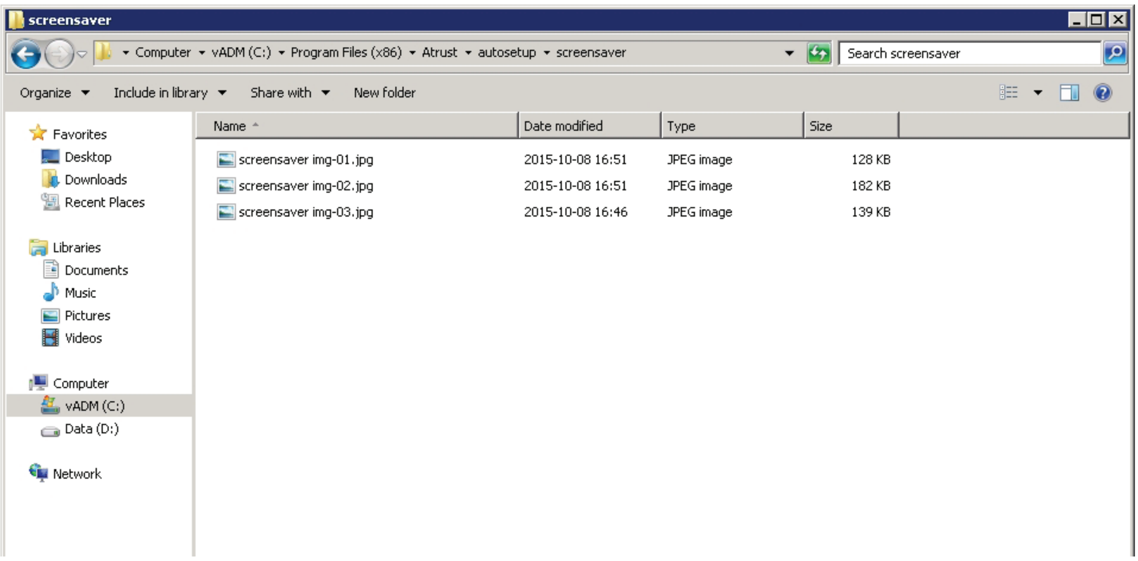
Please do the following to get screensaver image files ready for use:

1. On the computer where Atrust Device Manager is installed, find the path: **C:\\Program Files (x86)\Atrust\autosetup\screensaver**.

NOTE

- This is the default path. It might be different if you choose another path while installing Atrust Device Manager.

2. Put your screensaver images under this path.



Name	Date modified	Type	Size
screensaver img-01.jpg	2015-10-08 16:51	JPEG image	128 KB
screensaver img-02.jpg	2015-10-08 16:51	JPEG image	182 KB
screensaver img-03.jpg	2015-10-08 16:46	JPEG image	139 KB

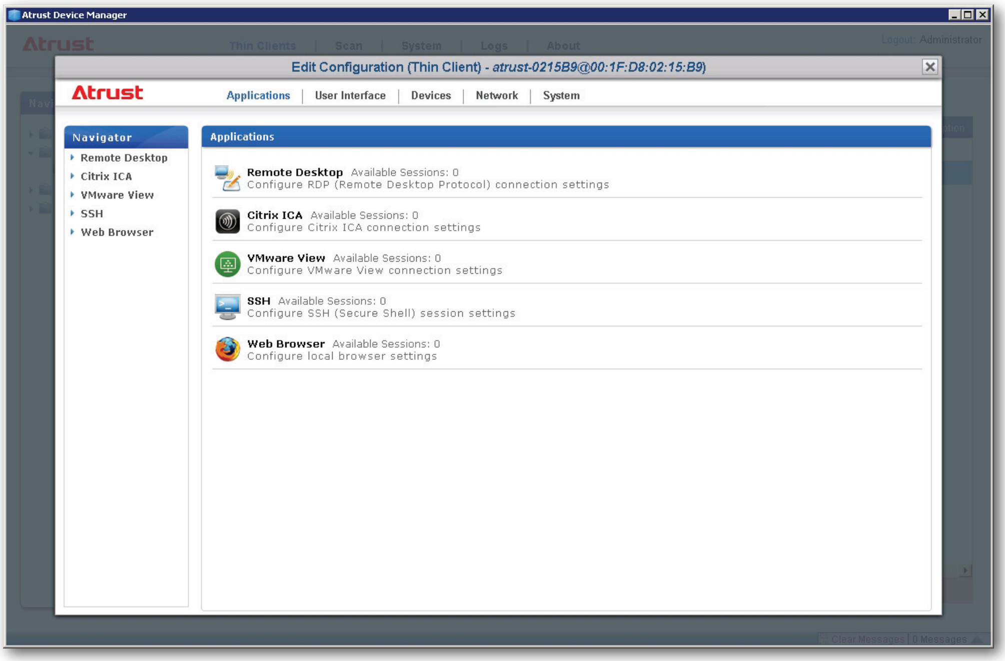
NOTE

- **Supported Image Formats:** JPG, JPEG, BMP, and PNG.
- **Image Size Limit:** 5 MB.

Enabling the Image Mode of Screensaver

To enable the Image mode of Screensaver for your thin clients via Atrust Device Manager, please do the following:

1. Launch Atrust Device Manager.
2. 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.
3. The Client list appears in Management area.
4. Click to select the desired client, and then click **Edit Configuration**. The Edit Configuration window for that client appears.



Edit Configuration (Thin Client) - *atrust-0215B9@00:1F:D8:02:15:B9)*

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

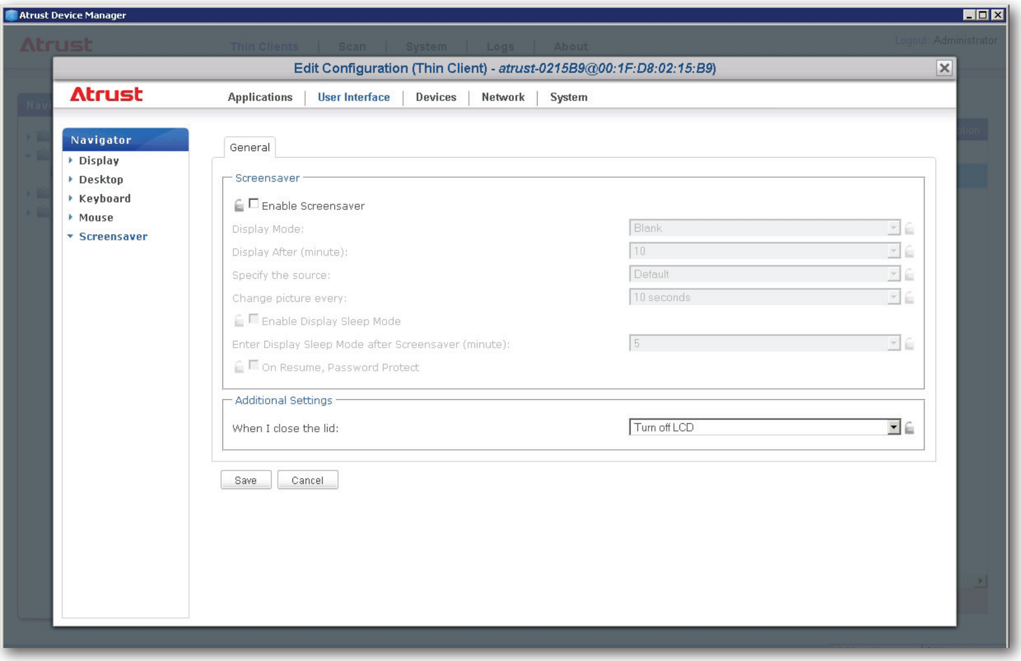
Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

Web Browser Available Sessions: 0
Configure local browser settings

5. Click **User Interface** > **Screensaver**.



Edit Configuration (Thin Client) - *atrust-0215B9@00:1F:D8:02:15:B9)*

Screensaver

□ Enable Screensaver

Display Mode: Blank

Display After (minute): 10

Specify the source: Default

Change picture every: 10 seconds

□ Enable Display Sleep Mode

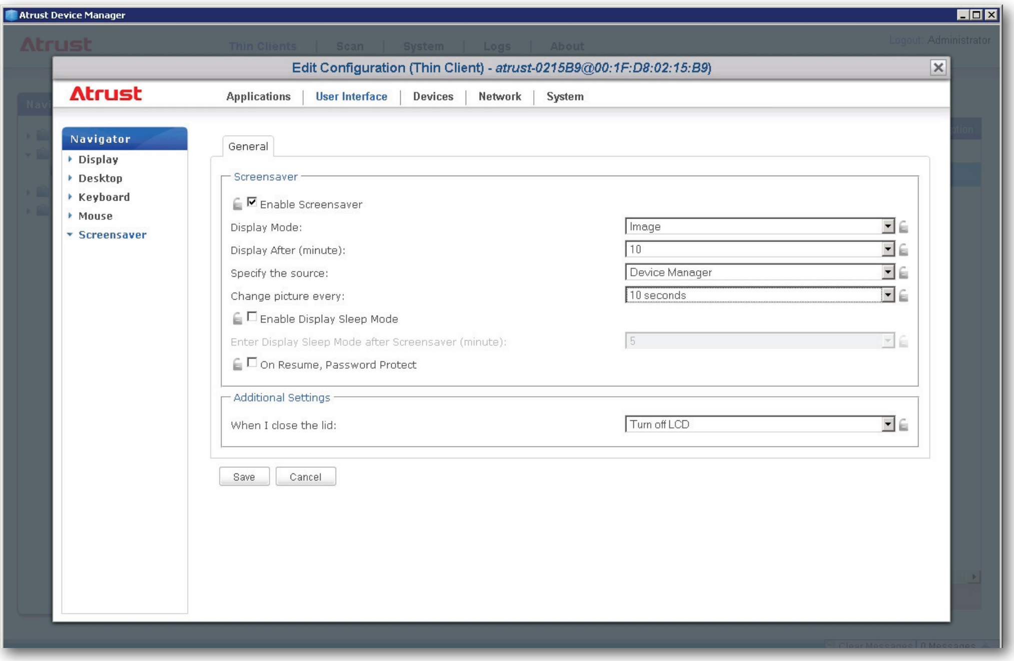
Enter Display Sleep Mode after Screensaver (minute): 5

□ On Resume, Password Protect

Additional Settings

When I close the lid: Turn off LCD

6. Check **Enable Screeensaver**, select **Image** as the display mode, specify **Device Manager** as the source, configure other settings, and then click **Save** to confirm.



Edit Configuration (Thin Client) - *atrust-0215B9@00:1F:D8:02:15:B9)*

Screensaver

☑ Enable Screensaver

Display Mode: Image

Display After (minute): 10

Specify the source: Device Manager

Change picture every: 10 seconds

□ Enable Display Sleep Mode

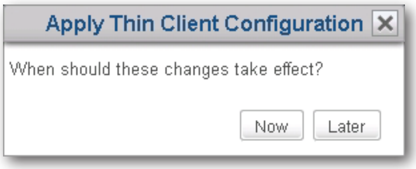
Enter Display Sleep Mode after Screensaver (minute): 5

□ On Resume, Password Protect

Additional Settings

When I close the lid: Turn off LCD

7. A window appears prompting to apply the configuration.



Apply Thin Client Configuration

When should these changes take effect?

8. Click **Now** to apply immediately, and follow the on-screen instructions to complete the task. A restart to the thin client is required.

NOTE

- If **Later** is selected, then you need to push settings to the client later for the change to take effect.

TIP

- Through the similar steps, you can also edit a profile on Atrust Device Manager and apply configuration to a group of thin clients.

A.3 Configuring Your DHCP or DNS Server for Auto Registration

The Scenario where Applicable

If Auto Registration is enabled on both your Atrust Device Manager and thin clients, when thin clients are online, they will be automatically registered and managed by Atrust Device Manager. However, you could configure your DHCP or DNS server to better ensure Auto Registration mechanism. This appendix provides instructions on how to configure your DHCP or DNS server for Auto Registration.

Atrust Device Manager: v2.20.xxx / v2.08.048 or later.

NOTE

- Please note thin clients may need new firmware to support Auto Registration.

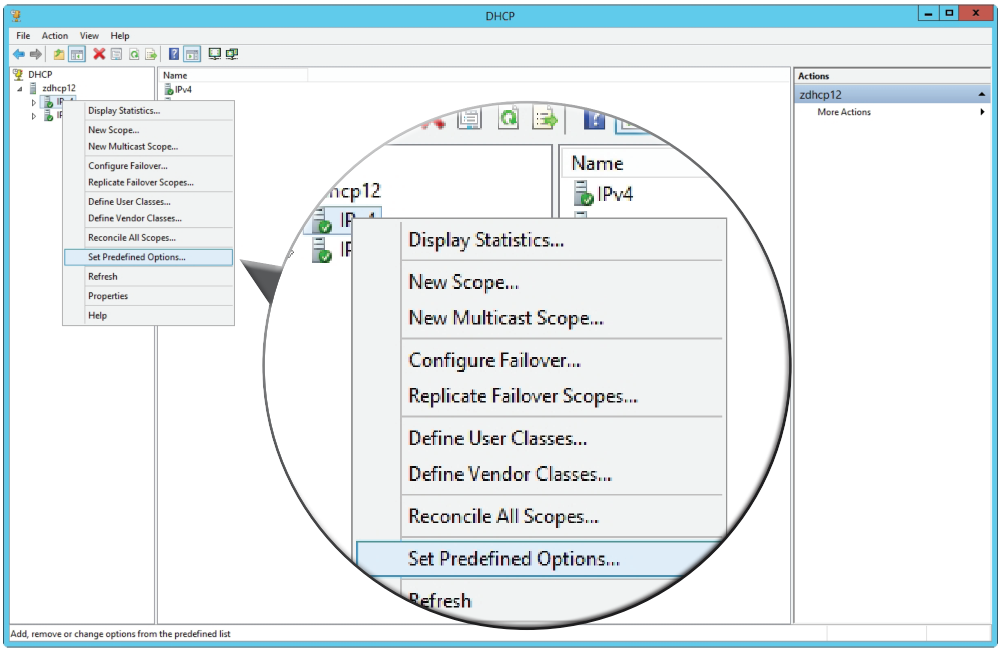
Configuring Your DHCP Server for Auto Registration

To configure your DHCP server for Auto Registration, please do the following:

NOTE

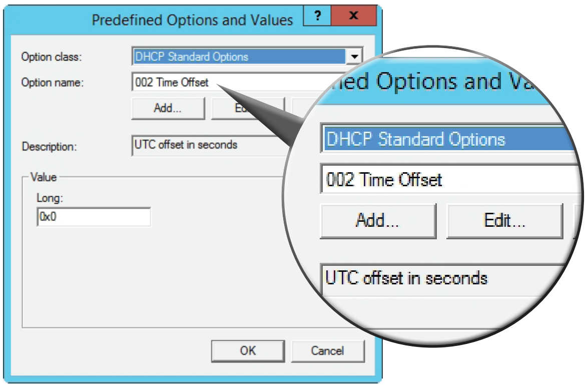
- Instructions here are based on a DHCP server implemented with Windows Server 2012 R2. A DHCP server with a different OS or edition might have different steps.

1. Log in to your DHCP server with an administrator account.
2. Click **Start** > **Administrative Tools** > **DHCP** to launch the DHCP management console.
3. Expand the tree in the left pane, right-click on **IPv4** to open the popup menu, and then select **Set Predefined Options**.



Add, remove or change options from the predefined list

4. On the opened dialog box, click **Add**.



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 002 Time Offset

Add... Edit...

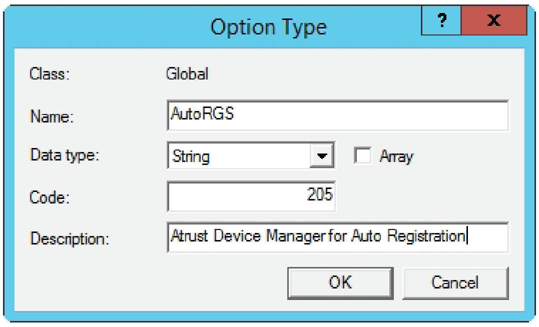
Description: UTC offset in seconds

Value

Long: 0x0

OK Cancel

5. On the opened dialog box, type the desired option name, click the drop-down menu to select **String** as the data type, enter **205** in the Code field, add the desired description, and then click **OK** to confirm. The newly added option is shown in the drop-down menu.



Option Type

Class: Global

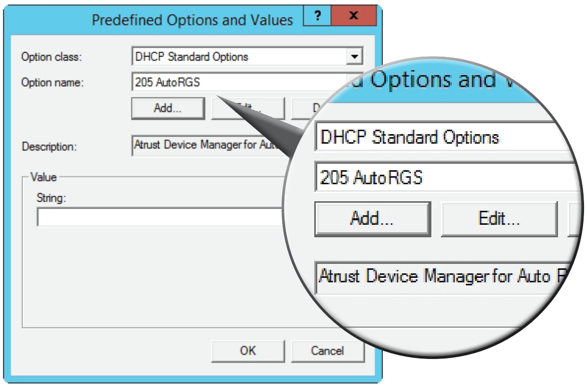
Name: AutoRGS

Data type: String □ Array

Code: 205

Description: Atrust Device Manager for Auto Registration

OK Cancel



Predefined Options and Values

Option class: DHCP Standard Options

Option name: 205 AutoRGS

Add... Edit...

Description: Atrust Device Manager for Auto Registration

Value

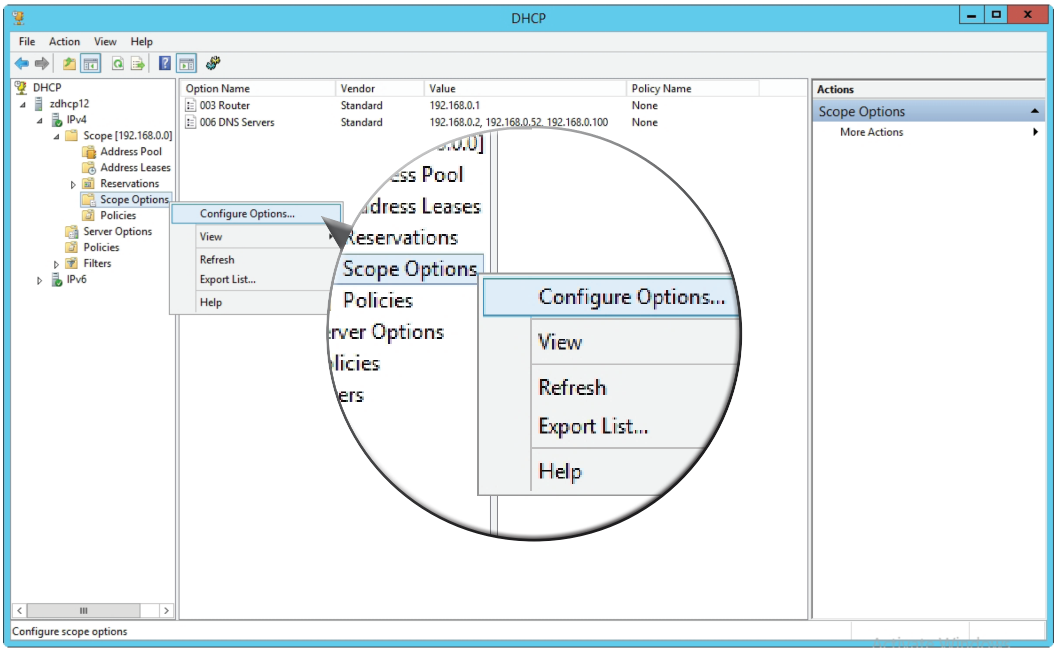
String:

OK Cancel

6. Click **OK** to close the dialog box.

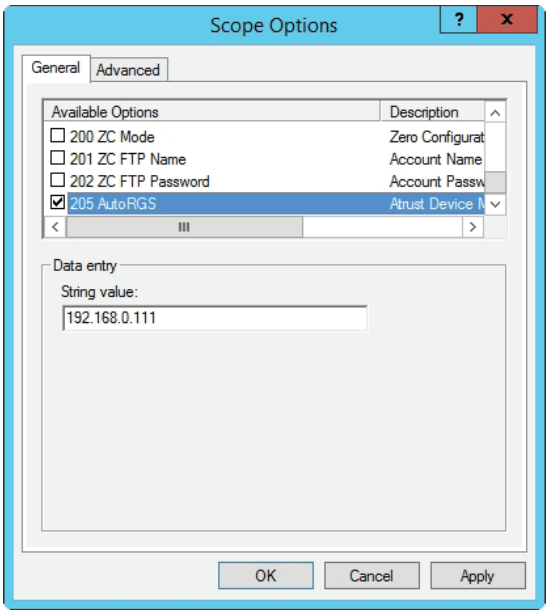
7. Add an option to tell thin clients where to get registered (the management console, i.e., the target Atrust Device Manager):

   (a) In the left pane, expand the IP Scope node for thin clients, right-click on **Scope Options** to open a popup menu, and then click **Configure Options**.



Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.0.1	None
006 DNS Servers	Standard	192.168.0.2, 192.168.0.52, 192.168.0.100	None

(b) On the opened dialog box, use the scroll bar to locate and select the Code 205 option, and then type the IP address of target Atrust Device Manager as the string value.



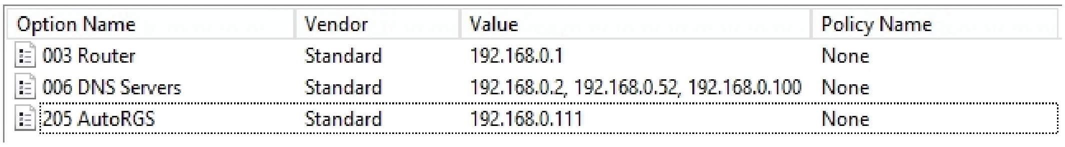
Available Options	Description
☐ 200 ZC Mode	Zero Configurat
☐ 201 ZC FTP Name	Account Name
☐ 202 ZC FTP Password	Account Passw
☑ 205 AutoRGS	Atrust Device M

Data entry

String value:

192.168.0.111

(c) Click **OK** to confirm. The new entry is shown in the middle pane.



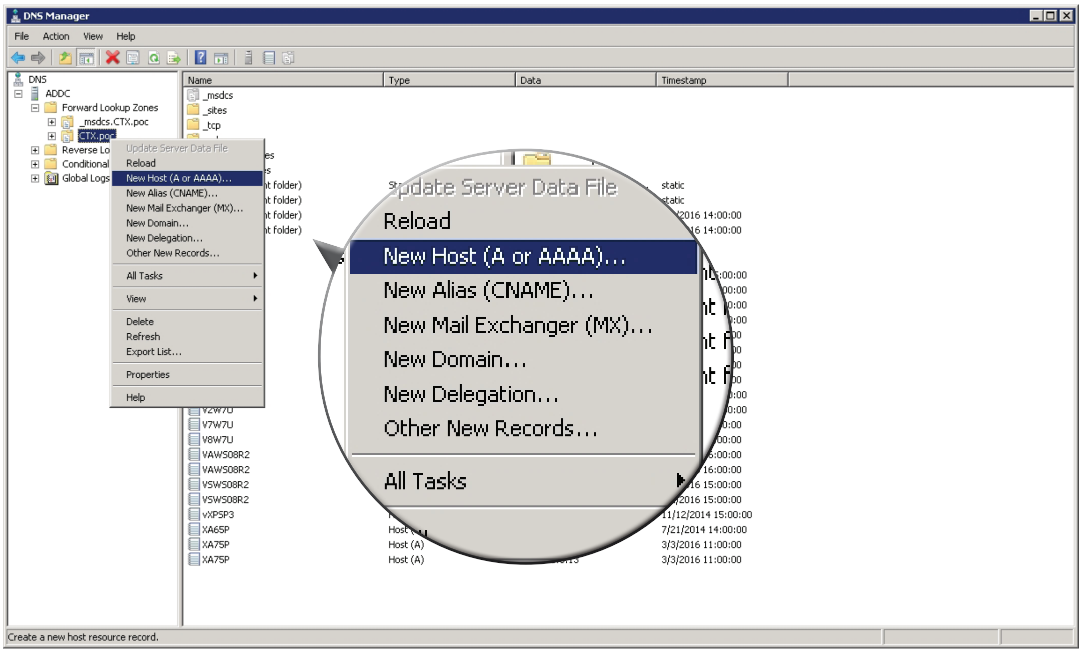
Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.0.1	None
006 DNS Servers	Standard	192.168.0.2, 192.168.0.52, 192.168.0.100	None
205 AutoRGS	Standard	192.168.0.111	None

Configuring Your DNS Server for Auto Registration

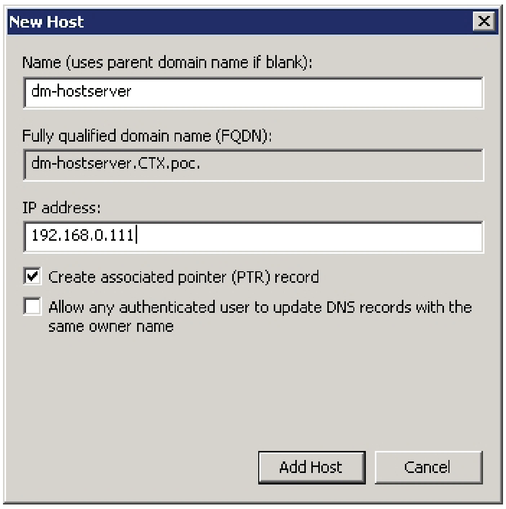
To configure your DNS server for Auto Registration, please do the following:

1. Log in to your DNS server with an administrator account.
2. Click **Start** > **Administrative Tools** > **DNS** to launch DNS Manager.
3. Add a Host entry to tell thin clients where to get registered (the management console, i.e., the target Atrust Device Manager):

   (a) In the left pane, expand the node of **Forward Lookup Zones**, right-click on the node of the domain, and then select **New Host (A or AAAA)**.



   (b) Type **dm-hostserver** in the Name field, the IP address of target Atrust Device Manager in the IP address field, and then click **Add Host** to add this new entry.



New Host

Name (uses parent domain name if blank):

dm-hostserver

Fully qualified domain name (FQDN):

dm-hostserver.CTX.poc.

IP address:

192.168.0.111

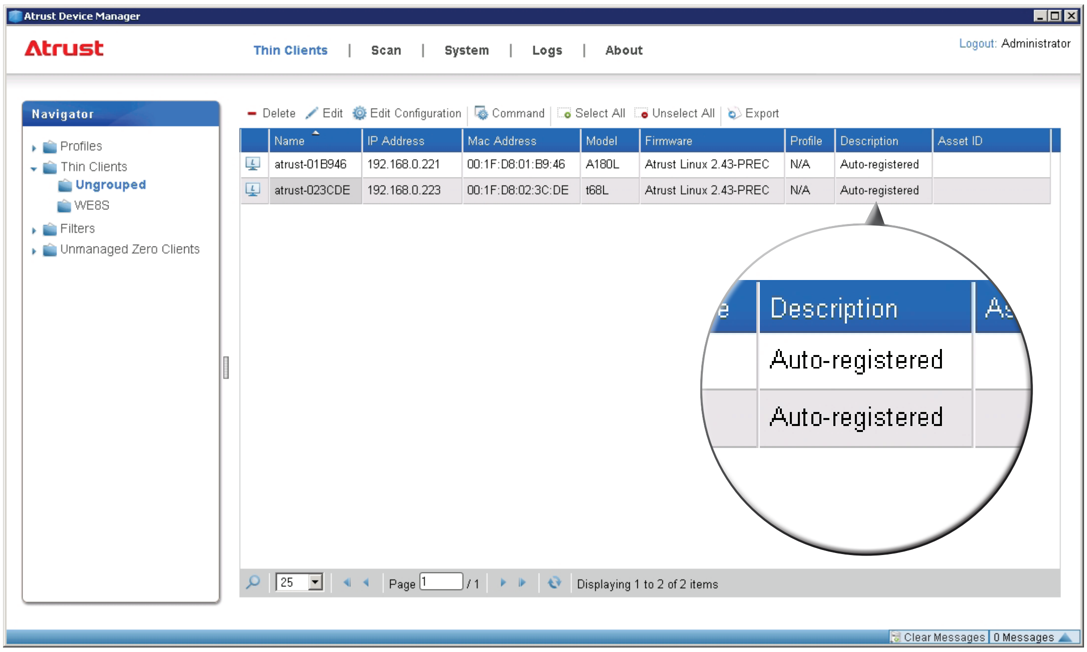
☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

What to Expect When Thin Clients are Online

If configurations on the server side are ready for Auto Registration, when an Auto-Registration-capable thin client is online, it will get registered on target Atrust Device Manager, and therefore managed by this instance of Atrust Device Manager.

Thin clients will be automatically added under **Ungrouped** of the target Atrust Device Manager. For thin clients added by Auto-Registration, you can find **Auto-registered** in their Description column as shown below.



	Name	IP Address	Mac Address	Model	Firmware	Profile	Description	Asset ID
	atrust-01B946	192.168.0.221	00:1F:D8:01:B9:46	A180L	Atrust Linux 2.43-PREC	N/A	Auto-registered	
	atrust-023CDE	192.168.0.223	00:1F:D8:02:3C:DE	t68L	Atrust Linux 2.43-PREC	N/A	Auto-registered	

Displaying 1 to 2 of 2 items

A.4 Customizing Remote Reboot and Shutdown of Thin Clients

The Scenario where Applicable

By default, when you reboot / shut down a thin client remotely through Atrust Device Manager, a warning message will appear to notify the user of the planned reboot / shut down and allow the user to cancel the action if necessary.

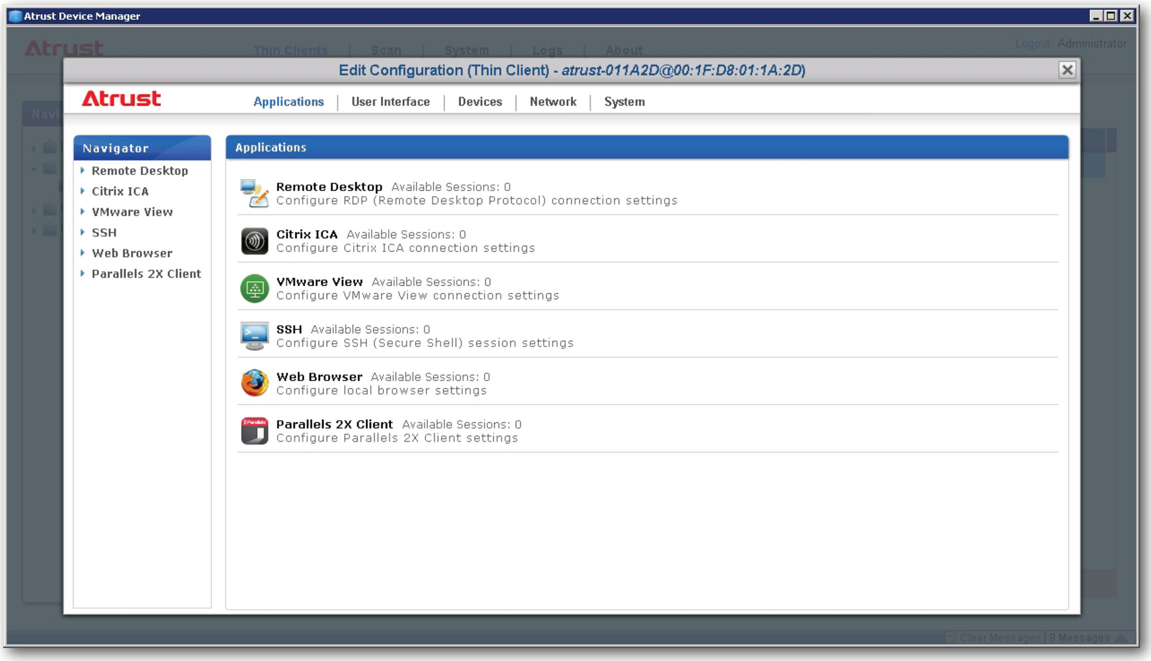
This appendix provides instructions on how to customize settings on Atrust Device Manager to change the default remote reboot / shut down behaviors for thin clients.

Atrust Device Manager: v2.20.024 or later.

Customizing Remote Reboot and Shutdown

To customize remote reboot and shutdown behaviors for a thin client, please do the following:

1. Launch Atrust Device Manager.
2. 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.
3. The Client list appears in Management area.
4. Click to select the desired client, and then click **Edit Configuration**. The Edit Configuration window for that client appears.



Edit Configuration (Thin Client) - *atrust-011A2D@00:1F:D8:01:1A:2D)*

Remote Desktop Available Sessions: 0
Configure RDP (Remote Desktop Protocol) connection settings

Citrix ICA Available Sessions: 0
Configure Citrix ICA connection settings

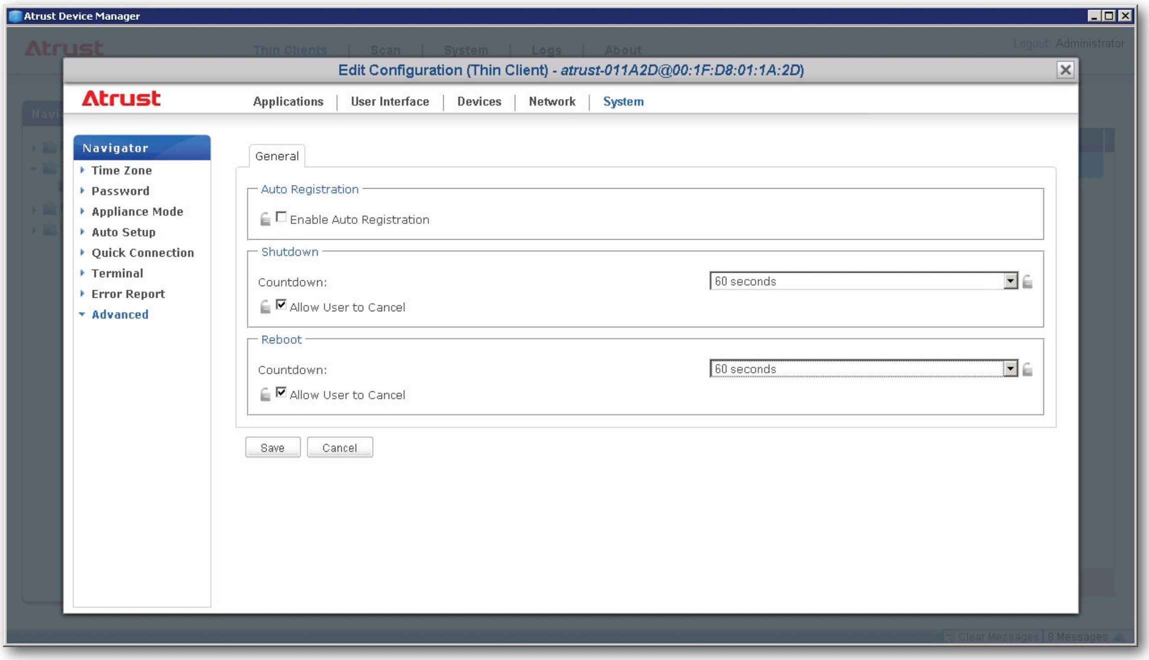
VMware View Available Sessions: 0
Configure VMware View connection settings

SSH Available Sessions: 0
Configure SSH (Secure Shell) session settings

Web Browser Available Sessions: 0
Configure local browser settings

Parallels 2X Client Available Sessions: 0
Configure Parallels 2X Client settings

5. Click **System** > **Advanced**.



Edit Configuration (Thin Client) - *atrust-011A2D@00:1F:D8:01:1A:2D)*

Auto Registration

□ Enable Auto Registration

Shutdown

Countdown: 60 seconds

☑ Allow User to Cancel

Reboot

Countdown: 60 seconds

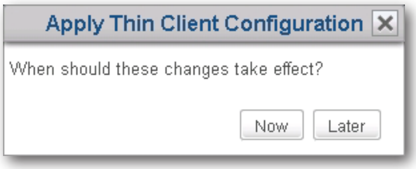
☑ Allow User to Cancel

NOTE

- By default, the user will get a 60 seconds countdown message about reboot / shut down and is allowed to cancel that action.

6. Check / Uncheck **Allow User to Cancel** to allow / disallow the user to cancel an action, click the drop-down menu to select the desired seconds / minutes to count down, and then click **Save** to confirm.

7. A window appears prompting to apply the configuration.



Apply Thin Client Configuration

When should these changes take effect?

8. Click **Now** to apply immediately, and follow the on-screen instructions to complete the task. A restart to the thin client is required.

NOTE

- If **Later** is selected, then you need to push settings to the client later for the change to take effect.

TIP

- Through the similar steps, you can also edit a profile on Atrust Device Manager and apply configuration to a group of thin clients.

Atrust