



Intel® Education

Theft Deterrent

Deployment Guide

August 2016

Legal Notices

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

The API and software may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright © 2011 Intel Corporation.

* Third party names and brands may be claimed as the property of others.

Table of Contents

1.	Introduction	1
1.1	Document purpose and scope	1
1.2	Terminology	1
1.2.1	Abbreviations	1
1.2.2	Terms	1
1.3	Revision History	1
1.4	Reference Document	2
2.	Theft Deterrent Overview	3
2.1	Deployment Workflow	4
3.	Plan Theft Deterrent server Deployment	5
3.1	Choose Theft Deterrent Solution Architecture	5
3.1.1	Centralized Architecture	6
3.1.2	Decentralized Architecture	6
3.1.3	Hierarchized Architecture	7
3.2	Choose Database and Download Server Locations	8
3.2.1	Choose Database Hosting	9
3.2.2	Choose Download Feature Hosting	9
4.	Theft Deterrent server Requirements	10
4.1	Requirements for Decentralized or Hierarchized Architecture	10
4.2	Requirements for deploying Centralized Architecture	10
4.2.1	Requirements for Theft Deterrent server	11
4.2.2	Requirements for Download Server	12
4.3	General Requirements	13
4.3.1	Operating System Requirements	13
4.3.2	Domain Name Requirement	13
4.3.3	Security Guideline	13
4.3.4	Other Requirements	14
5.	Deploy Theft Deterrent server on Debian	15
5.1	Install Dependencies	15
5.2	Install Theft Deterrent server	15
5.3	Best Practice of Performance Tuning	17
5.4	Upgrade Theft Deterrent server	18
5.5	Repair or Re-install Theft Deterrent server	18
5.6	Uninstall Theft Deterrent server	20
6.	Deploy Theft Deterrent server on Windows	21
6.1	Install Theft Deterrent server	21
6.2	Best Practice of Performance Tuning	23
6.2.1	Common Configuration	23
6.2.2	Tune the Performance	26
6.3	Upgrade Theft Deterrent server	26
6.4	Repair or Re-install Theft Deterrent server	28
6.5	Uninstall Theft Deterrent server	28
7.	Theft Deterrent server Pre-configurations	30
7.1	First Time Configurations	30
7.1.1	Activate Theft Deterrent server	30
7.1.2	Reactivate Theft Deterrent server	31
7.1.3	Set up Server Name & Address	32
7.1.4	Set up E-mail Notification Service	32
7.2	Modify the Server Log Level	33
7.3	Server Installation Directories and Log Files	33
8.	Use Separate Download Server	35
8.1	Configure Download Server	35

8.2	Configure Download Feature on Theft Deterrent server	35
9.	Manually Deploy Theft Deterrent client and guardian	37
9.1	Deploy Theft Deterrent client and guardian on Windows	37
9.1.1	Prerequisite	37
9.1.2	Install with Command Line	38
9.1.3	Install with Install Wizard	38
9.2	Deploy Theft Deterrent client and guardian on Debian	39
9.2.1	Install Dependency	39
9.2.2	Install Theft Deterrent client and guardian	39
9.3	Pre-set server address and address modify protection password	40
9.4	Open Theft Deterrent client	41
9.4.1	Open Theft Deterrent client on Windows	41
9.4.2	Open Theft Deterrent client on Debian	41
9.5	Installation Directories and Log Files	43
10.	Troubleshooting.....	45
10.1	Theft Deterrent server Installation Failed	45
11.	FAQ	46
12.	Appendix.....	49
12.1	Choose Root Key Pair	49
12.2	Choose Server Support Mode	49
12.3	How to Understand the Network Stability	50
12.4	How to Calculate the Required Network Bandwidth	51
12.5	How to Improve the Download Performance	51
12.6	How to Back up Theft Deterrent server	52
12.7	How to offline Transfer Devices to Theft Deterrent server 4.x	52

List of Figures

Figure 1 - Theft Deterrent architecture	3
Figure 2 - Centralized Architecture.....	6
Figure 3 - Decentralized Architecture.....	7
Figure 4 - Hierarchized Architecture.....	7
Figure 5 - Theft Deterrent server Options	8
Figure 6 - Local or Separate Download Feature	9
Figure 7 - Database Location	16
Figure 8 - Select Root Public Key Type (Stand-alone Mode)	16
Figure 9 - Import Root Public Key (Stand-alone Mode).....	17
Figure 10 - Repair or Re-install Theft Deterrent server	19
Figure 11 - Database Location	21
Figure 12 - Server Support Mode	22
Figure 13 - Stand-alone Mode	22
Figure 14 - Import Root Public Key (Stand-alone Mode).....	23
Figure 15 - Configure Performance (1)	24
Figure 16 - Configure Performance (2)	24
Figure 17 - Configure Performance (3)	25
Figure 18 - Add Trusted Sites.....	25
Figure 19 - Configure Security Level	26
Figure 20 - Repair or re-install Theft Deterrent server	28
Figure 21 - Activate Server (1)	31
Figure 22 - Activate Server (2)	31
Figure 23 - Set up E-mail Notification Service	32
Figure 24 - Server Tabs	33
Figure 25 - Configure Download Server.....	36
Figure 26 - Client Inactive Tray Icon (Windows)	41
Figure 27 - Client Inactive Tray Icon.....	42
Figure 28 - Shortcut on GNOME	42
Figure 29 - Shortcut on GNOME Classic.....	43
Figure 30 - Choose Server Support Mode.....	50
Figure 31 - Check Network Latency	50
Figure 32 - Back up the server	52
Figure 33 - Run KeyManagement Tool	53
Figure 34 - Import Pre-activated Package	53

1. Introduction

1.1 Document purpose and scope

This document introduces the procedures to deploy Intel® Education Theft Deterrent solution for version 4.x.

The document contains the following information:

- Introduction to the Theft Deterrent solution
- Requirements of the Theft Deterrent server depending on the deployment scenarios
- Deployment steps for the Theft Deterrent server
- Steps to migrate from earlier versions of the Theft Deterrent server to version 4.x
- Pre-configuration steps of the Theft Deterrent server
- Configuration steps to enable the Theft Deterrent server to use a separate download server
- Deployment steps for the Theft Deterrent client and guardian 4.x
- Troubleshooting and FAQ

1.2 Terminology

1.2.1 Abbreviations

<i>Abbreviation</i>	<i>Description</i>
server	Theft Deterrent server
client	Theft Deterrent client

1.2.2 Terms

<i>Term</i>	<i>Description</i>
device	Intel® classmate PC or Intel® Education Tablet
online devices	The devices that are connected with the server network and their clients are activated and communicating with the server.

1.3 Revision History

<i>Revision</i>	<i>Date</i>	<i>Comment</i>
0.62	2013/9	Add usage for server upgrade package and add re-install server section. Update the migrate tool usage
0.63	2013/11	Move migrate section to Toolkits User Guide. Add one dependency for Linux client.
0.64	2014/6	Change TD server minimize Hard disk size request

1.4 Reference Document

<i>Document</i>	<i>Date</i>
Intel® Education Theft Deterrent server User Manual	2013-04
Intel® Education Theft Deterrent client User Manual	2013-02
Intel® Education Theft Deterrent Root CA Server Deployment Guide	2013-04
Intel® Education Theft Deterrent Central Server Deployment Guide	2013-07
Intel® Education Theft Deterrent Toolkits User Guide	2013-11

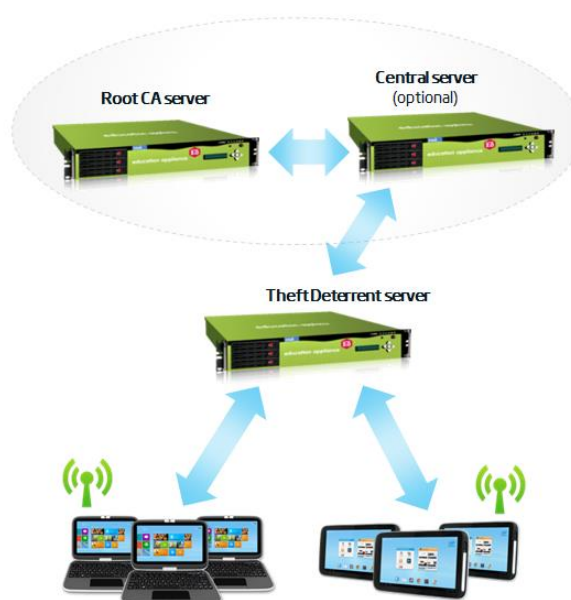
2. Theft Deterrent Overview

As part of the Intel® Education Software suite, Theft Deterrent provides a complete physical security management solution for your Intel® Education Tablet and Intel® classmate PC.

Note: The term **device** is used throughout this document to refer to Intel® Education Tablet and Intel® classmate PC.

To be successful with Theft Deterrent, you must first thoroughly plan and test the management features before you use Theft Deterrent in a production environment. As a powerful management application, Theft Deterrent can potentially affect every computer in your organization. When you deploy and manage Theft Deterrent with careful planning and consideration of your business requirements, Theft Deterrent can reduce your administrative overhead and total cost of ownership.

Figure 1 - Theft Deterrent architecture



Prior to deployment, it is necessary to understand the different components of Theft Deterrent:

- **Root CA server:** Each Theft Deterrent solution must contain one root CA server. This server generates and manages the root key pair, trusted by every Theft Deterrent client that it manages.
- **Central server:** An optional component of the Theft Deterrent solution that enables device transfer among schools.
- **Theft Deterrent server:** It manages the devices installed with the Theft Deterrent clients. The functions of this server include provision certificates, lock and unlock devices, etc.
- **Theft Deterrent client (client):** This component runs on devices and can lock and unlock devices based on the certificates received from the Theft Deterrent server.

2.1 Deployment Workflow

In general, a new deployment of the Theft Deterrent solution follows this order:

1. **Deploy root CA server**
2. **Deploy central server:** This step is optional.
3. **Deploy Theft Deterrent server:** This component can be deployed at school, district, or country-level.
4. **Deploy Theft Deterrent clients**

The remainder of this document focuses on the deployment of the server and the client. To deploy the root CA server, see the Intel® Education Theft Deterrent Root CA Server Deployment Guide. To deploy the central server, see the Intel® Education Theft Deterrent Central Server Deployment Guide.

3. Plan Theft Deterrent server Deployment

The server can be deployed in different scenarios to meet different customers' needs. Therefore, it is necessary to understand the options available and decide which option is appropriate for your environment:

- [Choose Theft Deterrent solution architecture](#): centralized, decentralized, or hierarchized
- [Choose the locations of the server database and download server](#): local or separate

For example, you can refer to the following options for a typical deployment scenario:

<i>Deployment Options</i>	<i>Recommended Option</i>	
Architecture	Centralized	Deploy server with your own root key pair
		No central server
		Deploy server with the Stand-alone mode with your own Root Public Key
Database hosting	Local database	
Download feature hosting	Separate download server	

For detailed information on how to choose these deployment options, see the following chapters.

3.1 Choose Theft Deterrent Solution Architecture

You can deploy the Theft Deterrent solution with one of the following architectures:

- [Centralized](#)
- [Decentralized](#)
- [Hierarchized](#)

Each architecture requires different network settings and different sets of deployment configurations. Please refer to the table below for the deployment configurations:

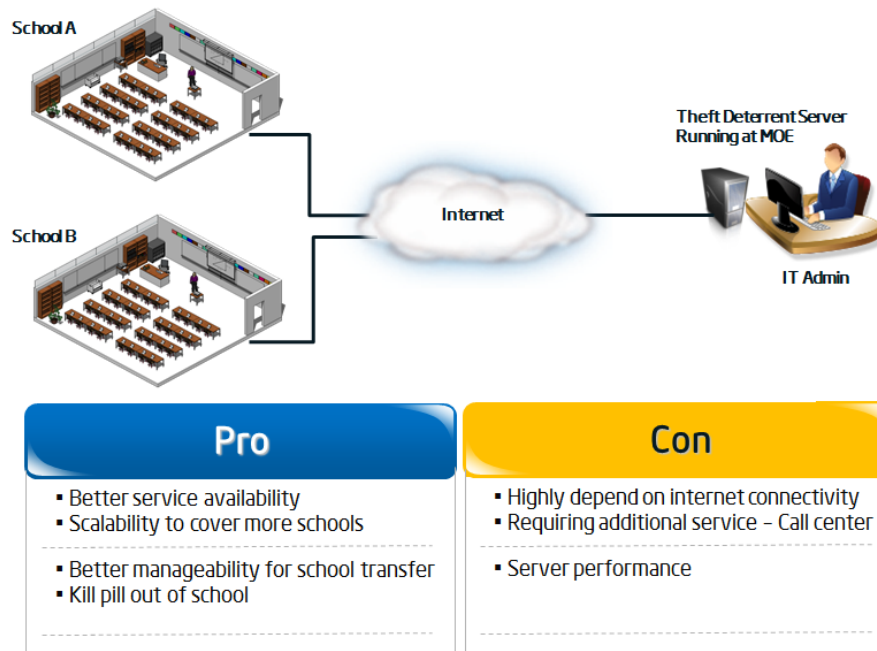
<i>Deployment Configurations</i>	<i>Descriptions</i>
Root key pair	Root CA server generates root key pair, trusted by every client that it manages. You can choose to deploy your own root CA server to generate your own root key pair or use the key pair from Intel.
Central server	Central server enables additional functions such as school transfer and server backup/restore. You can choose whether these are needed in your environment.
Server support mode	Stand-alone or Central Server Supported mode

See the following chapters for detailed information about the three architectures. For more information about the root key pair and server support modes, see [Appendix](#).

3.1.1 Centralized Architecture

The server is hosted at region or country level in centralized architecture. This architecture is recommended in general.

Figure 2 - Centralized Architecture



This architecture requires that the region or country has stable Internet connection. The deployment options selected for this architecture is as follows:

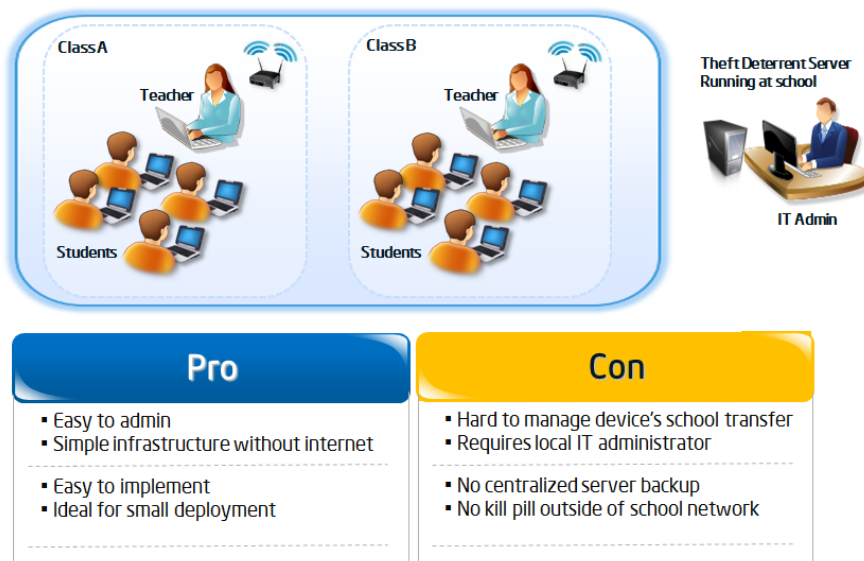
Deployment Configurations	Configured Settings
Root key pair	Your own root key pair
Central server	No central server
Server support mode	Stand-alone mode with your own Root Public Key

3.1.2 Decentralized Architecture

The server is hosted at individual school level in decentralized architecture. Select this architecture in either of the following cases:

- Deploying a test or demo server
- The schools or devices do not have stable Internet connection. For example, the [network latency](#) of your school network is larger than 300ms.

Figure 3 - Decentralized Architecture



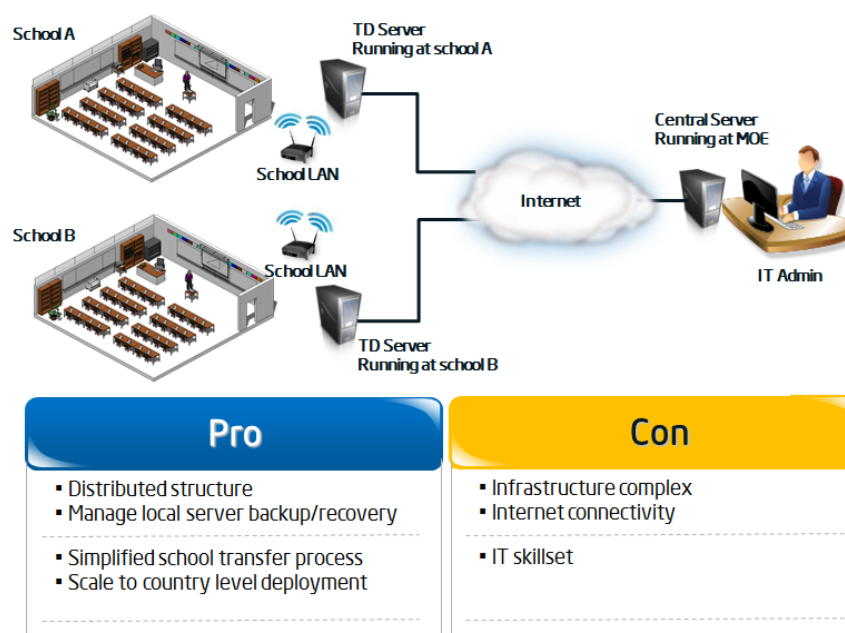
The network required for this architecture is LAN. The deployment options selected for this architecture is as follows:

Deployment Configurations	Configured Settings
Root key pair	Intel root key pair
Central server	No central server
Server support mode	Stand-alone mode with the Intel Root Public Key

3.1.3 Hierarchized Architecture

The server is hosted at individual school level in the hierarchized architecture. This architecture requires a central server.

Figure 4 - Hierarchized Architecture



LAN is required for each school hosting the server, while stable Internet connection is required for each school server to communicate with the central server hosted at country level.

The deployment options selected for this architecture is as follows:

<i>Deployment Configurations</i>	<i>Configured Settings</i>
Root key pair	Your own root key pair
Central server	Deploy central server
Server support mode	Stand-alone mode with your own Root Public Key or Central Server Supported mode



Note: If you choose to deploy the servers with **Central Server Supported** mode, make sure that the central server is accessible to the servers for server activation. For more information about the server support modes, see [Appendix](#).

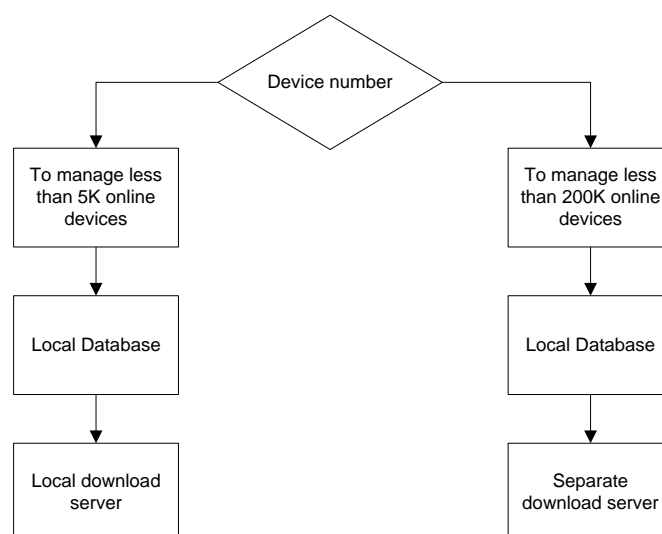
3.2 Choose Database and Download Server Locations

Once you determine the options for the Theft Deterrent architecture, you can consider having a separate database server or download server for better performance or scalability of your server:

<i>Deployment Options</i>	<i>Descriptions</i>
Database hosting	Database is created during server installation. You can choose to have the database created in the same server machine or in a different machine.
Download feature hosting	Download server stores client software packages that can be downloaded by clients version 4.x or above. You can choose to have the download server installed in the same server machine or in a different machine.

Please see process map below for guidance:

Figure 5 - Theft Deterrent server Options





Note: If you want to deploy a server to manage more than 200K devices, contact the local Intel TME for support.

See the following chapters for detailed information on how to choose the locations for the database and download servers.

3.2.1 Choose Database Hosting

The server consists of database and web service components which come with the server installation package. These components can be installed on a single machine or on different machines for better performance and scalability.

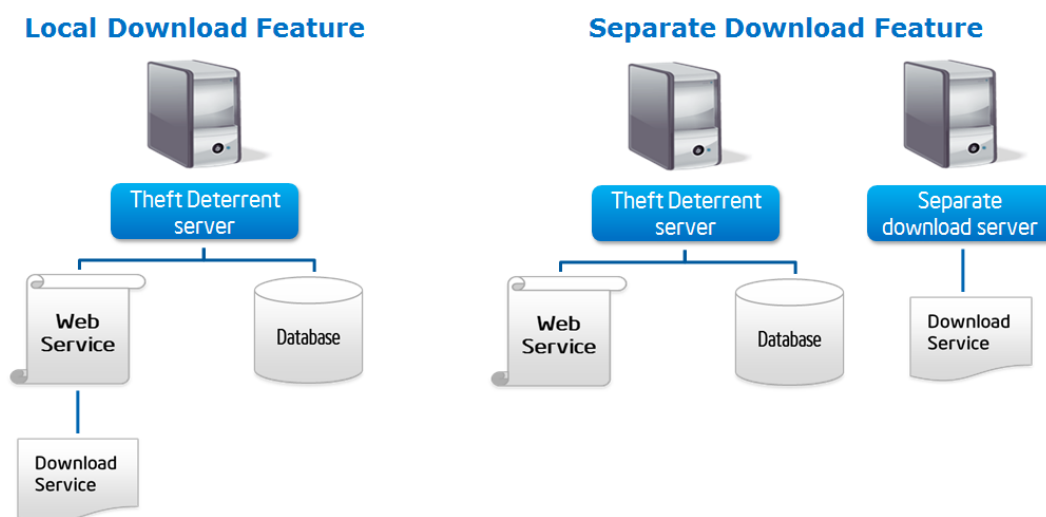
In general, it is recommended that you deploy the server with a local database unless your server is required to manage more than 200K online devices, in which case contact the Intel local TME for support.

3.2.2 Choose Download Feature Hosting

The server includes a **Smart Client Upgrade** function which provides clients with upgrade packages through HTTP download. The download performance is dependent on how you deploy the server download feature. You can deploy the feature with either of the following methods:

- Local: Deploy the download feature as a feature of the web service.
- Separate: Use a third-party download server to provide the download feature.

Figure 6 - Local or Separate Download Feature



In general, it is recommended that you deploy the server on the Internet with a separate download server if the number of online devices it manages is larger than 5K.

You can configure the server to specify the location where clients should download the packages according to the location of the download feature chosen. Detailed configuration steps are introduced in chapter 8.

For more information about the **Smart Client Upgrade** function, see the Intel® Education Theft Deterrent server User Manual.

4. Theft Deterrent server Requirements

The requirements of the server vary between the Theft Deterrent architectures: centralized, decentralized, or hierarchized.

Configure your hardware, software, and network to meet the requirements specific to your architecture and then follow the general requirements.

4.1 Requirements for Decentralized or Hierarchized Architecture

This section introduces the requirements for deploying the server in the decentralized or hierarchized architecture. Both architectures deploy the server on LAN in schools and the general deployment scenario assumes that the number of devices to be managed is less than 5K.

It is recommended that you deploy the server with the following modes:

- **Local database.**
- **Local download feature**

The hardware and network requirements for the server are as follows:

<i>Online devices</i>	<i>Requirement</i>	<i>Recommended configuration</i>	<i>Minimal configuration</i>
< 5K	Hardware	CPU: 1 x Intel® Xeon®, 4 cores Memory: 4 GB	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB
	OS	Linux or Windows	Linux or Windows
	Network bandwidth (Mbps)	10	4

The minimum hard disk space required is 2GB. However, the recommended hard disk space for the server is 30 GB and above.

4.2 Requirements for deploying Centralized Architecture

This section introduces the requirements for deploying the server in the centralized architecture. This architecture deploys the server on the Internet at region or country level. Therefore, the general deployment scenario assumes that the number of devices to be managed is more than 5K. First of all, the following requirements must be met:

- The server must be protected against network DDoS attack.
- All the schools and students at home must be able to access the server with enough bandwidth and network latency, which should be less than 300ms in both directions.

It is recommended that you deploy the server with the following modes:

Local database:

Unless your deployment plan specifies otherwise, deploy the server with the local database which supports the general deployment scenarios that manage less than 200K devices.

Separate download server:

It is recommended that you use a third-party download server. Also, do not share the download bandwidth with the web server bandwidth. Otherwise, the downloading might use too much bandwidth and cause network congestion which will prevent devices from connecting with the server.

4.2.1 Requirements for Theft Deterrent server

The requirements for the server differ according to the network latency, which will cause time delay when data transmits between the server and the clients. To estimate the latency of your network, see [Appendix](#).

If your network latency ≤ 300 ms, refer to the server requirements displayed in the following table. If your network latency > 300 ms, contact your local TME for support.

<i>Online devices</i>	<i>Requirement</i>	<i>Recommended configuration</i>	<i>Minimal configuration</i>
< 10K	Hardware	CPU: 1 x Intel® Xeon®, 4 cores Memory: 4 GB	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB
	OS	Linux or Windows	Linux or Windows
	Network bandwidth (Mbps)	2	1
10-50K	Hardware	CPU: 1 x Intel® Xeon®, 4 cores with hyper-thread Memory: 8 GB	CPU: 1 x Intel® Xeon®, 4 cores Memory: 8 GB
	OS	Linux or Windows	Linux or Windows
	Network bandwidth (Mbps)	9	4
50-100K	Hardware	CPU: 2 x Intel® Xeon®, 4 cores for each with hyper-thread Memory: 16 GB	CPU: 2 x Intel® Xeon®, 4 cores for each with hyper-thread Memory: 12 GB
	OS	Linux	Linux
	Network bandwidth (Mbps)	18	9
100-200K	Hardware	CPU: 2 x Intel® Xeon®, 6 cores for each with hyper-thread Memory: 24 GB	CPU: 2 x Intel® Xeon®, 4 cores for each with hyper-thread Memory: 16 GB
	OS	Linux	Linux
	Network bandwidth (Mbps)	35	18

The minimum hard disk required is **15** GB. However, the recommended hard disk space for the server is 30 GB and above.



Note: The log folder needs cost 10G as maximum. So need the minimum hard disk size 15GB to avoid any issue happen.



Note: The network bandwidths recommended above are estimated according to the device numbers in four ranges. To calculate the network requirement for your specific device number, see [Appendix](#).

4.2.2 Requirements for Download Server

You can either set up a separate download server or use an existing download services provided by a Content Delivery Network (CDN) operator, a cloud based download server, etc.

The download server you choose will affect the download performance. For information on how to improve the download performance, see [Appendix](#).



Note: The download feature you use must support HTTP download.

If you choose to use an existing download service, make sure that the service provider offers stable download functions and you can skip this chapter.

If you want to set up your own download server, make sure that the following requirements are met.

Online devices	Requirement	Recommended configuration	Minimal configuration
< 10K	Hardware	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB
	OS	Linux or Windows	Linux or Windows
	Network bandwidth (Mbps)	6	3
10-50K	Hardware	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB	CPU: 1 x Intel® Xeon®, 2 cores Memory: 4 GB
	OS	Linux or Windows	Linux or Windows
	Network bandwidth (Mbps)	26	13
50-100K	Hardware	CPU: 1 x Intel® Xeon®, 4 cores Memory: 8 GB	CPU: 1 x Intel® Xeon®, 2 cores Memory: 8 GB
	OS	Linux	Linux
	Network bandwidth (Mbps)	43	21

100-200K	Hardware	CPU: 1 x Intel® Xeon®, 4 cores Memory: 12 GB	CPU: 1 x Intel® Xeon®, 4 cores Memory: 8 GB
	OS	Linux	Linux
	Network bandwidth (Mbps)	74	37



Note: The network bandwidths recommended above are estimated according to the device numbers in four ranges. To calculate the network requirement for your specific device number, see [Appendix](#).

4.3 General Requirements

4.3.1 Operating System Requirements

The server supports the following operating systems:

- **Windows:** Windows Server 2008 R2 64-bits
- **Linux:** Debian 6.0.3 64-bits/32-bits and above. You can find this operating system from the [Debian official website](#).

4.3.2 Domain Name Requirement

For centralized and hierarchized architecture, the servers or the central server are hosted on the Internet. Therefore, it is recommended that you configure a static domain name for the servers.

4.3.3 Security Guideline

The server is the root of trust for all devices in the Theft Deterrent solution. Once deployed, it is the responsibility of the IT admin to protect the server against unauthorized use or online attacks. Therefore, it is strongly recommended that you follow these guidelines to protect the server:

Physical security:

- Lock the machine in the cabinet and deny unauthorized personnel from physically accessing the server.

Network security:

- Install firewall, IPS, etc.

Operating system security:

- Configure the security settings of the operating system.
- Update the operating system and install security patches regularly.
- Close all the services not necessary for the server or restrict the services to be available only to internal IP. For example, the remote desktop/VNC.

Operating System administrator security:

- Secure the admin/root account of the operating system.

- Do not change the access permissions of the configuration files and keystore files, which are set to read only and accessible by admin/root account only by default.
- Do not add unnecessary account to the operating system or open guest accounts.

Theft Deterrent account security:

- Keep the passwords of the database server account and the database administrator account secure.
- If the database server is deployed on a separated machine, keep the machine in the internal network and configure the database server to be accessible by the web server only.
- Keep the user account passwords of the server secure. For example, require users to change their passwords frequently and never share their passwords with anyone.

General security:

- The server admin and other users should not log in the server from a public or shared computer. Also, it is recommended that you close all other websites when logged in the server.
- The server admin and other users must not misuse the server.

Device security (activation and check-in):

- It is recommended that you activate the devices in factory. The devices are protected by the Theft Deterrent solution only after activation completes.
- Guarantee that the devices can check in with the server.



Note: It is highly recommended that you do not install any unrelated software on the server machine.

4.3.4 Other Requirements

Also, if you have installed a server earlier than version 3.x (including 3.x) on the system, it is highly recommended that you uninstall this server and its dependencies (Tomcat and PostgreSQL) before installing the current server to avoid port conflict.

However, if you want to keep the earlier version of the server, you must stop its dependency, Tomcat, while installing and running the current server.

5. Deploy Theft Deterrent server on Debian

This chapter introduces the procedures to deploy the server on Debian.

The deployment steps install the download feature as part of the web service by default. If you want to use a separate download server, complete the following deployment steps and then configure the server to use the separate download server with the steps in chapter 8.

5.1 Install Dependencies

You must install the following dependencies on your Debian system before installing the server:

Dependency	Version
sudo	>=1.7
ufw	>=0.2
python	>=2.6
dialog	>=1.0

To install the dependencies, follow these steps:



Note: Connect the machine to the Internet or use the Debian CD to install the dependencies.

1. Change to root account with the following command. Input password when needed:

```
su -
```

2. Open the sources list located at `/etc/apt/sources.list` and add the following lines. Replace **[release]** with the [Debian release version](#).

```
deb http://cdn.debian.net/debian/ [release] main
deb-src http://cdn.debian.net/debian [release] main
```

3. Update the sources list with the following command:

```
apt-get update
```

4. Install **python**, **ufw**, **dialog**, and **sudo** with the following command:

```
apt-get install python ufw dialog sudo
```

5.2 Install Theft Deterrent server

Copy the server installation package (`Theft_Deterrent_server_v4.0.3010X.[version]`) to any folder in the local disk. Go to the folder and then run the following commands:

1. Change to root account and input password when needed:

```
su -
```

2. Change the file permission of the installation package:

```
chmod +x Theft_Deterrent_server_v4.0.3010X.[version]
```

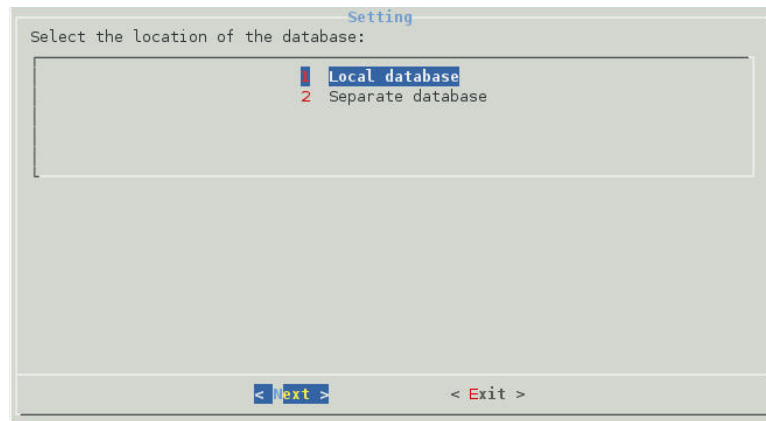
3. Run the installation package to open the install wizard:

```
./Theft_Deterrent_server_v4.0.3010X.[version] install
```

Follow these steps to deploy the server:

1. Select the language of your choice and then select **Next**. Press **Enter**.
2. Press **Enter** to accept the license agreement.
3. Select the **Local database** option and then select **Next**. Press **Enter**.

Figure 7 - Database Location

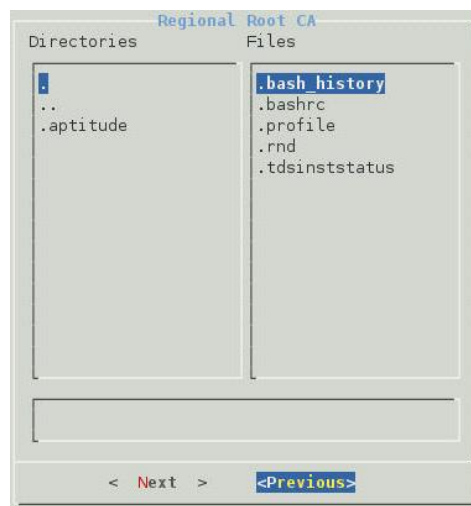


4. Set a password for the database server. Select **Next** and then press **Enter**.
5. Select a [server support mode](#) of your choice and then select **Next**. Press **Enter**.
6. If you choose to install the **Stand-alone** mode, select the Root Public Key type for your deployment on the next page.

Figure 8 - Select Root Public Key Type (Stand-alone Mode)



7. If you choose to deploy the server with **your own Root Public Key**, you must import the Root Public Key file (with the extension **.pubkey** or **.bin**) by copying the key to your local machine and then inputting the location of the key in the following window. (e.g. /opt/CmpcRoot.pubkey)

Figure 9 - Import Root Public Key (Stand-alone Mode)

Note: In the install wizard, use **Tab** or arrow keys to move between the windows. Within the directory or filename windows, use the up or down arrow keys to scroll the current selection. Use the **Space** bar to confirm the selection.

8. On the next step, set a password and email for the master admin account. Select **Next** and then press **Enter**.
9. Confirm the settings and then select **OK**. Press **Enter**.
10. Wait for the installation to complete.

Note: The password must be 8 to 30 characters in length and must contain at least one lowercase letter [a-z], uppercase letter [A-Z], number [0-9], and special character. It must not contain sequences of the same character (e.g. aa, 33, ##) or numbers that are longer than 5 characters (e.g. 12345, 67890).

To deploy the server with a separate database, contact the Intel local TME for support.

5.3 Best Practice of Performance Tuning

The default configuration of the server has limited the resource assignment, which could be a bottleneck for the server performance. To improve the performance of the server, you can tune the database service, web service, log, and download service with the **perfconfig** tool.

If your server is deployed on LAN and manages less than 5K online devices, no tuning step is required and you can skip this chapter.

Otherwise, improve server performance with the following steps:

1. Run the following commands with root privilege to start the **perfconfig** tool:

```
cd /usr/local/theftdeterrentserver
./perfconfig
```

2. Select a language of your choice.
3. Select the number of online devices that your server will manage.
4. You might also need to configure the following settings:
 - **Is your server deployed on LAN or the Internet?**
 - **Input the default download speed limit (KB/s):** Set a download limit for the local download feature. This setting will not affect any separate download server.

5. Input **1** and press **ENTER** to restart the web service.

5.4 Upgrade Theft Deterrent server

You can upgrade the server from version 4.x to a higher version. All the data and settings of the server are kept after the upgrade. Before upgrading, it is recommended that you [back up the server](#).

There are two kinds of upgrade package:

1. Upgrade only the TDserver itself without 3rd party dependency, using package named as Theft_Deterrent_server-**upgrade**_v4.0.3010X.[version] can be used for the size is much smaller than full installer package.
2. Upgrade both the TDserver and 3rd party dependency, using the installer package Theft_Deterrent_server_v4.0.3010X.[version] for the upgrade.

To upgrade a TDserver without 3rd party dependency, follow these steps:

1. Copy the latest server upgrade package (named as Theft_Deterrent_server-upgrade_v4.0.3010X.[version]) to the local disk.
2. Open the installation wizard by following the steps.

```
./Theft_Deterrent_server-upgrade_v4.0.3010X.[version] install
```

3. Select a language of your choice and accept the license agreement.
4. Then wait for the wizard to complete the upgrade.
5. Clear cache of your browser before login to server again.

To upgrade a TDserver with 3rd party dependency, follow these steps:

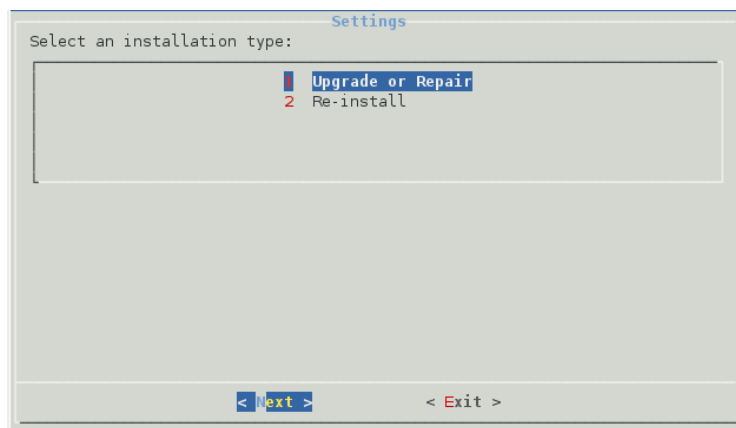
1. Copy the latest server upgrade package (named as Theft_Deterrent_server-upgrade_v4.0.3010X.[version]) to the local disk.
2. Open the installation wizard by following the steps.

```
./Theft_Deterrent_server_v4.0.3010X.[version] install
```

3. Select a language of your choice and accept the license agreement.
4. On the next page, select **Upgrade or Repair** to upgrade with keep all data.
5. Follow the installation wizard to complete the upgrade for TDserver and 3rd party dependency.
6. Clear cache of your browser before login to server again.



Note: The browser will cache old server and make the webpage display maybe distort after server upgrade.

Figure 10 - Upgrade Theft Deterrent server

5.5 Repair or Re-install Theft Deterrent server

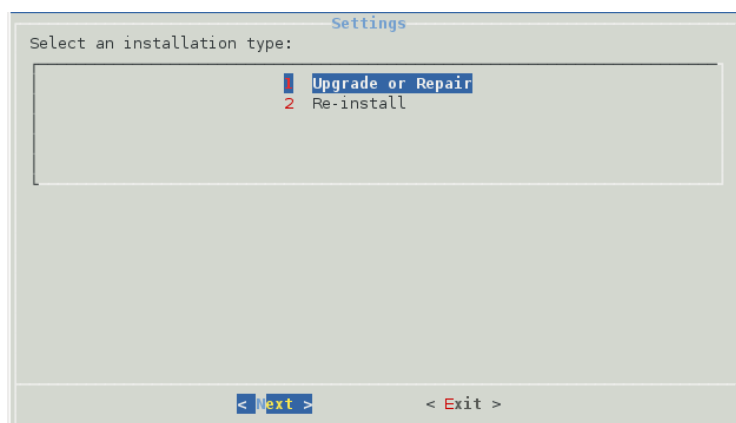
If upgrade failed, the current server may be corrupted. You can repair the server with the current installation package. And you can reinstall the server to remove the server data, settings and key files. Before repair or re-install, it is recommended that you [back up the server](#).

To repair or re-install a server, follow these steps:

1. Copy the latest serve install package (Theft_Deterrent_server_v4.0.3010X.[version]) to the local disk.
2. Open the installation wizard by following the steps in chapter 5.2.

```
./Theft_Deterrent_server_v4.0.3010X.[version] install
```

3. Select a language of your choice and accept the license agreement.
4. On the next page, select **Upgrade or Repair** to keep all data and **Re-install** to remove all data of your current server.

Figure 11 - Repair or Re-install Theft Deterrent server

5. Follow the installation wizard to complete the installation.

5.6 Uninstall Theft Deterrent server

If you want to uninstall the server, it is recommended that you [back up the server](#) before the action.



Note: Make sure that no device is managed by the server any more. Otherwise, the devices might be locked within a certain period of time.

To uninstall the server, follow these steps:

1. Go to the directory that contains the server installation package.
2. Run the following command with root privilege to uninstall the server.

```
./Theft_Deterrent_server_v4.0.3010X.[version] remove
```

6. Deploy Theft Deterrent server on Windows

This chapter introduces the procedures to deploy the server on Windows.

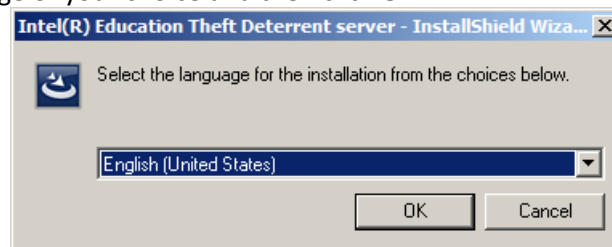
The deployment steps install the download feature as part of the web service by default. If you want to use a separate download server, complete the following deployment steps and then configure the server to use the third-party download server with the steps in chapter 8.

6.1 Install Theft Deterrent server

Copy the server installation package (Theft_Deterrent_server_v4.0.10000.[version].zip) to the local disk and then extract the installation package into a temporary folder. In the temporary folder, right-click **setup.exe** and select **Run as administrator** to open the installation wizard.

Follow these steps to deploy the server:

1. Select a language of your choice and then click **OK**.

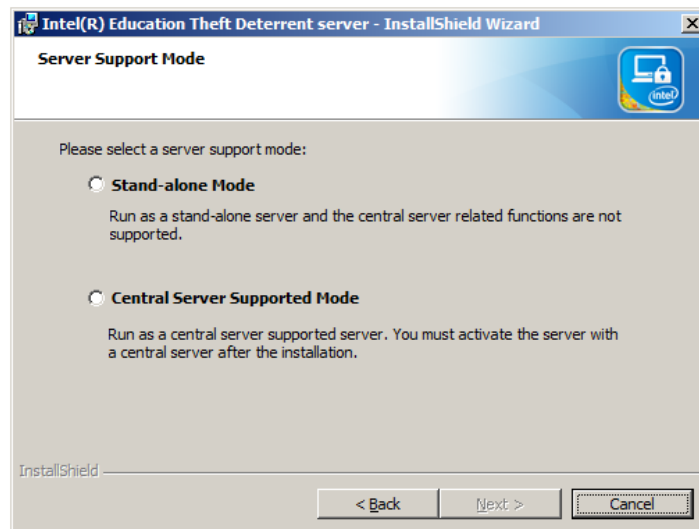


2. Accept the license agreement and then click **Next**.
3. Select **Local Database** and then click **Next**.

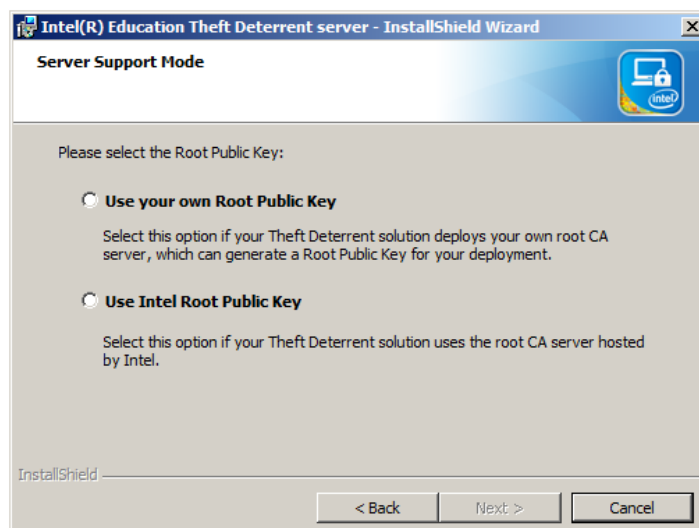
Figure 12 - Database Location



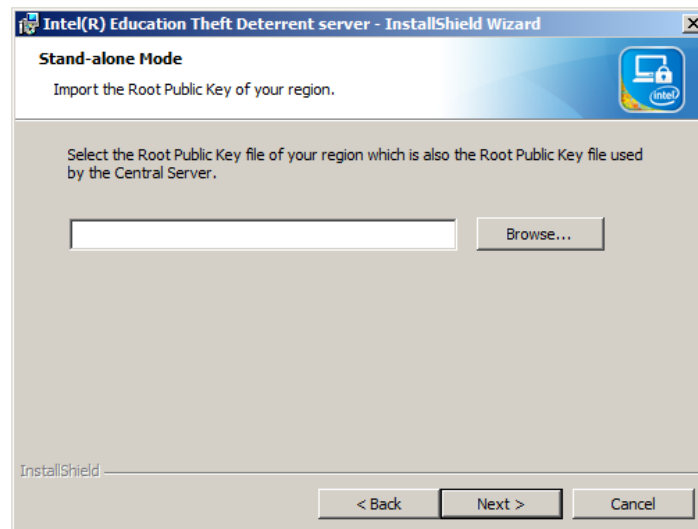
4. Set a password for the database server and then click **Next**.
5. Select a [server support mode](#) of your choice and then click **Next**.

Figure 13 - Server Support Mode

6. If you choose to install the **Stand-alone** mode, select the Root Public Key type for you deployment on the next page.

Figure 14 - Stand-alone Mode

7. If you choose to deploy the server with **your own Root Public Key**, you must import the Root Public Key file (with the extension **.pubkey** or **.bin**) by copying the key to your local machine and then browse to the location of the key. (e.g. C:\CmpcRoot.pubkey)

Figure 15 - Import Root Public Key (Stand-alone Mode)

8. On the next step, set a password and email for the master admin account and then click **Next**.
9. Confirm the settings and then click **Install**.
10. The installation will be completed in about 20 minutes.



Note: The password must be 8 to 30 characters in length and must contain at least one lowercase letter [a-z], uppercase letter [A-Z], number [0-9], and special character. It must not contain sequences of the same character (e.g. aa, 33, ##) or numbers that are longer than 5 characters (e.g. 12345, 67890).

To deploy the server with separate database, contact the Intel local TME for support.

6.2 Best Practice of Performance Tuning

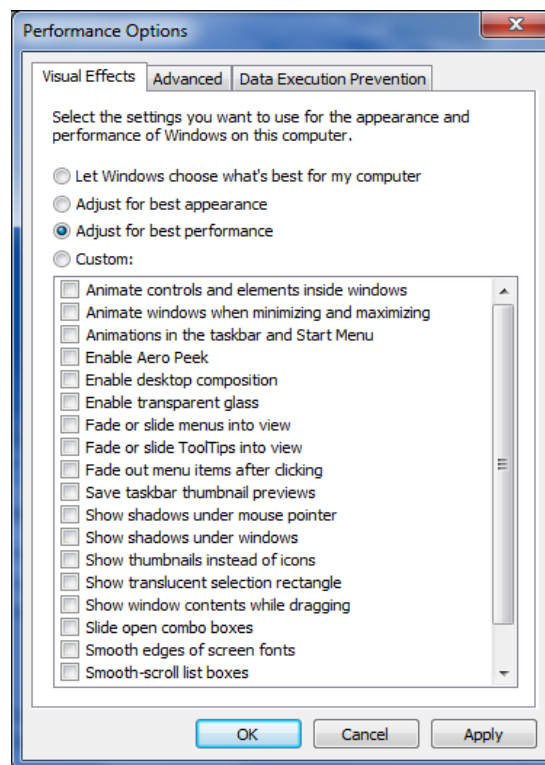
If your server is deployed on LAN, no tuning step is required and you can skip this chapter.

If your server is deployed on the Internet, improve the performance of your server with the following steps because the default configuration of the server has limited the resource assignment, which could be a performance bottleneck.

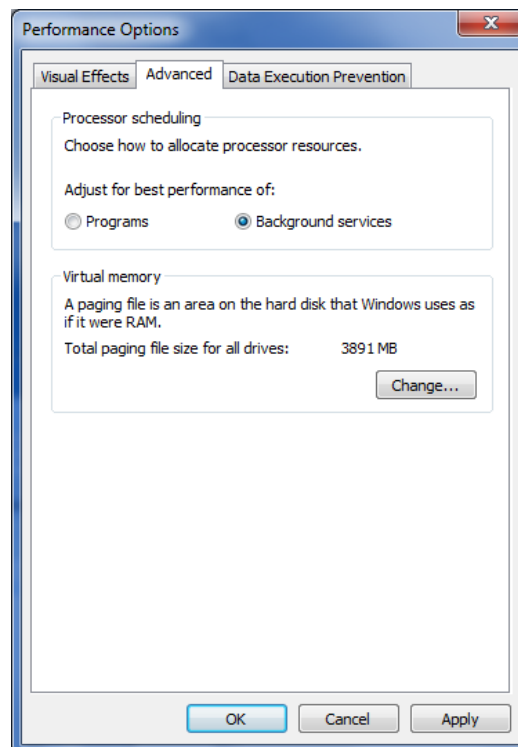
6.2.1 Common Configuration

Configure the performance options in Windows with the following steps:

1. From Windows desktop, click the **Start** menu -> **Control Panel** -> **System and Security** -> **System** -> **Advanced system settings**.
2. On the popup window, switch to the **Advanced** tab and click **Settings** in the **Performance** area.
3. In the **Visual Effects** tab, select the **Adjust for best performance** option as shown below and then click **Apply**.

Figure 16 - Configure Performance (1)

4. Switch to the **Advanced** tab, select **Background services** in the **Processor scheduling** area and then click **OK**.

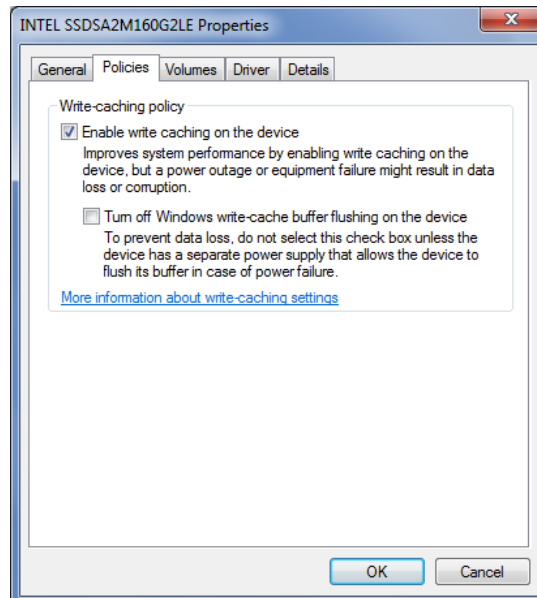
Figure 17 - Configure Performance (2)

Enable Write-caching for hard disks with the following steps:

1. From Windows desktop, click the **Start** menu-> **Control Panel** -> **Hardware** -> **Device manager**.

2. Double-click **Disk drivers** in the **Device Manager** window.
3. Right-click the hard disk device where the server is installed and select **Properties**.
4. On the popup window, click on the **Policies** tab and check **Enable write caching on the device**. Then click **OK**.

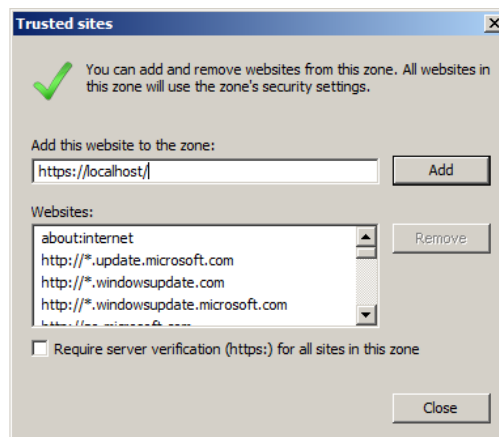
Figure 18 - Configure Performance (3)



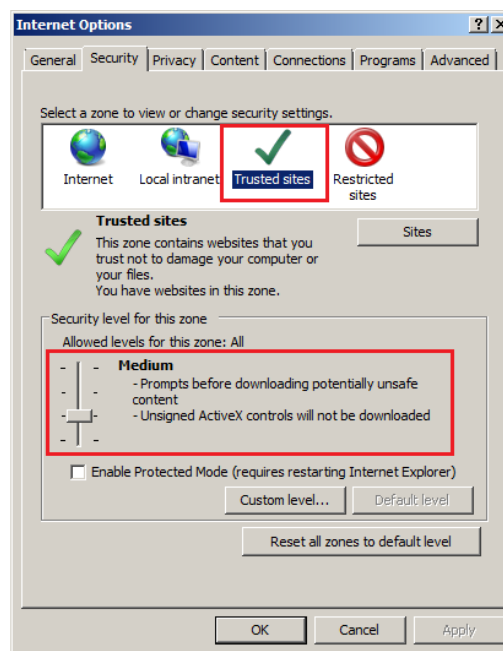
Add the server URL to **Trusted sites** with the following steps:

1. On Internet Explorer, click **Tools -> Internet Options -> Security Tab**.
2. On the **Security** page, select **Trusted Sites** and click the **Sites** button.
3. On the popup window, input <https://localhost/> and then click the **Add** button.

Figure 19 - Add Trusted Sites



4. Click **Yes** on the confirmation window. Click **Close**.
5. Make sure that the security level for **Trusted sites** is **Medium** and then click **OK**.

Figure 20 - Configure Security Level

6.2.2 Tune the Performance

The default configuration of the server has limited the resource assignment, which could be a bottleneck for the server performance. To improve the performance of the server, you can tune the database service, web service, log, and download service with the **perfconfig** tool.

If your server is deployed on LAN and manages less than 5K online devices, no tuning step is required and you can skip this chapter.

Otherwise, improve server performance with the following steps:

1. Run the following commands with admin privilege to start the **perfconfig** tool:

```
cd C:\Program Files\Intel Education Software\Theft Deterrent server\bin
```

```
call perfconfig.bat
```

2. Select a language of your choice.
3. Select the number of online devices that your server will manage.
4. You might also need to configure the following settings:
 - **Is your server deployed on LAN or the Internet?**
 - **Input the default download speed limit (KB/s):** Set a download limit for the local download feature. This setting will not affect any separate download server.
5. Input **1** and press **ENTER** to restart the server.

6.3 Upgrade Theft Deterrent server

If upgrade failed, the current server may be corrupted. You can repair the server with the current installation package. Before repair or re-install, it is recommended that you [back up the server](#).

There are two kinds of upgrade package:

3. Upgrade only the TDserver itself without 3rd party dependency, using package named as Theft_Deterrent_server-**upgrade**_v4.0.10000.[version] can be used for the size is much smaller than full installer package.
4. Upgrade both the TDserver and 3rd party dependency, using the installer package Theft_Deterrent_server_v4.0.10000.[version] for the upgrade.

To upgrade a TDserver without 3rd party dependency, follow these steps:

1. Copy the latest server upgrade package (named as Theft_Deterrent_server-upgrade_v4.0.10000.[version].zip) to the local disk then extract the installation package into a temporary folder. In the temporary folder, right-click **setup.exe** and select **Run as administrator** to open the installation wizard.
2. Select a language of your choice and accept the license agreement.
3. Then wait for the wizard to complete the installation.
4. Clear cache of your browser before login to server again.

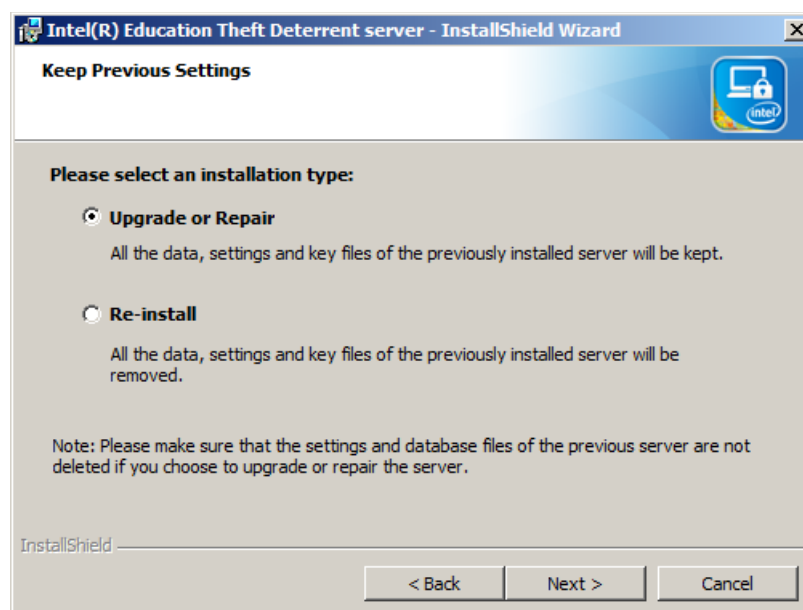
To upgrade a TDserver with 3rd party dependency, follow these steps:

1. Copy the latest server upgrade package (named as Theft_Deterrent_server-upgrade_v4.0.10000.[version]) to the local disk.
2. Open the installation wizard by following the steps.

```
./Theft_Deterrent_server_v4.0.10000.[version] install
```

3. Select a language of your choice and accept the license agreement.
4. On the next page, select **Upgrade or Repair** to upgrade with keep all data.
5. Follow the installation wizard to complete the upgrade for TDserver and 3rd party dependency.
6. Clear cache of your browser before login to server again.

Figure 21 – Upgrade Theft Deterrent server



Note: The browser will cache old server and make the webpage display maybe distort after server upgrade.

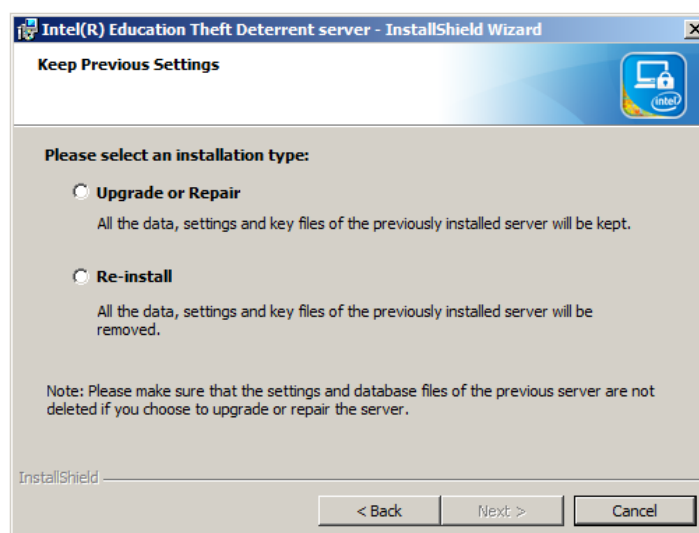
6.4 Repair or Re-install Theft Deterrent server

If upgrade failed, the current server may be corrupted. You can repair the server with the current installation package. And you can reinstall the server to remove the server data, settings and key files. Before repair or re-install, it is recommended that you [back up the server](#).

To repair or re-install a server, follow these steps:

1. Copy the latest server upgrade package (named as Theft_Deterrent_server_v4.0.10000.[version].zip) to the local disk then extract the installation package into a temporary folder. In the temporary folder, right-click **setup.exe** and select **Run as administrator** to open the installation wizard.
2. Select a language of your choice and accept the license agreement.
3. Select **Upgrade or Repair** to keep all data and **Re-install** to remove all data of your current server.

Figure 22 – Repair or re-install Theft Deterrent server



4. Follow the installation wizard to complete the installation.

6.5 Uninstall Theft Deterrent server

If you want to uninstall the server, it is recommended that you [back up the server](#) before the action.



Note: Make sure that no device is managed by the server any more. Otherwise, the devices might be locked within a certain period of time.

You can uninstall the server by using either the installation package or the **Control Panel**.

To uninstall the server with the installation package, follow these steps:

1. Open the folder that contains the installation package.
2. In the folder, right click **setup.exe** and select **Run as administrator** to open the uninstall wizard.
3. Click **Next** on the welcome page. Click **Next**.
4. Click **Remove** to uninstall the server.
5. Wait for the process to complete and then click **Finish**.
6. Reboot the system.

To uninstall the server from the **Control Panel**, follow these steps:

1. Click the **Start** menu -> **Control Panel** -> **Programs** -> **Programs and Features**.
2. Right-click **Intel(R) Education Theft Deterrent server** and select **Uninstall**.
3. Click **Yes** to confirm the action.
4. Click **Yes** to reboot the system.

7. Theft Deterrent server Pre-configurations

After server installation completes, you can use the server functionalities by accessing the server webpage with the following URL, where **[serverURL]** is the IP address or hostname of the server.

- [https://\[serverURL\]/TheftDeterrent](https://[serverURL]/TheftDeterrent)

To log in the server with the master admin account, use the following credentials:

- The username is **admin**
- The password is the one set during the installation process.

7.1 First Time Configurations

When you log in the server for the first time, you must complete certain settings before accessing the server functionalities. The settings differ according to the server support mode, which is set during the installation of the server.

Server Support Mode	First login settings
Stand-alone	<ul style="list-style-type: none">• Set up Server Name & Address• Set up Email Server
Central Server supported	<ul style="list-style-type: none">• Activate the server or reactivate the server• Set up Server Name & Address• Set up Email Server

7.1.1 Activate Theft Deterrent server

If the server is installed with the **Central Server supported** mode, you must activate or reactivate the server with the central server during first login. You can skip this chapter if the server is installed with the **Stand-alone** mode.

By activating the server with the central server, you achieve the following functionalities:

- Register the school information of the server on the central server.
- Back up the keystore and database information of the server on the central server.
- Enable the server to manage the devices pre-activated in factory.
- Enable the server to transfer devices via the central server to other servers.

Make sure that the server is connected with the central server.

If the server has never been registered or activated on the central server, follow these steps to activate the server:

1. On the **Activate Theft Deterrent server** page (**Step 1**), input all server information and the IP address of the central server.
2. Click **Register Server** and your activation request will be sent to the central server.

Figure 23 - Activate Server (1)

Activate Theft Deterrent server

Step 1: Register the information of the Theft Deterrent server to the Central Server and get the activation code.

Server name: East High School Server

Location: East Lake

Contact person: support admin

E-mail: admin@school.com

Phone number: 022-1995554444

Central Server address: 192.168.1.158 (online registration)

Only skip this step if you want to reactivate the server.

Register Server Skip

- When your request is approved by the central server admin, you will receive an activation code. The approval process might take a while and you can log out of the server during this period.
- After you receive the activation code, log in the server and click **Register Server** on the **Activate Theft Deterrent server** page (**Step 1**). You can skip this step if you did not log out the server.
- On the **Activate Theft Deterrent server** page (**Step 2**), input the activation code and the IP address of the central server. Then click **Activate Server**.

Figure 24 - Activate Server (2)

Activate Theft Deterrent server

Step2: Enter the activation code received from the Central Server to activate the Theft Deterrent server.

Activation Code: 77777777-9999-44d7-ba99-0e00e0000000

Central Server Address: 192.168.1.158 (online activation)

< Back Activate Server

- When you see the activation success message, click **OK**.

7.1.2 Reactivate Theft Deterrent server

If you had already activated a server that later crashed and its key pair are lost permanently, you can replace the crashed server by installing a new server with the **Central Server supported** mode. Then follow these steps to reactivate the server:

- Contact central server admin offline to request an activation code for reactivation.
- On the **Activate Theft Deterrent server** page (**Step 1**), click **Skip**.
- On the **Activate Theft Deterrent server** page (**Step 2**), input the activation code and the IP address of the central server. Then click **Reactivate Server**.

- When you see the reactivation success message, click **OK**.

When reactivation completes, you can manage the devices that were managed by the crashed server when the devices connect with this server.

For more information about server activation, see the Intel® Education Central Server User Manual.

7.1.3 Set up Server Name & Address

Server name

- Server name must be less than 128 characters in length.
- If the server is installed with the **Central Server supported** mode, the server name is already set during the activation process.

Server IP address/ URL

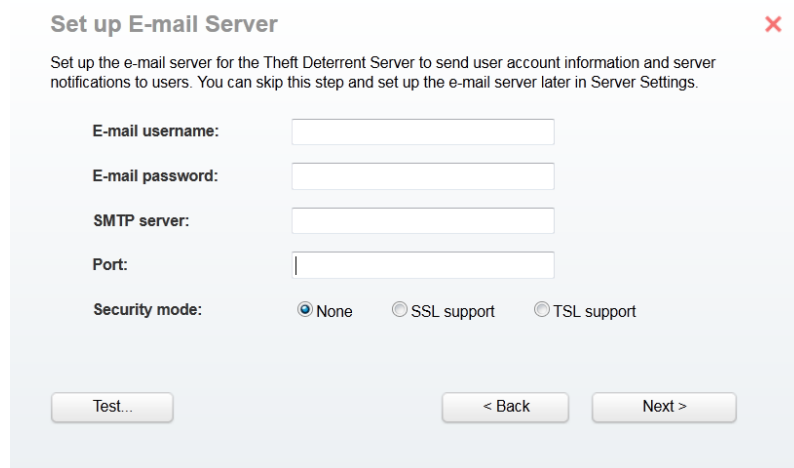
- Server address is the IP address or URL of the server machine.
- This server address will be broadcasted to the clients when the **Automatic Server Broadcast** function is turned on.

7.1.4 Set up E-mail Notification Service

You can set up the e-mail service to send user account and server information to users via e-mail. Input the following information:

- E-mail username:** the e-mail address of your e-mail account
- E-mail password:** the password of your e-mail account
- SMTP server:** the hostname of the SMTP server.
- Port:** the port number of the SMTP server.
- Security Mode:** select a security mode.

Figure 25 - Set up E-mail Notification Service



After the email service is configured correctly, the server will send out e-mails in the following cases:

<i>When to send e-mails?</i>	<i>Recipient</i>
Admin creates new user accounts	The new user
Admin resets user passwords	The user

Someone forgets his/her password and requests password reset	The person him/herself
Someone sets up the E-mail Notification function	The e-mail addresses that this person configured for the function

After you complete the first login settings, you will see the server **Home** page. You can also open the **Inventory**, **Groups & Accounts**, and **Settings** pages to access different functions.

Figure 26 - Server Tabs



7.2 Modify the Server Log Level

By default, the server is set with the **DEBUG** log level to log all precise contexts concerning its running status in case any error occurs and requires debugging.

The log levels affect the server performance as follows:

Log Level	Server Performance	Information Detail
DEBUG	Low	High
INFO	Medium	Medium
WARN	High	Low

If you are experiencing slow server performance, it is recommended that you lower the server log level with the following steps. Otherwise, you can skip this chapter.

- Open the log configure file:
 - Debian:** `/opt/TheftDeterrentserver/Site/webapps/TheftDeterrent/WEB-INF/classes/log4j.properties`
 - Windows:** `%SystemDrive%\Program Files\Intel Education Software\Theft Deterrent server\Site\webapps\TheftDeterrent\WEB-INF\classes\log4j.properties`
- Set the log level to **INFO** or **WARN** by changing a line in the configure file as follows:

log4j.logger.com.intel=INFO

or

log4j.logger.com.intel=WARN
- Restart the server:
 - Debian:** run the following command: `service theftdeterrentserver restart`
 - Windows:** click the **Start** menu -> **All Programs** -> **Intel Education Software** -> **Theft Deterrent server** -> **Start Server**.

7.3 Server Installation Directories and Log Files

While using the server, make sure that you follow these rules:

- On both Windows and Debian, do not change the access permission to the installation directories.
- On Windows, do not access the installation directories with a standard user account by inputting the administrator password when prompted by Windows User Account Control.

The installation directories of the server are as follows:

Windows:

- %SystemDrive%\Program Files\Intel Education Software\Theft Deterrent server
- %SystemDrive%\ProgramData\TheftDeterrent2

Debian:

- /opt/TheftDeterrentserver
- /etc/TheftDeterrent2

The location of the binary files and log files are as follows:

<i>Operating System</i>	<i>Linux</i>	<i>Windows</i>
Shortcut	/usr/local/theftdeterrentserver	Start menu -> Intel Education Software -> Theft Deterrent server
Log folder	/var/log/theftdeterrentserver /opt/TheftDeterrentserver/Site/logs	%systemdrive%\log\theftdeterrentserver

8. Use Separate Download Server

To use a separate download server for your server, you must first complete the deployment steps in chapter 5 or 6 and the pre-configuration steps in chapter 7. Then configure the server to use the separate download server.


You can either set up a separate download server or use an existing download services provided by a CDN operator, a cloud based download server, etc. If you want to set up your own download server, see [Configure Download Server](#).

8.1 Configure Download Server

The deployment or configuration steps of the third-party download server are beyond the scope of this document. You can contact your third-party server provider for support.

However, if you have not decided which third-party download server to use, you can install another Theft Deterrent server to function as a download server with the following steps:

1. Install another Theft Deterrent server on a machine that meets the [download server requirements](#).
2. Copy the client upgrade packages to the following location manually, according to your operating system:
 - **Windows:** C:\Program Files\Intel Education Software\Theft Deterrent server\Site\webapps\tdupdate
 - **Debian:** /opt/TheftDeterrentserver/Site/webapps/tdupdate


 **Note:** To obtain a client upgrade package, which ranges from 2MB to 10MB in size, contact the Intel local TME.

3. Connect this download server to the same network as the server.

8.2 Configure Download Feature on Theft Deterrent server

When the download server is ready, configure the server to use the download server with the following steps:

1. Log in the server and open the **Advanced** page under **Settings**.
2. Click the **Configure download server(s)** link in the **Smart Client Upgrade** area.
3. Input the following information:
 - **Server Name:** the name of the download server.
 - **URL:** the location of the upgrade packages in the download server, which must be in HTTP scheme. For example, if you use another Theft Deterrent server as the download server, the URL is `http://[DownloadServer URL]/tdupdate/`

 **Note:** This URL is provided to clients for downloading upgrade packages when the **Smart Client Upgrade** function is enabled. However, you must copy the upgrade packages to your download server manually.

- **Concurrent Download Limitation:** the maximum number of devices that can download the upgrade packages at the same time.

- **Client Speed Limitation:** the maximum network speed for a device to download the upgrade packages.

4. Click the **Save** Button.

You can configure multiple download servers. However, it is recommended that you keep the maximum number of download servers below 15.

You can select one or multiple download servers to implement the download function at the same time. The local server is the local download feature provided by default.

Note: When you add, edit, or delete a download server, the configuration takes effect only after you click the **Save** button.

Figure 27 - Configure Download Server

Click "Add Server" and fill in the information to add a download server. Click a table cell to edit the information.

Enable	Server Name	URL	Concurrent Download Limitation	Client Speed Limitation	Delete
<input type="checkbox"/>	shwde6433	Local Address	100	--	
<input checked="" type="checkbox"/>	TD Download server	http://192.168.1.100/tdupdate/	300	200 KB/s	X

Add Server

Save Cancel

For more information on how to configure the separate download server, contact your local TME for support.

9. Manually Deploy Theft Deterrent client and guardian

The client and the Theft Deterrent guardian (guardian) are Theft Deterrent components that run on devices. The client can lock and unlock devices based on the certificates received from the Theft Deterrent server while the guardian is a client protection application that restores the client if it is uninstalled or disabled.

Both components support the following operating systems:

- Windows 7 or 8
- Debian 7 32-bits
- Debian 7 64-bits
- Android

The client and guardian are usually preloaded in factory during the manufacture of the devices. If your device is not preloaded with a client or guardian, you can deploy the components manually. As a best practise, the client should be kept running at all times. Therefore, for each client deployed, you must deploy a guardian on the same device.

This chapter introduces the steps to deploy the client and guardian on devices running the Windows or Debian operating system. For all devices running the Android operating system, the client and guardian are always preloaded and thus would not require manual deployment.



Note: The device's TPM must be initialized in manufactory line before you deploy the client and guardian or the components will report error.

9.1 Deploy Theft Deterrent client and guardian on Windows

For devices running the Windows operating system, the installation package (Theft_Deterrent_client_guardian_[version].zip) supports two deployment methods:

- Command line, which Installs client and guardian together.
- Install wizards, which Install client and guardian separately.

For large deployments, it is recommended that you use the command line to install the client and guardian. Such deployment provides efficiency because the two components are deployed together while no user interaction is required during the process.

If you are deploying on a single device, you can use the install wizards, which are more user-friendly.

9.1.1 Prerequisite

Before you install the client, you must install **.Net 3.5 SP1** on the Windows operating system if not already installed.

- For Windows 7, you can install **.Net 3.5 SP1** either by turning on the feature in **Windows Feature** or by downloading and installing the package from [Microsoft website](#).
- For Windows 8, download and install **.Net 3.5 SP1** from [Microsoft website](#).

9.1.2 Install with Command Line

To install the client and guardian with command line, follow these steps:

1. Extract the installation package (Theft_Deterrent_client_guardian_*[version]*.zip) into a temporary folder, for example, C:\TD.
2. Click the **Start** menu -> **Accessories** -> right-click **Command Prompt** -> select **Run as administrator**.
3. Go to the **bin** folder in the temporary folder with a command such as the following:

```
cd c:\TD\bin
```

4. Run **install.bat**.

```
install.bat
```

The device will restart automatically once the installation completes. The client displays the language of the operating system

If the display language of the operating system is English, Portuguese, Turkish, or Spanish, the client follows the same display language. Otherwise, the client is displayed in English.

9.1.3 Install with Install Wizard

To install the client with the install wizard, follow these steps:

1. Extract the installation package (Theft_Deterrent_client_guardian_*[version]*.zip) into a temporary folder.
2. In the temporary folder, open the **agent** folder under **bin**, right-click **setup.exe**, and select **Run as administrator** to open the installation wizard.
3. Select a language of your choice and then click **OK**.
4. Click **Next** on the welcome page.
5. Set the protection password for the client and then click **Next**. If you do not want to set the password, leave the password field blank, click **Next** and then click **OK** on the confirmation window.
6. Click **Next** to start the installation. This might take a few minutes.
7. When the installation completes, click **Finish**.
8. Click **Yes** on the popup window to reboot the system.



Note: The protection password must be 6 to 30 characters in length and must contain at least one uppercase letter [A-Z], one lowercase letter [a-z], one number [0-9], and one special character. If you set up the protection password during the installation, the password is required when you change the client settings or uninstall the client. The protection password can be reset by the server admin.

To install the guardian with the install wizard, follow these steps:

1. Extract the installation package (Theft_Deterrent_client_guardian_*[version]*.zip) into a temporary folder.
2. In the temporary folder, open the **guardian** folder under **bin**, right-click **setup.exe**, and select **Run as administrator** to open the installation wizard.
3. Select a language of your choice and then click **OK**.
4. Click **Next** on the welcome page.

5. Set the protection password for the client and then click **Next**. If you do not want to set the password, leave the password field blank, click **Next** and then click **OK** on the confirmation window.
6. Click **Next** to start the installation. This might take a few minutes.
7. When the installation completes, click **Finish**.
8. Click **Yes** on the popup window to reboot the system.



Note: The protection password must be 6 to 30 characters in length and must contain at least one uppercase letter [A-Z], one lowercase letter [a-z], one number [0-9], and one special character. This protection password will replace the password set during the client installation.

9.2 Deploy Theft Deterrent client and guardian on Debian

9.2.1 Install Dependency

You must install **dbus** on your Debian 7 operating system if not already installed. To install **dbus**, follow these steps:



Note: Connect the machine to the Internet or use the Debian CD.

1. Change to root account with the following command. Input password when needed:

```
su -
```

2. Install **dbus** with the following command:

```
apt-get install dbus wireless-tools dmidecode
```

9.2.2 Install Theft Deterrent client and guardian with full package

If you have the release package named as Theft_Deterrent_client_guardian_[version].tar.gz, follow these steps to install:

Copy the server installation packages (Theft_Deterrent_client_guardian_[version].tar.gz) to any folder in the local disk. Go to the folder and then run the following commands with root privilege:

1. Change to root account with the following command. Input password when needed:

```
su -
```

2. Extract the installation package into a temporary folder, for example, /tmp, with a command such as the following:

```
tar -zxvf install.tar.gz -C /tmp
```

3. Go to the **bin** folder in the temporary folder:

```
cd /tmp/bin
```

4. Run the installation script:

```
chmod a+x install.sh  
./install.sh [Language]
```

Replace **[language]** with one of the following values to assign a display language for the client. The default display language is English.

9.2.3 Install Theft Deterrent client and guardian with separately package

If you have 3 separately release package, follow these steps to install:

1. Copy the three installation packages to any folder in. (e.g., /tmp/) :
 - **Theft_Deterrent_client_[version].zip**
 - **Theft_Deterrent_guardian_[version].zip**
 - **theftdeterrentclient-lib_[version].deb**
2. Change to root account with the following command. Input password when needed:

```
su -
```

3. Go to the folder containing the installation package. For example,

```
cd /tmp
```

4. Install client dependence libraries:

```
dpkg -i theftdeterrentclient-lib_[version].deb
```

5. Unzip client and Install client with specific language:

```
unzip Theft_Deterrent_client_[version].zip  
./Theft_Deterrent_client_[version] install [Language]
```

6. Unzip the guardian and Install guardian:

```
unzip Theft_Deterrent_guardian_[version].zip  
./Theft_Deterrent_guardian_[version] install
```

Note: [language] table refer to below:

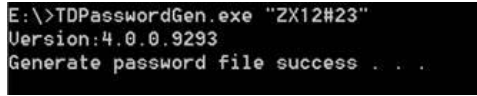
Values	Language
en-US	English
pt-BR	Portuguese
tr-TR	Turkish
es-MX	Spanish

After installation completes, the client is opened automatically.

9.3 Pre-set server address and address modify protection password

The server address can be preset in master image, so all the client will have the server address before it shipped out to end customer.

A password to protect the server address being changed can be preset in the master image as well. This password will be reset to the protection password in server setting once after the client connects with the server.


Item	Windows method	Linux method	Android method
Server address	In Master image: edit the address and Save.		A file named as tdip.txt under sdcard/
Address protection password	Set during install process	<ol style="list-style-type: none"> 1. Generate a password encryption file - passwordPro.ini  2. Copy the passwordPro.ini under the client install path. 	

9.4 Open Theft Deterrent client



The client and guardian are loaded automatically at system start-up. You can open the client from either the client tray icon or the shortcut according to your operating system. For more information on how to use the client, see the Intel® Education Theft Deterrent client User Manual.

9.4.1 Open Theft Deterrent client on Windows

If your operating system is Windows 7, you can open the client with either of the following methods:

- Click the Theft Deterrent client application icon  on the desktop.
- Right-click the client tray icon and select **Open Theft Deterrent client**.

If your operating system is Windows 8, you can open the client with one of the following methods:

- Click the Theft Deterrent client application icon  on the Start screen.
- Click the Theft Deterrent client application icon  on the desktop.
- Right-click the client tray icon on the desktop and select **Open Theft Deterrent client**.

If the client is in **Inactive** status, right-click the client tray icon on the desktop and select **Help** for instructions on how to activate the client.

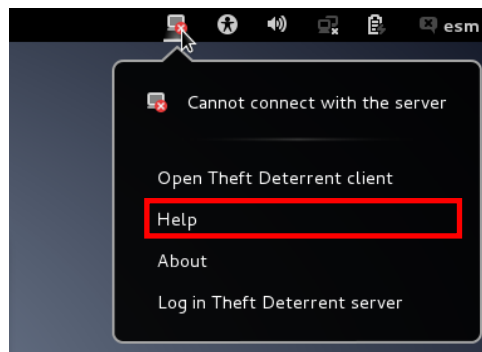
Figure 28 – Client Inactive Tray Icon (Windows)



9.4.2 Open Theft Deterrent client on Debian

If your operating system is Debian 7, you can open the client by clicking the client tray icon on the upper-right corner of the desktop. If the client is in **Inactive** status, right-click the tray icon and select **Help** for instructions on how to activate the client.

Figure 29 – Client Inactive Tray Icon



Note: The client tray icon is only supported in GNOME 3.4 or above.

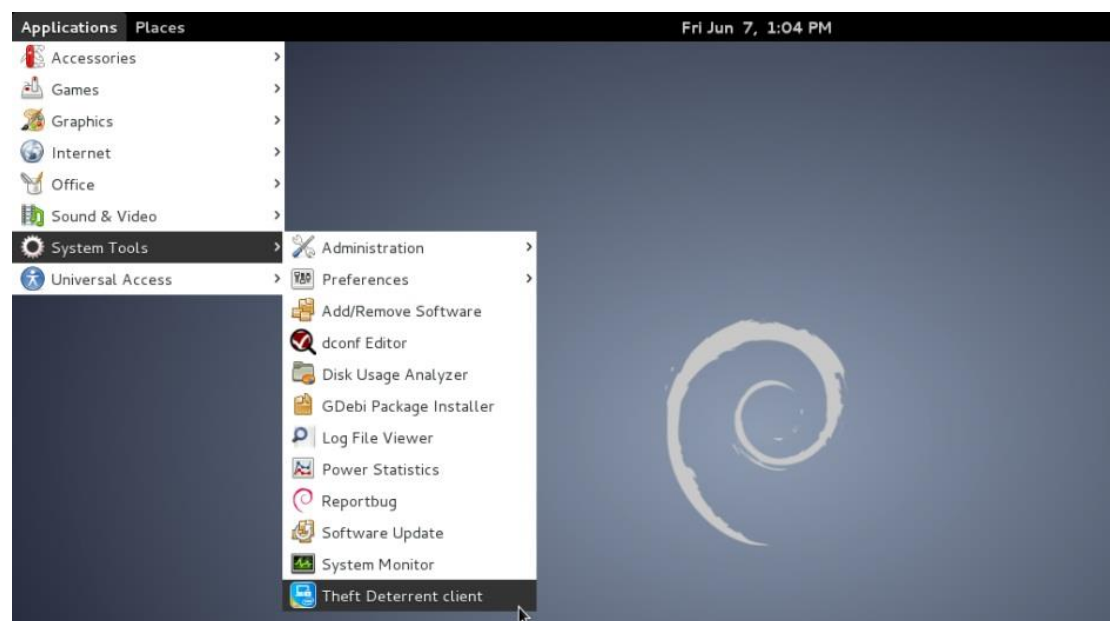
Also, if your Debian 7 displays the GNOME desktop, you can open the client by clicking **Applications -> All -> the Theft Deterrent client icon**.

Figure 30 - Shortcut on GNOME



If your Debian 7 displays the GNOME Classic desktop, you can open the client by clicking **Applications -> System Tools -> Theft Deterrent client**.

Figure 31 - Shortcut on GNOME Classic



9.5 Installation Directories and Log Files

The installation directories of the client and guardian are as follows:

Operating system	Component	Installation Directory
Windows 7 or 8 32-bits	Client	C:\Program Files\Intel Education Software\Theft Deterrent client\
	Guardian	C:\Program Files\Intel Education Software\Theft Deterrent guardian\
Windows 7 or 8 64-bits	Client	C:\Program Files (x86)\Intel Education Software\Theft Deterrent client\
	Guardian	C:\Program Files (x86)\Intel Education Software\Theft Deterrent guardian\
Debian 7	Client	/opt/TheftDeterrentclient/client/
	Guardian	/opt/TheftDeterrentclient/guardian/
Android	Client	/data/data/com.intel.cmpc.td.agent/
	Guardian	/data/data/com.intel.cmpc.td.guardian.service/

The location of the log files are as follows:

Operating system	Log
Windows 7 or 8	C:\ProgramData\Intel\TheftDeterrent
Debian 7	/var/theftdeterrent /opt/TheftDeterrentclient/client/Theft_Deterrent_client.autorun.log
Android	/data/data/com.intel.cmpc.td.agent/agent.log



Note: For devices running Android, it is recommended that you install the **Android Debug Bridge (adb)** to access the log files. For example, you can copy the log files to another directory with the following command:

```
adb pull /data/data/com.intel.cmpc.td.agent/agent.log
```

For more information about **adb**, see [Android Debug Bridge](#).

10. Troubleshooting

10.1 Theft Deterrent server Installation Failed

If the installation of the server failed, the install wizard displays an error message. Follow the solutions in this table according to the error message displayed.

Error message	Solution
Environment variables not found.	Your installation package might be corrupted. Please contact the designated support personnel.
Installer files are missing.	
Installer is missing or incorrect.	
Failed to write in installer file.	
Installer file copying failed.	
Installer file removing failed.	
Deploying failed.	
SSL key creating failed.	
Webserver register failed.	
Database register failed.	
Broadcast register failed.	
Database setting failed.	
Socket Connecting failed. Please make sure that no database management tool is connected to the database.	Disconnect any database management tool from the database server.

For more details about the installation error, check the log files in the following location:

- On Debian: /var/log/theftdeterrentserver/install
- On Windows: %systemdrive%\log\theftdeterrentserver\install

11. FAQ

1. How do I start, stop, and restart the server as well as check server status?

Answer: The steps differ according to the server operating system:

- **Windows:** Click **Start** menu -> **All Programs** -> **Intel Education Software-> Theft Deterrent server** -> click **Start Server**, **Stop Server** or **Check Server Status**.
- **Debian:** Run the following commands with root privilege:

```
service theftdeterrentserver start
service theftdeterrentserver stop
service theftdeterrentserver restart
service theftdeterrentserver status
```

Note: In Windows, if the server is running, you can restart the server by clicking the **Start Server** option. If the server is installed with a separate database, make sure that you run the command on both the web server and the database server.

2. What do I do if the server webpages are distorted?

Answer: First of all, make sure that you are using a web browser supported by the server:

- Firefox
- Chrome
- Internet Explorer 8 or above

Also, it is recommended that you clear the cache, cookies and history in your browser regularly.

3. Why does the client version 2.x keeps rebooting the device after connecting with the server?

Answer: The issue might be caused by either of the following reasons:

- The client is connected with and approved by a wrong server. To solve the issue, modify the URL in the client connection settings to connect the client to its related server.
- The system time on the device is earlier than that on the server. To solve the issue, synchronize the system time between the device and the server, delete the **CMPC TDS SN.xxxxx** certificate in your web browser and connect the device with the server again.

4. Why does the client version 2.x keeps receiving a message asking to install SSL certificate?

Answer: For clients with version earlier than 4.x, user must first install the CA certificate by accepting the install message before the client can be activated by the server. However, if the system time of the device is earlier than that on the server, the CA certificate cannot be installed correctly and the client will keep receiving the install message.

To solve the issue, synchronize the system time between the device and the server.

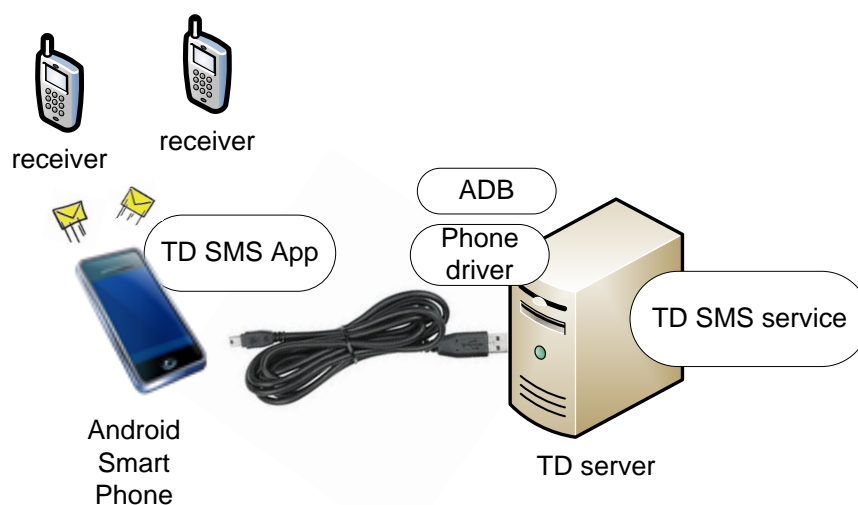
5. What is the broadcast service?

Answer: The broadcast service is the server component that performs the **Automatic Server Broadcast**, which functions only on LAN.

In the current version of the server, the web service and the broadcast service are always installed on the same machine and no configuration is required for the broadcast service during deployment. Therefore, this service is not mentioned in the server overview.

6. How to configure the TD SMS feature?

Answer: TD SMS feature is applied to send TD short messages to receivers through an Android phone connected to TD server.



To configure the SMS feature, at first, you need to complete the following installations on the server and Android phone sides respectively:

- **Server side**
 - **TD SMS service:** It will be pre-installed in the server by the TD server installer package.
 - **ADB (Android ADB service):** For Windows, the ADB will be pre-installed in the server by the TD server installer package.
 - **Phone driver:** It needs to be downloaded from the phone webpage according to the specific phone type.
- **Android phone side**
 - **TD SMS App:** It needs to be installed and launched in the Android phone to display a PIN code in order to identify the phone.

Then, follow these steps to complete the configuration of the SMS feature:

- Connect the server and the Android phone with a USB cable.
- Log in the server webpage, and go to **Settings->General->SMS Notification** to input the PIN code shown by TD SMS App and set receiver's phone number and the frequency of notification, then click the **Save** button.

7. Will I lose all server data when I uninstall the server?

Answer: When you uninstall the server with the steps in chapter 5.6 or 6.5, all the data and settings of the server are not removed from the machine. Therefore, you can restore the data and settings with the upgrade steps when you install a new server on the machine.

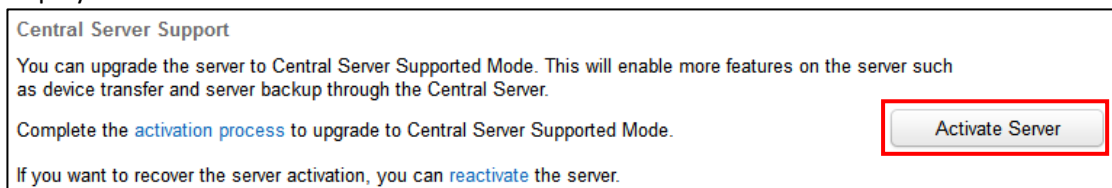
8. Can I upgrade from my server 3.x to a server 4.x in another language? For example, from a server 3.x in Spanish to a server 4.x in English.

Answer: Yes. By following the upgrade steps in chapter **Error! Reference source not found.**, you can upgrade your server 3.x to server 4.x regardless of the server display language. The server 4.x supports 4 displays languages: English, Spanish, Portuguese, and Turkish. You can change the display language on server 4.x webpage according to your needs.

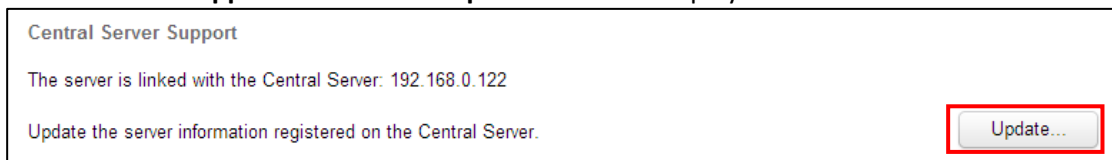
9. How do I find out the server support mode of my server?

Answer: During the deployment of the server, either of following server support mode is selected: **Stand-alone** or **Central Server supported** mode. To find out the server support mode, open the **Advanced** page under **Settings** and check the **Central Server Support** area.

- **Stand-alone** mode with Intel Root Public Key: the webpage does not contain such an area.
- **Stand-alone** mode with your own Root Public Key: the **Activate Server** button is displayed as follows:



- **Central Server supported** mode: the **Update** button is displayed as follows:



10. How do I find the version of the server?

Answer: The server version number is displayed at the bottom of the server webpage.

11. How do I find the version of the client?

Answer: Open the client tray manual from the client tray icon and click **About**. The client version number is displayed on the popup window.

12. Appendix

12.1 Choose Root Key Pair

Although Intel hosts a root CA server for external usage, it is strongly recommended that you deploy your own root CA server, which can support a central server for your Theft Deterrent solution.

Also, by running your own root CA server, you will have full control of your Theft Deterrent solution. You will be responsible for the management of your own root CA server instead of interacting with the Intel root CA server admin.


12.2 Choose Server Support Mode

The server supports two modes:

- **Stand-alone** mode
- **Central Server supported** mode


While the **Stand-alone** mode contains two options:

- Deploy with your own Root Public Key (Import the Root Public Key to the server during deployment)
- Deploy with the Intel Root Public Key (No importing step required)

 **Note:** The Root Public Key is generated by the root CA server. For more information, see the Intel® Education Theft Deterrent Root CA Server User Manual.

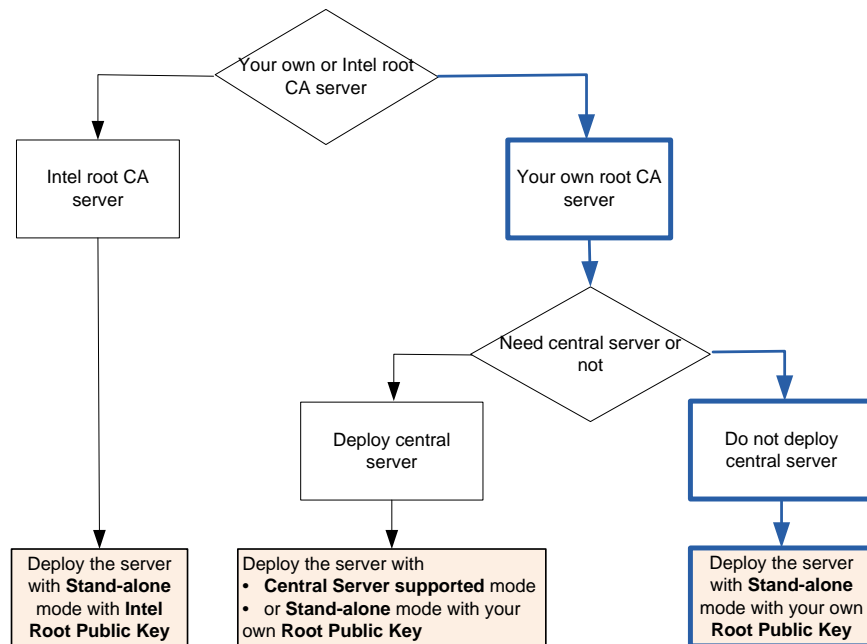
See the following table for more information about the server modes.

<i>Server Support Mode</i>	<i>Root Public Key</i>	<i>Theft Deterrent Components</i>	<i>Descriptions</i>
Stand-alone	Deploy with the Intel Root Public Key	Intel root CA server	<ul style="list-style-type: none"> • No server activation is required after the installation. • Cannot upgrade to other modes.
	Deploy with your own Root Public Key	Your own root CA server & (Optional) central server	<ul style="list-style-type: none"> • You can use the server without activation. • You can activate the server. (The server is transformed to the Central Server supported mode)
Central Server supported		Your own root CA server & central server	<ul style="list-style-type: none"> • You must activate the server after the installation.

 **Note:** Server activation is the process of registering the server information on the central server to enhance the server function.

You must choose a mode for your server during deployment according to the deployment scenario of your Theft Deterrent solution:

Figure 32 - Choose Server Support Mode



Once deployment completes, you cannot change the Root Public Key used in the Theft Deterrent solution. Make sure that you deployed the server with the correct mode before you connect any device to the server.

12.3 How to Understand the Network Stability

You can understand the network stability through the network latency. Connect a test machine to the network to stand for the server and ping a URL or IP address, such as a device IP, with the following command.

```
ping [URL]
```

The result should include a series of numbers representing the communication delay, which looks as follows:

Figure 33 - Check Network Latency

```
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=41ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128
Reply from 192.168.1.2: bytes=32 time=3ms TTL=128
Reply from 192.168.1.2: bytes=32 time=2ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 41ms, Average = 12ms
```

Find the average round trip times, which is an approximate value for the network latency.

Usage the latency should be smaller than 100ms. If the network latency always bigger than 300ms, it mean your network is quite stable.

12.4 How to Calculate the Required Network Bandwidth

Once powered on, devices will send heartbeat requests to the server regularly (10 minutes by default). In general, the device will send 2.5K bytes to the server, and receive more than 3.3K bytes from the server during each heartbeat.

However, because the devices will not send heartbeat requests simultaneously, you must estimate the peak times of the heartbeat requests to calculate the required network bandwidth.

- Peak times = peak requests / average requests

In general, the minimal peak times is 2, but it is recommend that you use 4.

The network bandwidth required at school for devices to connect with the server:

- Download bandwidth (Mbps) = $\frac{\text{online devices}}{\text{heartbeat interval}} * \text{device download rate} * \text{peak times} * 8$
- Upload bandwidth (Mbps) = $\frac{\text{online devices}}{\text{heartbeat interval}} * \text{device upload rate} * \text{peak times} * 8$

You can set device download rate = 3.3K bytes/s and device upload rate = 2.5K bytes/s.

The network bandwidth required for the web server:

- Download bandwidth (Mbps) = $\frac{\text{online devices}}{\text{heartbeat interval}} * \text{server download rate} * \text{peak times} * 8$
- Upload bandwidth (Mbps) = $\frac{\text{online devices}}{\text{heartbeat interval}} * \text{server upload rate} * \text{peak times} * 8$

You can set server download rate = 2.5K bytes/s and server upload rate = 3.3K bytes/s.

The network bandwidth required for the download server:

$$\text{Network bandwidth (Mbps)} = \frac{\text{upgrade file} * \text{number of devices}}{3600 * \text{download hours per day} * \text{download days}} * \frac{8}{\text{valid bandwidth usage}}$$

For example, the upgrade file for the client is about 6.5MB in general. If the devices are powered on 8 hours a day, 100K devices try to download the upgrade file in 7 days, and only 60% bandwidth usage is valid, then the required network bandwidth is as follows:

$$\frac{6.5 * 100000}{3600 * 8 * 7} * \frac{8}{60\%} = 43Mbps$$

In general, the more devices, the more valid bandwidth usage. It is recommended that set devices to complete the download in 7 to 14 days.

12.5 How to Improve the Download Performance

The download server sends upgrade packages to devices to fix bugs or update client features. The upgrade packages are generally larger than 6.5MB and therefore the download server will require large bandwidth for many devices to download the packages simultaneously.

You can improve the download performance of your server with one or several of the following methods to reduce the bandwidth requirements.

- **Set up several download servers**

For example, if devices use two ISPs, A and B, to connect with the server, it would be too costly to put the download server into an Internet data centers (IDC) that has good connection to both ISPs. In such cases, you can set up download servers in both ISP A and ISP B.

- **Use Content Delivery Network (CDN) or cloud based download server**

Because client upgrade occurs only occasionally, you can use a CDN service or cloud based download server instead of setting up your own download server. For more information, please contract CDN or cloud service provider.

- **Set the HTTP proxy in the school**

If the schools have HTTP proxy, you can configure the devices to use the proxy, which saves download bandwidth and time.

12.6 How to Back up Theft Deterrent server

To back up the server, follow these steps:

1. [Log on the server](#) and open the **Advanced** page under **Settings**.



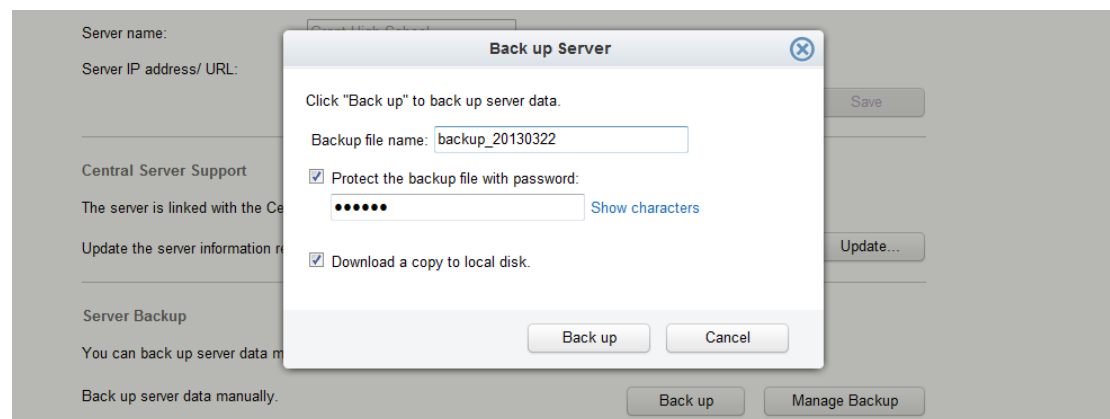
Note: You must complete the [pre-configuration steps](#) before you can access the **Advanced** page.

2. Click the **Back up** button.
3. To protect the backup files with password, select the option and input a password.
4. To save a copy of the backup file to local disk, select the option.
5. Click **Back up**.
6. If you chose to save a copy, select a location and save the file.



Note: The password must be 6 to 30 characters in length. This password will be required when you restore the server.

Figure 34 - Back up the server



12.7 How to offline Transfer Devices to Theft Deterrent server 4.x

To offline transfer devices from an old server, version earlier than 3.x (including 3.x), to a new server (version 4.x) without central server, obtain the **KeyManagement** tool from your local TME and then follow these steps:

On the new server:

1. Log in the new server and click **Export** on the **Security** page under **Settings** to export the server Public Key (**Pub_Key.bin**) to a USB disk.

On the old server:

2. Create a temporary folder named KeyMigrate. Copy the Public Key exported in step 1 and the **KeyManagement** tool to the folder.
3. Go to the folder and run the following command with root privilege and a pre-activated package named **tcopp_XXXXXXXXXXXXXXXXXXXXX_XXXXXXXXXXXXXXXXXXXXX.bin** will be generated in the folder:

```
java -jar KeyManagement.jar -a -b Pub_Key.bin
```

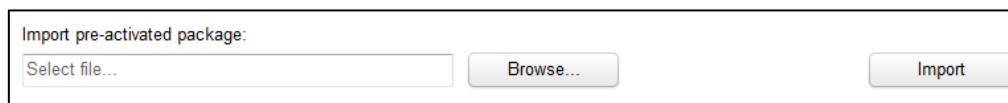
Figure 35 - Run KeyManagement Tool

```
root@debian:/home/matrix/Desktop# cd KeyMigrate/
root@debian:/home/matrix/Desktop/KeyMigrate# java -jar KeyManagement.jar -a -b Pub_Key.bin
Pre-activated packet saved in file tcopp_1c6f6adca5f1d56886d6_c641af646f9aa64c67a6.bin
```

On the new server:

4. Log in the new server and open the **Security** page under **Settings**. Browse to the pre-activated package and click **Import**.

Figure 36 - Import Pre-activated Package



Import pre-activated package:

Select file...

On the devices:

5. Right-click the client tray icon and select **Settings**.
6. On the client window, click **Edit** -> input password if required -> change **Theft Deterrent Server Address** to the address of the new server -> click **OK**.

On the new server:

7. After a while, a **Pending Approvals** tab appears under **Inventory**. Select the devices and click **Approve Device**.



Note: The device records are displayed in orange to notify users that the devices are installed with a client of earlier versions.

8. After the devices reboot and connect to the server again, the device records are moved to the **Device Management** page under **Inventory**. You can now manage the devices with the new server.