Intel® Education

Theft Deterrent

Deployment Guide

December 2014

Legal Notices

Table of Contents

List of Figures

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

Abbreviation	*Description*
server	Theft Deterrent server
client	Theft Deterrent client

1.2.2 Terms

Term	*Description*
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

Revision	*Date*	*Comment*
0.61	2013/9	Add usage for server upgrade package and add re-install server section. Update the migrate tool usage

1.4 Reference Document

Document	*Date*
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

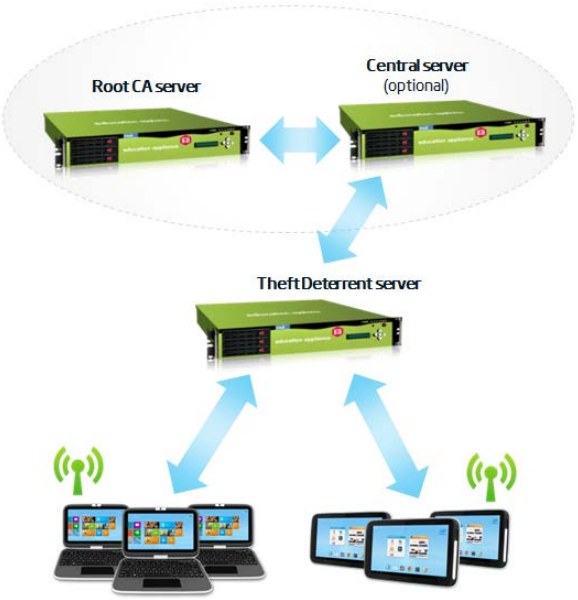
2. Theft Deterrent Overview

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:

Deployment Options	*Recommended Option*	
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:

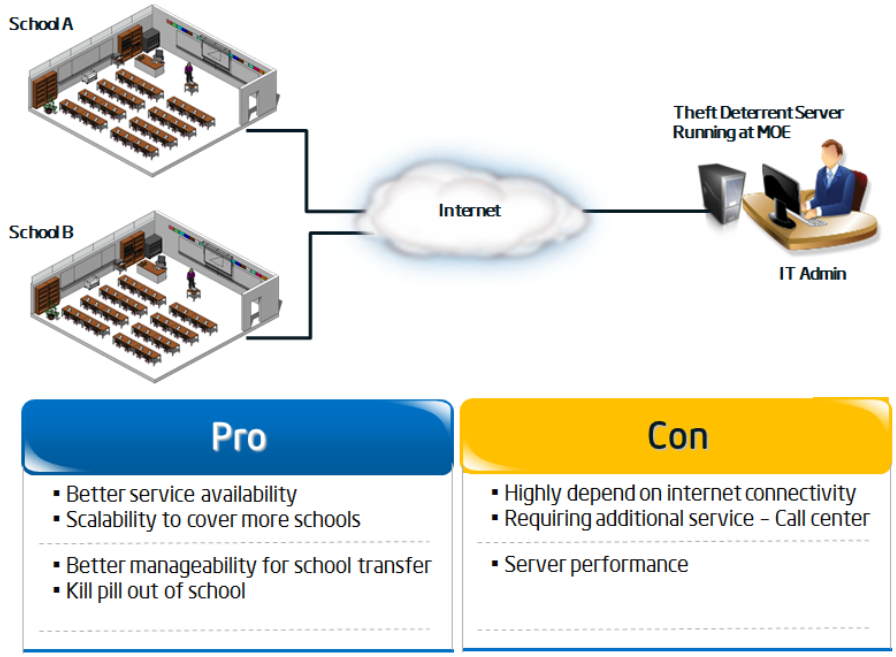
Deployment Configurations	*Descriptions*
Root key pair	Root CA server generates root key pair, trusted by every client that it manages. You can choose to deploy your own root CA server to generate your own root key pair or use the key pair from Intel.
Central server	Central server enables additional 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:

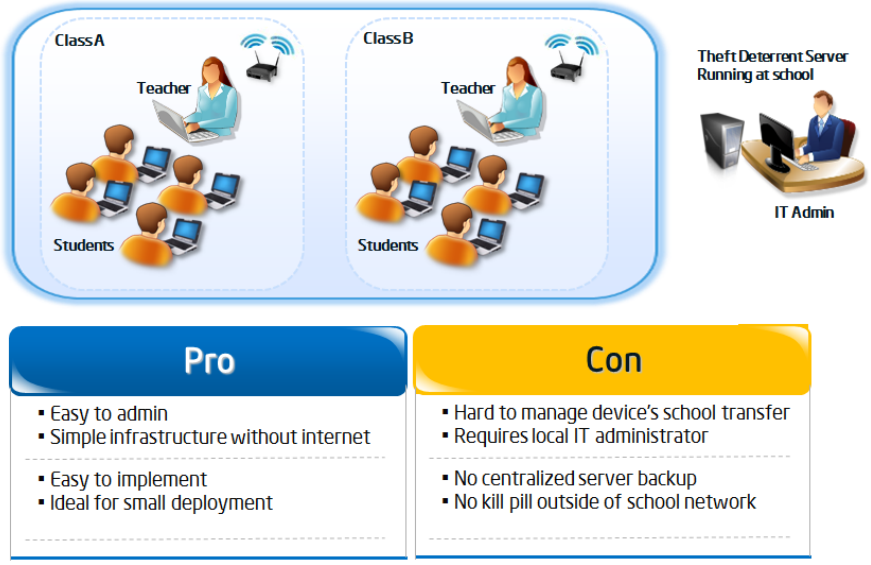
Deployment Configurations	*Configured Settings*
Root key pair	Your own root key pair
Central server	No central server
Server support mode	**Stand-alone** mode with your own Root Public Key

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



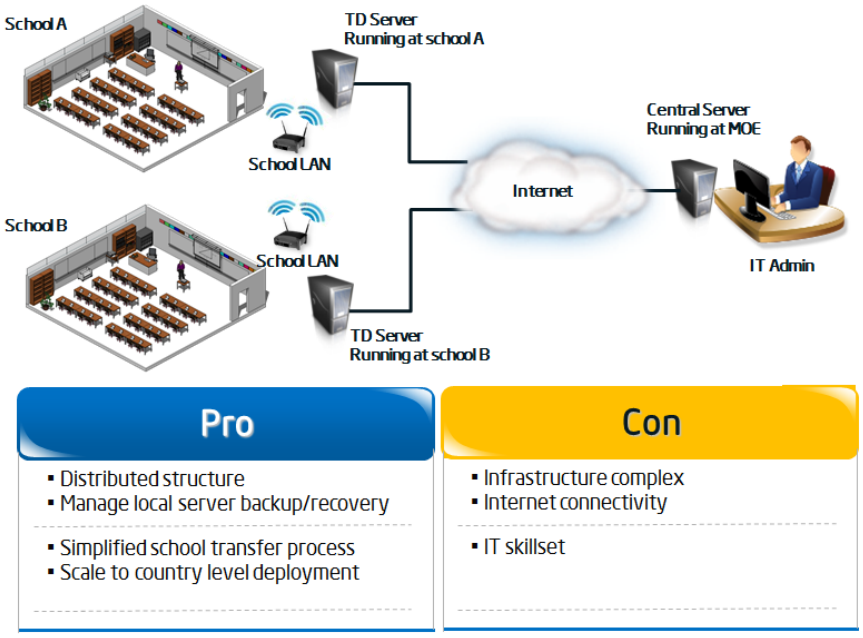
The network required for this architecture is LAN. The deployment options selected for this architecture is as follows:

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:

Deployment Configurations	*Configured Settings*
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.

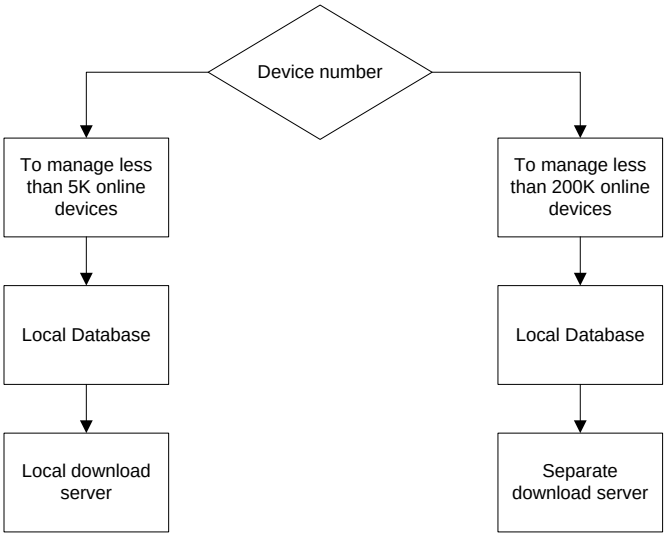
3.2 Choose Database and Download Server Locations

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:

Deployment Options	*Descriptions*
Database hosting	Database is created during server installation. You can choose to have the database created in the same server machine or on 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 on 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.

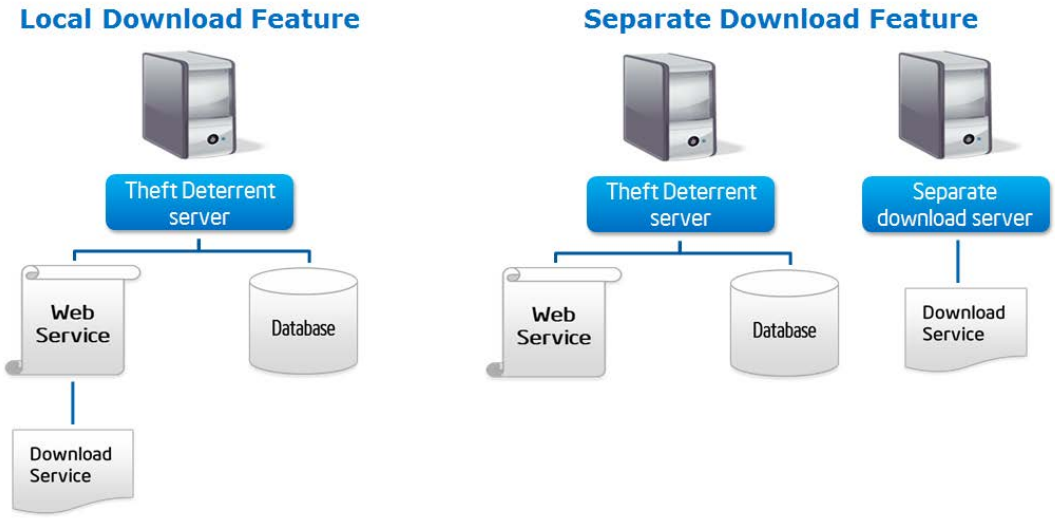
In general, it is recommended that you deploy the server with a local database unless your server is required to manage more than 200K online devices, in which case contact the Intel local TME for support.

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 9.

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:

Online devices	*Requirement*	*Recommended configuration*	*Minimal configuration*
< 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 congest 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 <= 300ms, the server requirements are displayed in the following table. If your network latency > 300ms, contact your local TME for support.

Online devices	*Requirement*	*Recommended configuration*	*Minimal configuration*
< 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	35	18

	(Mbps)		

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

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 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 9.

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]
```

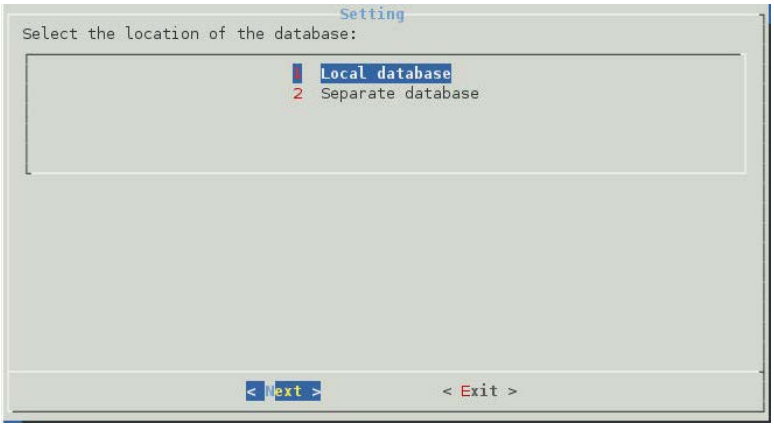
3. Run the installation package to open the install wizard:

```
./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

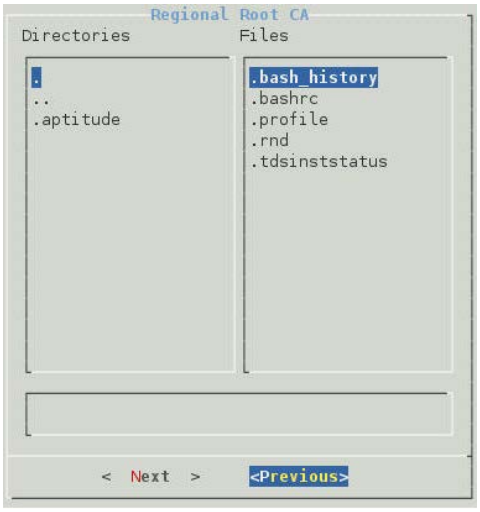


4. Set a password for the database server. Select **Next** and then press **Enter**.
5. Select a server support mode of your choice and then select **Next**. Press **Enter**.
6. If you choose to install the **Stand-alone** mode, select the Root Public Key type for you deployment on the next page.

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.

To upgrade a server, 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 installation.
5. 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.

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.

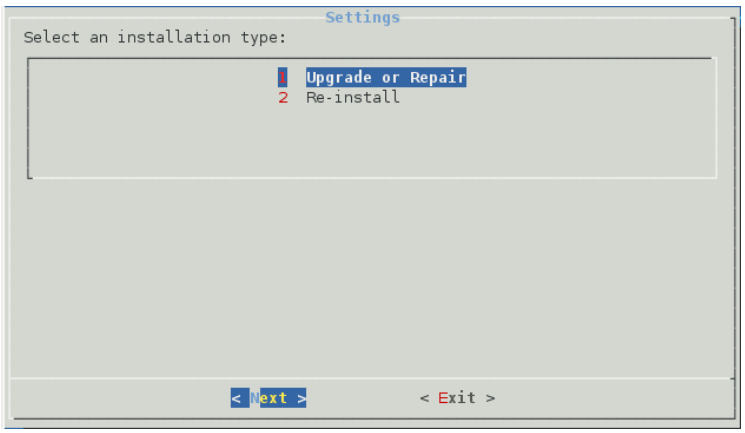
To repair or re-install a server, follow these steps:

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 10 - 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 seperate download server, complete the following deployment steps and then configure the server to use the third-party download server with the steps in chapter 9.

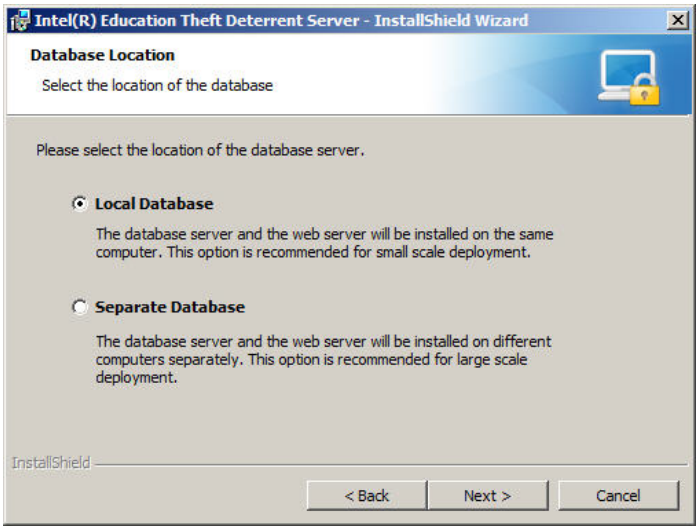
6.1 Install Theft Deterrent server

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 11 - 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**.

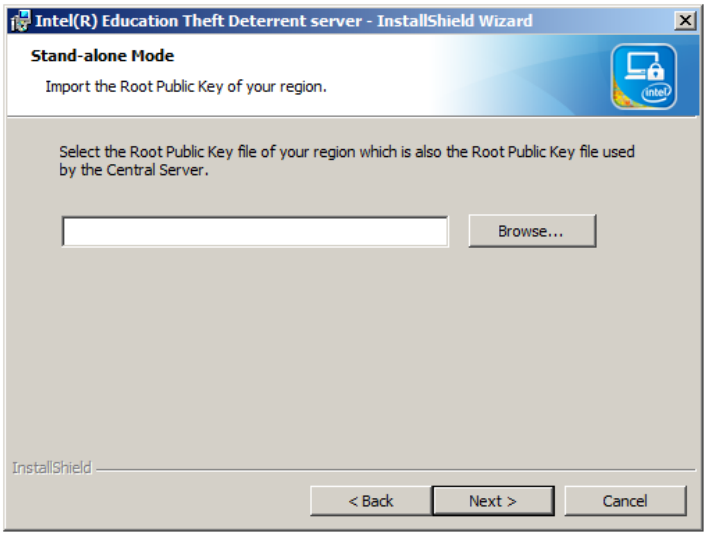
Figure 12 - Server Support Mode

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

Figure 13 - 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 14 - 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.

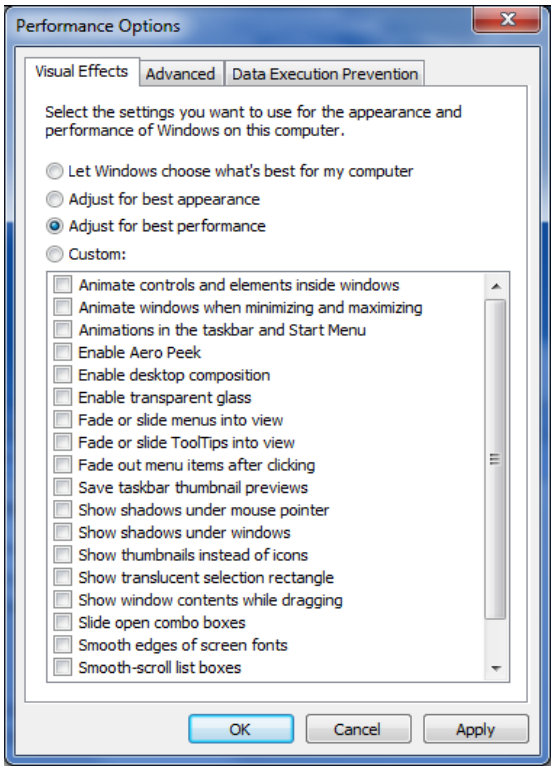
If your server is deployed on the Internet, improve the performance of your server with the following steps because the default configuration of the server has limited the resource assignment, which could be a performance bottleneck.

6.2.1 Common Configuration

Configure the performance options in Windows with the following steps:

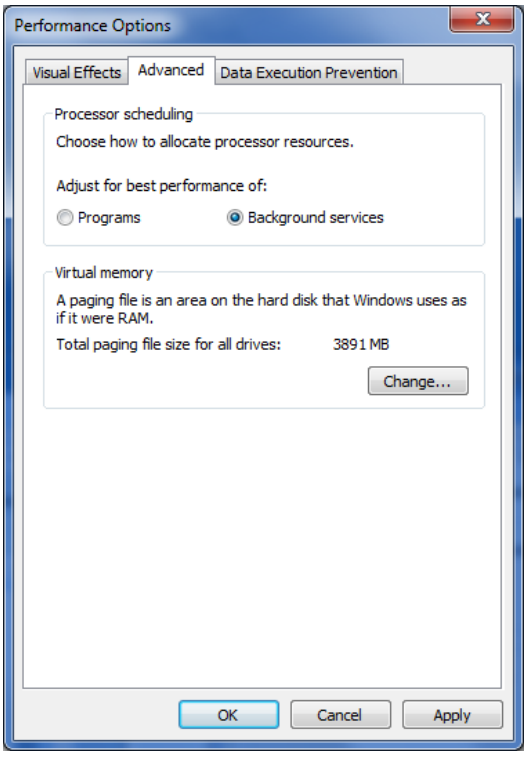
1. From Windows desktop, click the **Start** menu -> **Control Panel** -> **System and Security** -> **System** -> **Advanced system settings**.
2. On the popup window, switch to the **Advanced** tab and click **Settings** in the **Performance** area.
3. In the **Visual Effects** tab, select the **Adjust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

Figure 15 - Configure Performance (1)



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

Figure 16 - Configure Performance (2)

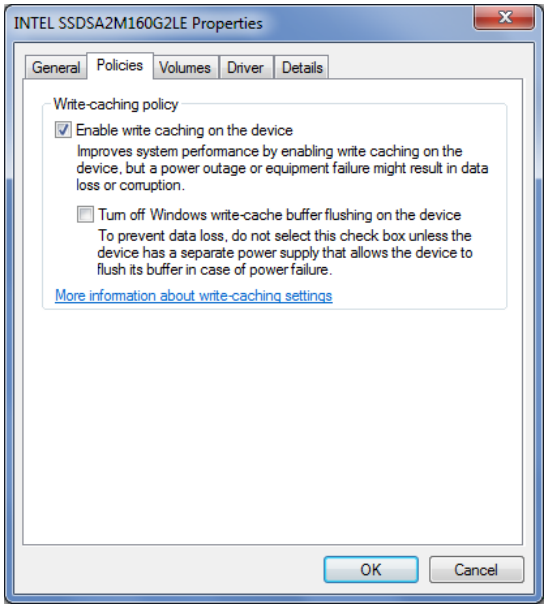


Enable Write-caching for hard disks with the following steps:

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 **Polices** tab and check **Enable write caching on the device**. Then click **OK**.

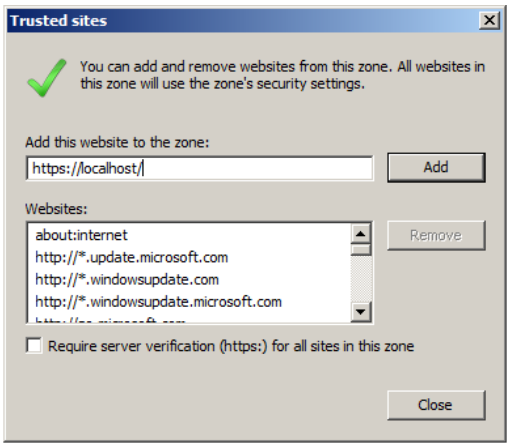
Figure 17 - Configure Performance (3)



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

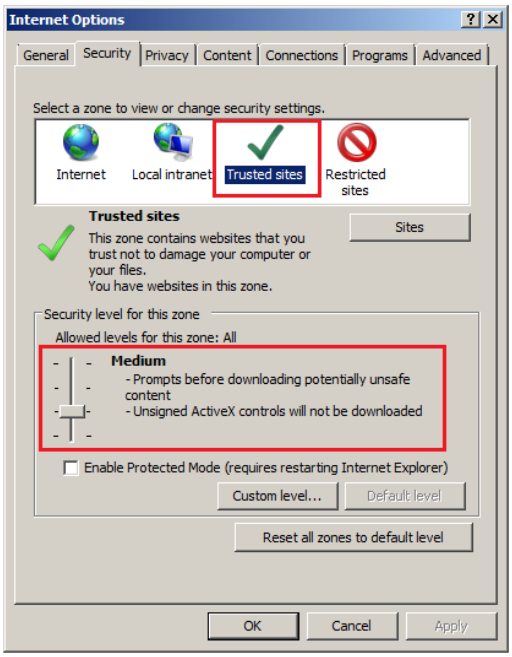
1. On Internet Explorer, click **Tools** -> **Internet Options** -> **Security Tab**.
2. On the **Security** page, select **Trusted Sites** and click the **Sites** button.
3. On the popup window, input https://localhost/ and then click the **Add** button.

Figure 18 - 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 19 - 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.

To upgrade a server, follow these steps:

1. Copy the latest server upgrade package (named as Theft_Deterrent_server-upgrade_v4.0.3010X.*[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.

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

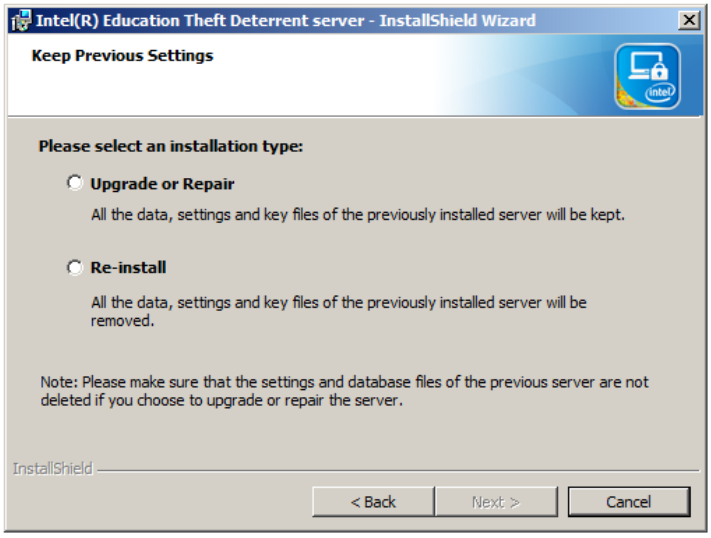
6.4 Repair or Re-install Theft Deterrent server

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 _v4.0.3010X.*[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 20 – 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. Migrate to Theft Deterrent server 4.x

To take advantage of the latest features, you can upgrade server from version 3.x to version 4.x and this chapter helps you plan for the upgrade. Since server 4.x is backward compatible with clients 2.x, upgrading the client to 4.x is not required but reconfiguration is so that the client 2.x can be managed by the latest server.

Note: To grade server 4.x to a higher version, follow the upgrade steps in chapter 5.4 or 6.3 according to your operating system.

You can upgrade the server 3.x with either of the following methods:

- Migrate to server 4.x installed on a different server machine
- Migrate to server 4.x installed on the same server machine

The first approach is recommended since it minimizes the impact of the current server system in production. For information on the requirements of the server machine, see chapter 4.

Regardless of the choice above, you must back up and migrate the current keystore and database to the new server to preserve the configuration and setting in place:

- Keystore contains the server keys and security certificates.
- Database contains an organized collection of the server data, which includes:
  - Device records
  - Device Tracking history
  - Accounts

7.1 Migration Tool

The keystore and database are not migrated automatically but server 4.x includes a migration tool, **migrate.jar**, in the installation directory to help you simplify the migration. The tool enables admin to copy the keystore and database from the server 3.x and merge them with the keystore and database in the latest server. By doing so, the clients that were managed by the server 3.x can be managed by the latest server.

7.1.1 Migration Requirements

The migration tool supports the following operating systems:

- Windows 2008 R2 64-bits
- Debian 6 or above 64-bits

You can migrate the server keystore and database across platforms but make sure that the server 3.x and 4.x run on the supported operating system.

Note: You can migrate between servers in different languages because the keystore and database are not language dependent.

Also, make sure the current server keystore and database are securely backed up before the migration.

The keystore and database migrated from the previous server will merge with that in server 4.x. Therefore, it is recommended that you also back up the keystore and database in server 4.x if it contains any existing device records or accounts.

7.1.2 Migration Options

Prior to running the tool, you need to understand the following options with regard to how you want to migrate the keystore and database:

Data	*Options*
Keystore	Because the server 3.x and 4.x use different server keys, you must decide which key to set as the default key for server 4.x when migration completes. If both server 3.x and 4.x have existing clients before the migration, one of these client group will download and update the server Public Key if their current keys are not set as the default key.
Database	Whether to merge the database of the old server with that of the new server.
Database - Account	Because the server 3.x and 4.x both contain an admin account, created by default during server deployment, you will need to decide whether to overwrite the admin account of the server 4.x with that of the server 3.x. You will see this option only if you choose to merge the database.

Once you understand the options, the next section will give you the details of running the tool.

7.2 Migrate to server on a different machine

7.2.1 Pre-migration Check

1. Install a server 4.x on a different server machine. See chapter 5 or 6 for detailed installation steps.
2. Make sure that the server 3.x is running correctly.
3. Run the following command on the server 3.x to check the Java version. Make sure that the version is Sun Java 6 or above.

```
java -version
```

Figure 21 - Check Java Version

```
java version "1.7.0_17"
Java(TM) SE Runtime Environment (build 1.7.0_17-b02)
Java HotSpot(TM) 64-Bit Server VM (build 23.7-b01, mixed mode)
```

4. If the server 3.x is installed on Windows, download and install **vcredist_x64.exe** from the Microsoft official website.

7.2.2 Migration steps

Then follow these steps to migrate the keystore and database of your old server to the new server:

On the server 4.x:

1. Find the migration tool (**migrate.jar**) at the following location according to your operating system and copy the tool to a removable device:

OS	*Migration Tool Location*
Debian	`/opt/TheftDeterrentserver/Tools/libs/migrate.jar`
Windows	`C:\Program Files\Intel Education Software\Theft Deterrent`

	server\Tools\libs\migrate.jar

On the server 3.x:

2. Copy **migrate.jar** from server 4.x to the old server. (e.g. `/root/migrate.jar`)
3. Go to the folder that contains the migration tool. For example:

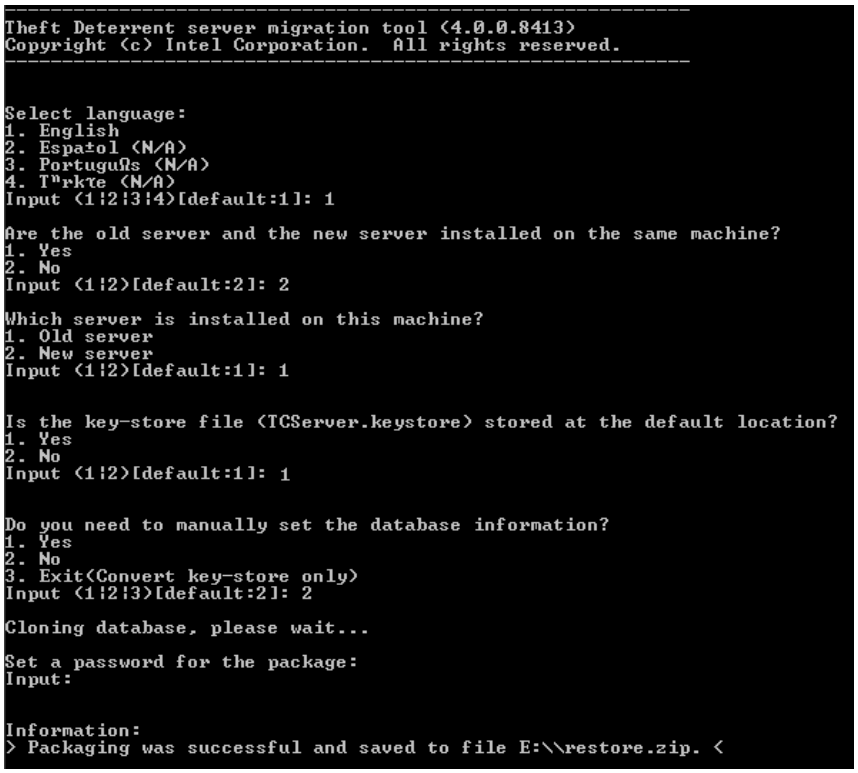
```
cd /root/
chmod a+x migrat.jar
```

4. Run the migration tool with root or admin privilege:

```
java -jar migrate.jar
```

5. You will be prompted for inputs shown in Figure 21. Select the options according to the table below:

Figure 22 - Migration Options on the Old Server



Prompts	*Descriptions*	*Select Option*
Select language	Select the display language of the migration tool.	1. English
Are the old server and the new server installed on the same machine?	Specify whether the old server and the new server are installed on the same machine because the migration steps for the two cases are different.	2. No
Which server is installed on this machine?	Specify whether this machine is the old server or the new server.	1. Old server
Is the key-store file (TCServer.keystore)	The migration tool backs up the old server keystore in the default location:	

stored at the default location?	• **Windows**: `C:\CMPC` • **Debian**: `/etc/theftdeterrent` If you have manually changed this keystore location for your current server, you will need to input the new location in the migration tool. Otherwise, select **1. Yes**.	
Do you need to manually set the database information?	The migration tool accesses the old server database with the default configurations. If you have manually changed the database configurations such as username, password, or database tool location, you will need to input the information in the migration tool. Otherwise, select **2. No**.	
Set a password for the package	The migration tool will create a package containing the keystore and database copied from the old server. It is recommended that you set a password for the package. However, you can leave the field blank if you do not want a password.	

A package named **restore.zip** will be created in the same folder as the migration tool.

On the server 4.x:

6. Copy **restore.zip** from the old server to the new server. (e.g. `/root/restore.zip`)
7. Run the following command with root or admin privilege according to your operating system to start the migration tool.

   - **Debian**:

   ```
   /usr/local/theftdeterrentserver/migrate <Max memory size>
   ```

   - **Windows**:

   ```
   cd C:\Program Files\Intel Education Software\Theft Deterrent server\bin
   call migrate.bat <Max memory size>
   ```

   <Max memory size>: a value, unit as M for the Java max memory size. If the parameter is empty, system will allocate max 1/4 of the system memory for Java. For 200K devices records, the system memory must bigger than 4G and the <Max memory size> parameter suggest to be 4000.

8. You will be prompted for inputs shown in Figure 22. Select the options according to the table below:

Figure 23 - Migration Options on the New Server

```
Select language:
1. English
2. Español (N/A)
3. Português (N/A)
4. Türkçe (N/A)
Input (1|2|3|4)[default:1]: 1

Are the old server and the new server installed on the same machine?
1. Yes
2. No
Input (1|2)[default:2]: 2

Which server is installed on this machine?
1. Old server
2. New server
Input (1|2)[default:1]: 2

Input the location of the "restore.zip" package:
Input: /root/restorize.zip

Input package password:
Input:


Information:
> The key-store was saved successfully. <

Do you want to migrate both the keystore and the database?
1. Key-store only
2. Key-store and database
Input (1|2)[default:2]: 2


Initializing database, please wait...

Do you want to set the keys from the old server keystore as the default keys?
1. Yes
2. No
Input (1|2)[default:1]: 2

Do you want to overwrite the data of the "admin" account?
1. Yes
2. No
Input (1|2)[default:2]: 1

Migrating for test now, please wait...

Information:
> Migration testing was successful. <

Commit it?
1. Yes
2. No
Input (1|2)[default:2]: 1

Migrating now, please wait...

Information:
> Migration testing was successful. <
                2 device(s) migrated. 0 device(s) not migrated.
                10 track(s) migrated. 0 track(s) not migrated.
                1 account(s) migrated. 0 account(s) not migrated.

> The operation will take effect after you restart the web server. <



The operation takes effect after the Theft Deterrent server restarts.
Do you want to restart now?
1. Yes
2. No
Input (1|2)[default:1]: 1

Restart now ... Done.
```

Prompts	*Descriptions*	*Select Option*
Select language	Select the display language of the migration tool.	1. English

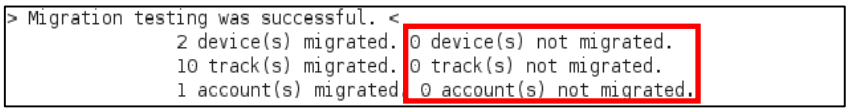
Are the old server and the new server installed on the same machine?	Specify whether the old server and the new server are installed on the same machine.	2. No
Which server is installed on this machine?	Specify whether this machine is the old server or the new server.	2. New server
Input the location of the "**restore.zip**" package:	e.g. `/root/restore.zip`	
Input package password:	The password set in the steps above.	
Do you want to migrate both the keystore and the database?	You can choose to migrate only the keystore if the new server is a test server for temporary usage, the server 3.x does not contain any device records or accounts, or you do not want to migrate any device records or accounts to the new server. In general, it is recommended that you migrate both the keystore and database so that you can manage the old devices with the new server without further action required.	1. keystore only 2. keystore and database
Do you want to set the keys from the old server keystore as the default keys?	Since the server 3.x and 4.x use different server keys, you must decide which key to set as the default key for server 4.x when migration completes. If both server 3.x and 4.x have existing clients before the migration, one of these client group will download and update the server Public Key if their current keys are not set as the default key. Therefore, to minimize the download and update action required, select this option if the device records migrated from the server 3.x outnumber the existing device records on the server 4.x. Select this option if the existing device records on the server 4.x outnumber the device records migrated from server 3.x.	1. Yes 2. No
Do you want to overwrite the data of the "admin" account?	If you want to replace the admin account of server 4.x with that of server 3.x, select **1. Yes**. If you want to keep the admin account of server 4.x, select **2. No**.	1. Yes 2. No

Confirm the settings to start the migration. Make sure that all the device records and accounts are migrated to server 4.x as shown in Figure 23. If you see any devices or accounts that cannot be migrated, you will be prompted with the following options:

- Skip these devices or accounts

- Or cancel the whole migration process

Figure 24 - Migration Result (On Different Server Machine)



Note: The tracks are the device IP history records that you can view on the server webpage.

Restart the server after migration completes.

7.3 Migrate to server on the same machine

It is recommended that you install the latest server on a different server machine. However, if no extra machine is available, you can install the new server on the same machine as the old server for upgrade.

7.3.1 Pre-migration Check

1. On server 3.x, stop Tomcat but make sure that the database is running correctly.

Run the script ControlTomcat6.sh to stop the TDv1 tomcat and remove it from the auto-startup list.

```
su
chmod a+x ControlTomcat6.sh
./ControlTomcat6.sh remove
```

Note: If you want to restore the TDv1 server in this machine, you can uninstall the TDv2 server, then run the script **./ControlTomcat6.sh restore**. A manual system restart is necessary before restore the TDv1 service.

2. Install a server 4.x on the current server machine. See chapter 5 or 6 for detailed installation steps.

7.3.2 Migration steps

Then follow these steps to migrate the keystore and database of your old server to the new server:

1. Run the following command with root or admin privilege according to your operating system to start the migration tool.

   - **Debian**:

```
/usr/local/theftdeterrentserver/migrate <Max memory size>
```

   - **Windows**:

```
cd C:\Program Files\Intel Education Software\Theft Deterrent server\bin
call migrate.bat <Max memory size>
```

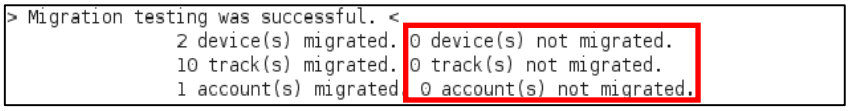
2. You will be prompted for several inputs. If the keystore and database of the old server have not been manually configured after server installation completed, select the

default options as listed in the table below. Otherwise, you might need to locate the key-store file or set the database information manually.

Choice	*Input*
Select language	1. English
Are the old server and the new server installed on the same machine?	2. Yes
Is the key-store file (TCServer.keystore) stored at the default location?	1. Yes
Do you want to set the keys from the old server keystore as the default keys?	Reference the table above.
Do you want to overwrite the data of the "admin" account?	Reference the table above.
Do you need to manually set the database information?	Reference the table above

Confirm the settings to start the migration. Make sure that all the device records and accounts are migrated to server 4.x as shown in Figure 24. If you see any devices or accounts that cannot be migrated, you can either skip these devices or accounts, or cancel the whole migration process.

Figure 25 - Migration Result (On the Same Server Machine)



Restart the server after migration completes.

7.4 Theft Deterrent Client Migration Options

After you complete the server migration steps, the server 4.x is ready to manage the clients from the old server. Since server 4.x is backward compatible with clients 2.x, you have the following client migration options:

- Upgrade the client by uninstalling the client v2.x and then install client and guardian v4.x.
- Keep the existing client v2.x. However, some server features might not be supported.

In both options, you might need to configure the client network settings if the server 4.x does not have the same URL as server 3.x. For more information, see the Intel® Education Theft Deterrent client User Manual.

For new devices deployed with client v4.x, all server features are supported. For more information about client first time setup, see the Intel® Education Theft Deterrent client User Manual.

7.4.1 Supported Features

For client version older than 2.x (including 2.x), you can manage the clients with the latest server but not all features are supported:

Function	*Client v4.x*	*Client v2.x*
Client Activation	Yes	Yes
Download and apply One-time Boot Certificate	Yes	Yes
Lock	Yes	Yes
Unlock with Unlock Code	Yes	Yes
Download and apply Global Certificate	Yes	Yes
Unlock with crash recovery package	Yes	Yes
Student log in to server	Yes	Yes
Automatic Server Broadcast /Auto-discovery	Yes	Yes
Sync up client status with server	Yes	Yes *
Configure Check-in Interval	Yes	Yes *
Modification Warning Days and Times	Yes	Yes *
Smart Client Upgrade	Yes	Yes *
Transfer device online	Yes	Partially supported
Password Protection	Yes	Yes *
Online help menu	Yes	No
Assign device to group	Yes	No
Remote unlock through network (for Android only)	Yes	No

* The function is supported only if it is used in the 2.x client before the migration.

For more information about the server features, see the Intel® Education Theft Deterrent server User Manual.

8. 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

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.

8.1 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	• Set up Server Name & Address • Set up Email Server
Central Server supported	• Activate the server or reactivate the server • Set up Server Name & Address • Set up Email Server

8.1.1 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:

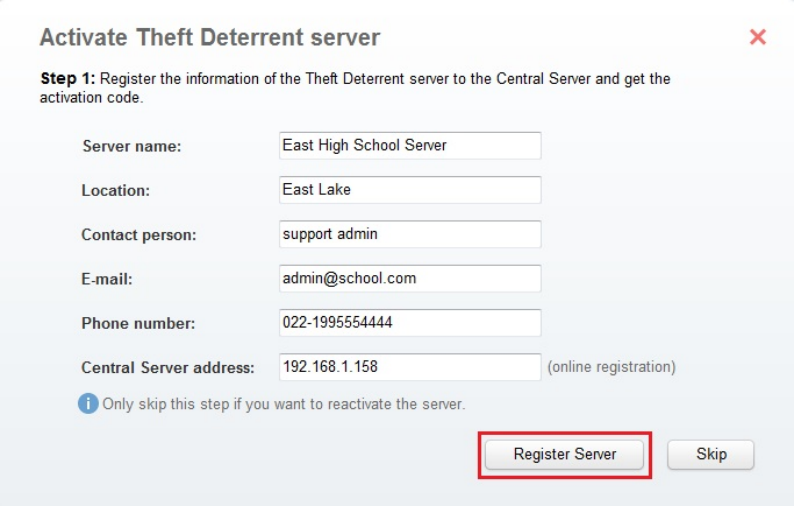
- Register the school information of the server on the central server.
- Back up the keystore and database information of the server on the central server.
- Enable the server to manage the devices pre-activated in factory.
- Enable the server to transfer devices via the central server to other servers.

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:

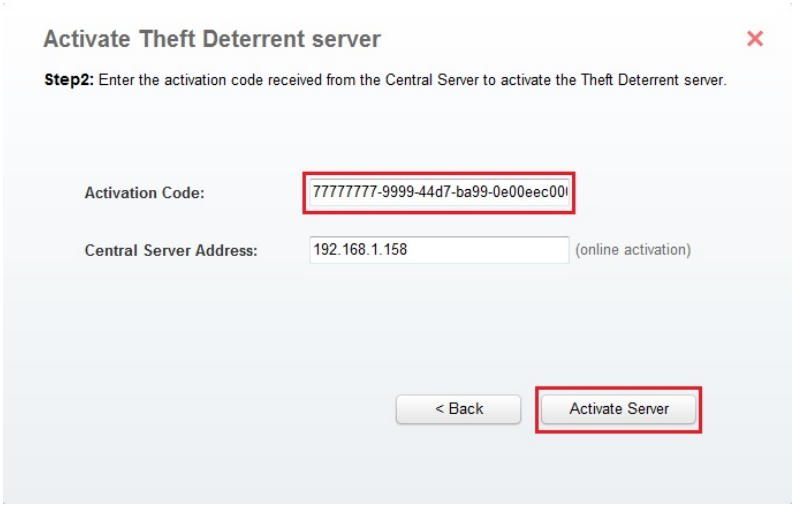
1. On the **Activate Theft Deterrent server** page (**Step 1**), input all server information and the IP address of the central server.
2. Click **Register Server** and your activation request will be sent to the central server.

Figure 26 - Activate Server (1)



3. 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.
4. 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.
5. 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 27 - Activate Server (2)



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

8.1.2 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:

1. Contact central server admin offline to request an activation code for reactivation.
2. On the **Activate Theft Deterrent server** page (**Step 1**), click **Skip**.
3. 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**.

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

When reactivation completes, you can manage the devices that were manage 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.

8.1.3 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

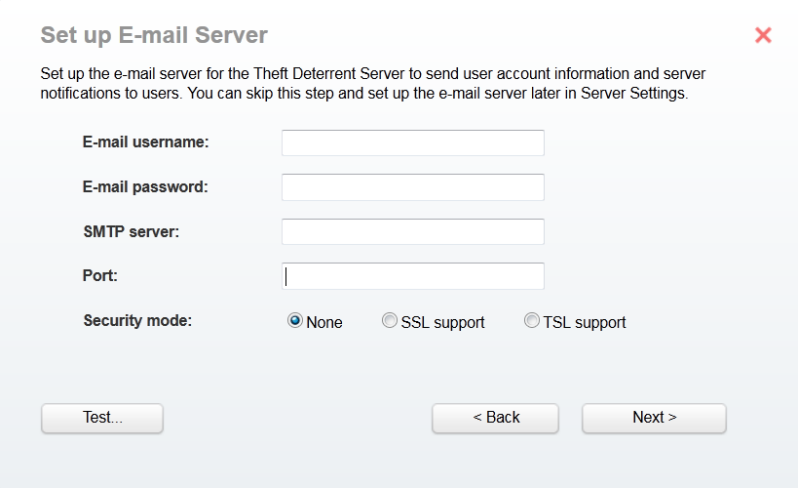
- Server address is the IP address or URL of the server machine.
- This server address will be broadcasted to the clients when the **Automatic Server Broadcast** function is turned on.

8.1.4 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 28 - Set up E-mail Notification Service



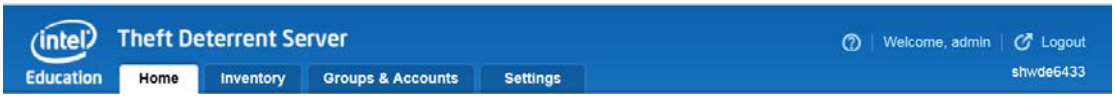
After the email service is configured correctly, the server will send out e-mails in the following cases:

When to send e-mails?	*Recipient*
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 29 - Server Tabs



8.2 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.

1. 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`
2. 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
   ```

3. 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**.

8.3 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:

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

9. 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 8. 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.

9.1 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.

9.2 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.

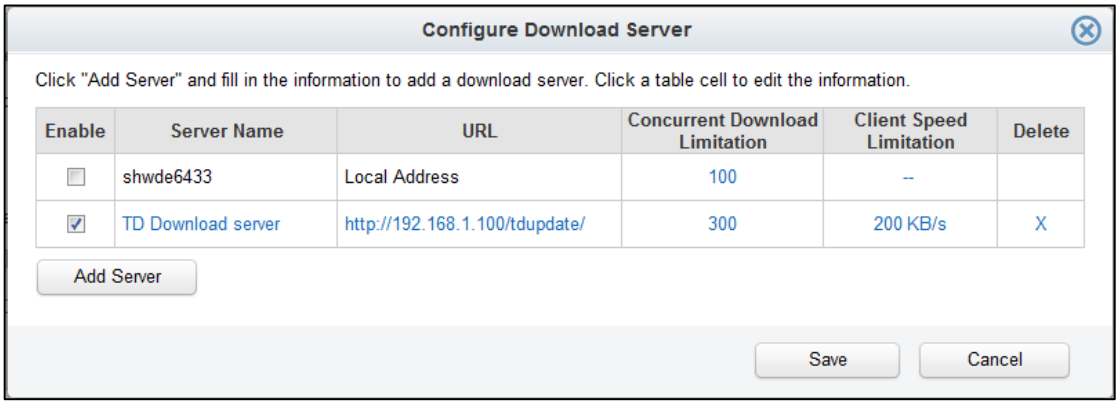
4. Click the **Save** Button.

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 30 - Configure Download Server



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

10. 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 manufactory 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.

10.1 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.

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.2 Deploy Theft Deterrent client and guardian on Debian

10.2.1 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
```

10.2.2 Install Theft Deterrent client and guardian

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.

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

After installation completes, the client is opened automatically.

10.3 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	1. Generate a password encryption file - passwordPro.ini
		`E:\>TDPasswordGen.exe "ZX12#23"`
		`Version:4.0.0.9293`
		`Generate password file success . . .`
		2. Copy the passwordPro.ini under the client install path.	

10.4 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.

10.4.1 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**.

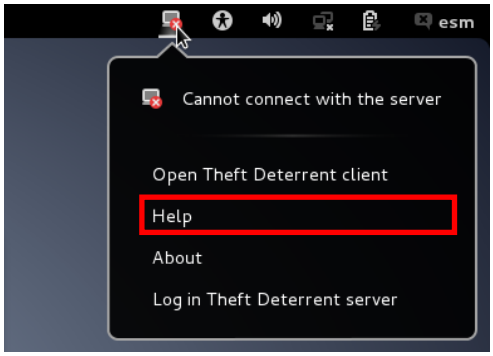
If the client is in **Inactive** status, right-click the client tray icon on the desktop and select **Help** for instructions on how to activate the client.

Figure 31 – Client Inactive Tray Icon (Windows)

10.4.2 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 32 – 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 33 - 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 34 - Shortcut on GNOME Classic

10.5 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.

11. Troubleshooting

11.1 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`

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

Answer: When you uninstall the server with the steps in chapter 5.5 or 6.4, 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.

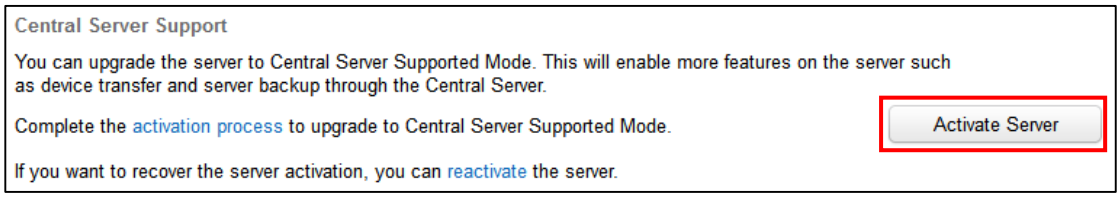
7. Can I upgrade from my server 3.x to a server 4.x in another language? For example, from a server 3.x in Spanish to a server 4.x in English.

Answer: Yes. By following the upgrade steps in chapter 7, 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.

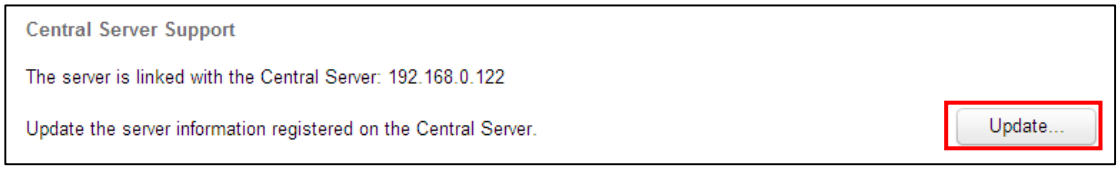
8. How do I find out the server support mode of my server?

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:



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

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

10. 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.

13. Appendix

13.1 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.

13.2 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.

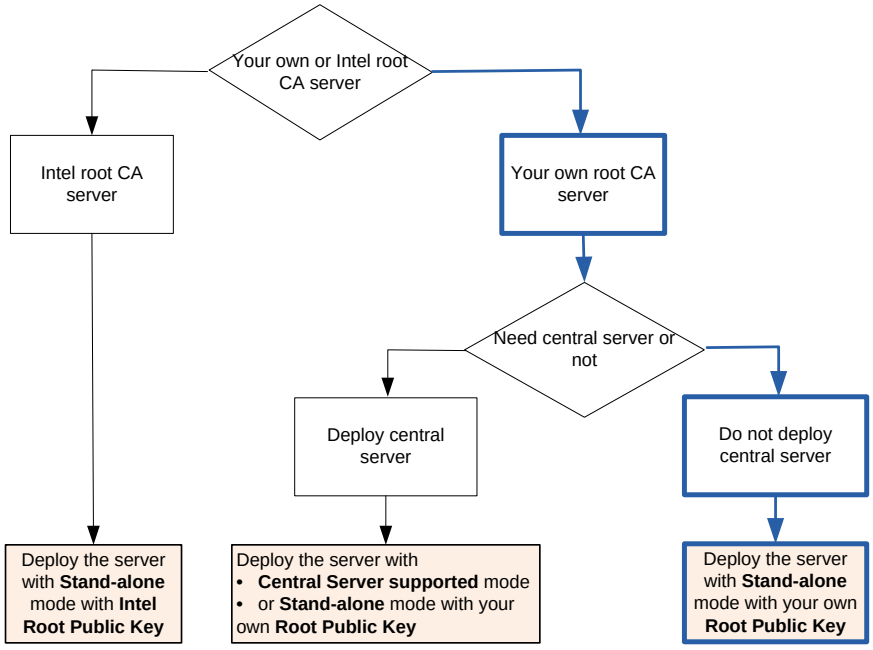
See the following table for more information about the server modes.

Server Support Mode	*Root Public Key*	*Theft Deterrent Components*	*Descriptions*
Stand-alone	Deploy with the Intel Root Public Key	Intel root CA server	• 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	• 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	• 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 35 - 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.

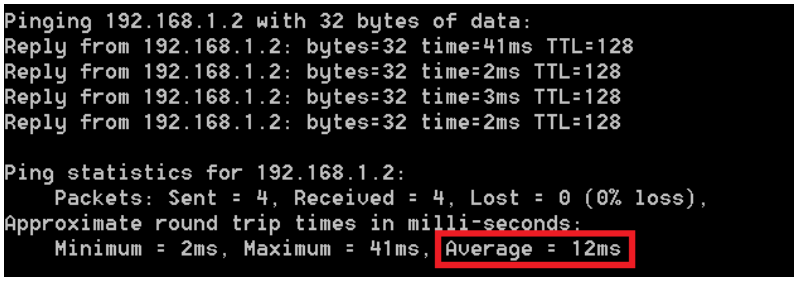
13.3 How to Understand the Network Stability

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 36 - Check Network Latency



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.

13.4 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 $\text{device download rate} = 3.3K\ bytes/s$ and $\text{device upload rate} = 2.5K\ bytes/s$.

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 $\text{server download rate} = 2.5K\ bytes/s$ and $\text{server upload rate} = 3.3K\ bytes/s$.

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.

13.5 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.

13.6 How to Back up Theft Deterrent server

To back up the server, follow these steps:

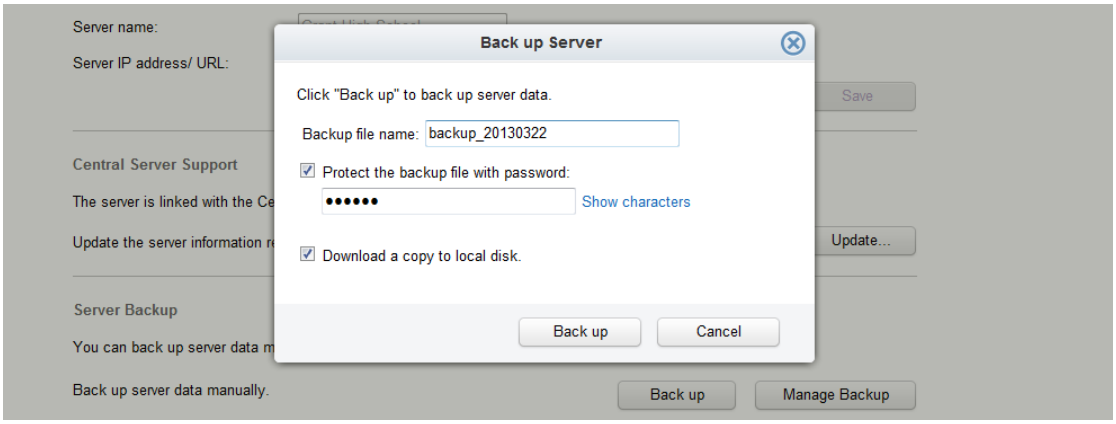
1. Log on the server and open the **Advanced** page under **Settings**.

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 37 - Back up the server



13.7 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_xxxxxxxxxxxxxxxxxxxx_xxxxxxxxxxxxxxxxxxxx.bin** will be generated in the folder:

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

Figure 38 - 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 39 - Import Pre-activated Package

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.