



Intel® Education Solutions

Intel® Education Solutions Theft Deterrent Training – Server Operation Guide

Legal Information

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY RELATING TO SALE AND/OR USE OF INTEL PRODUCTS, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT, OR OTHER INTELLECTUAL PROPERTY RIGHTS.

Intel, the Intel logo, Intel Atom, Intel Celeron, Intel Core are all trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

The hardware vendors of the bare bone notebooks and the interchangeable components remain solely responsible for the design, sale and functionality of their respective products, including any liability arising from product infringement and product warranty. Intel is not warranting the products of the hardware vendors.

Information regarding third-party products is provided solely for educational purposes. Intel is not responsible for the performance or support of third-party products does not make any representations or warranties whatsoever regarding quality, reliability, functionality, or compatibility of these devices or products.

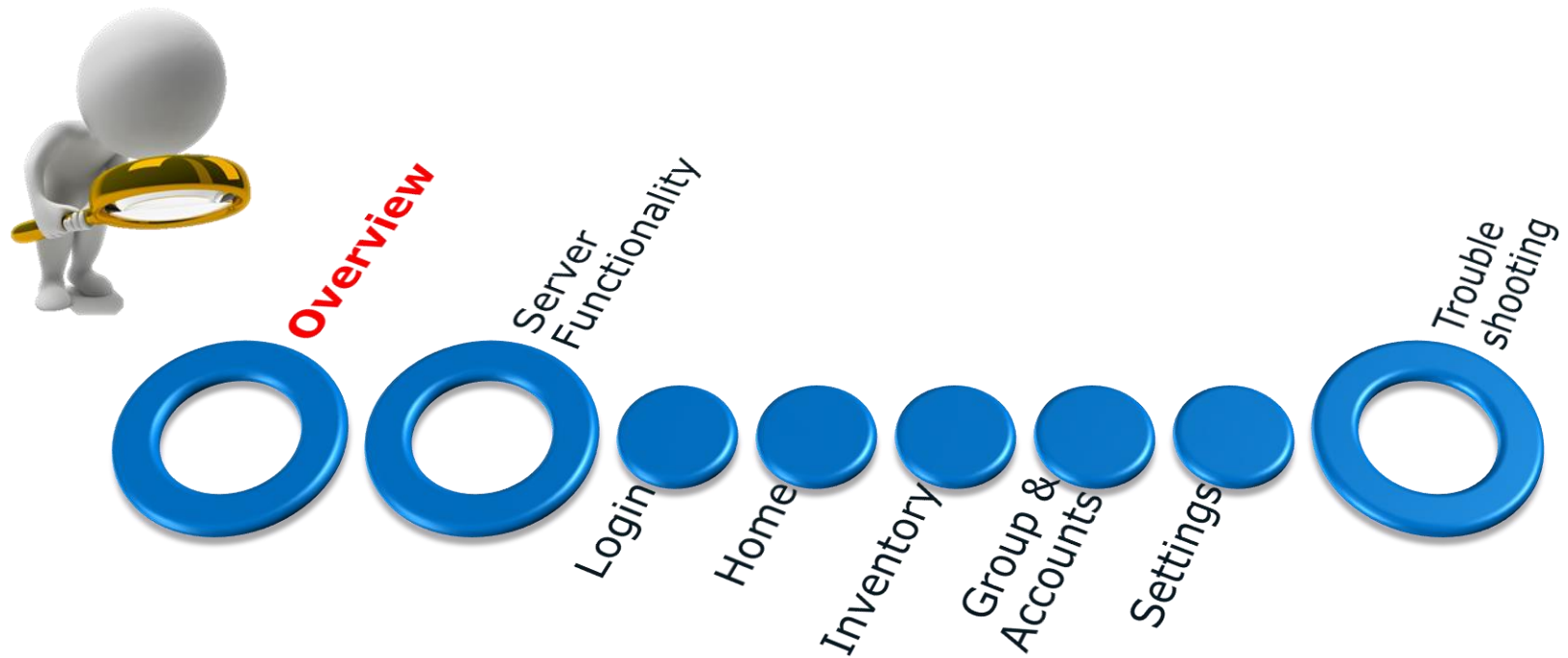
*Other names and brands may be claimed as the property of others.

Copyright © 2013, Intel Corporation. All rights reserved.

Revision History

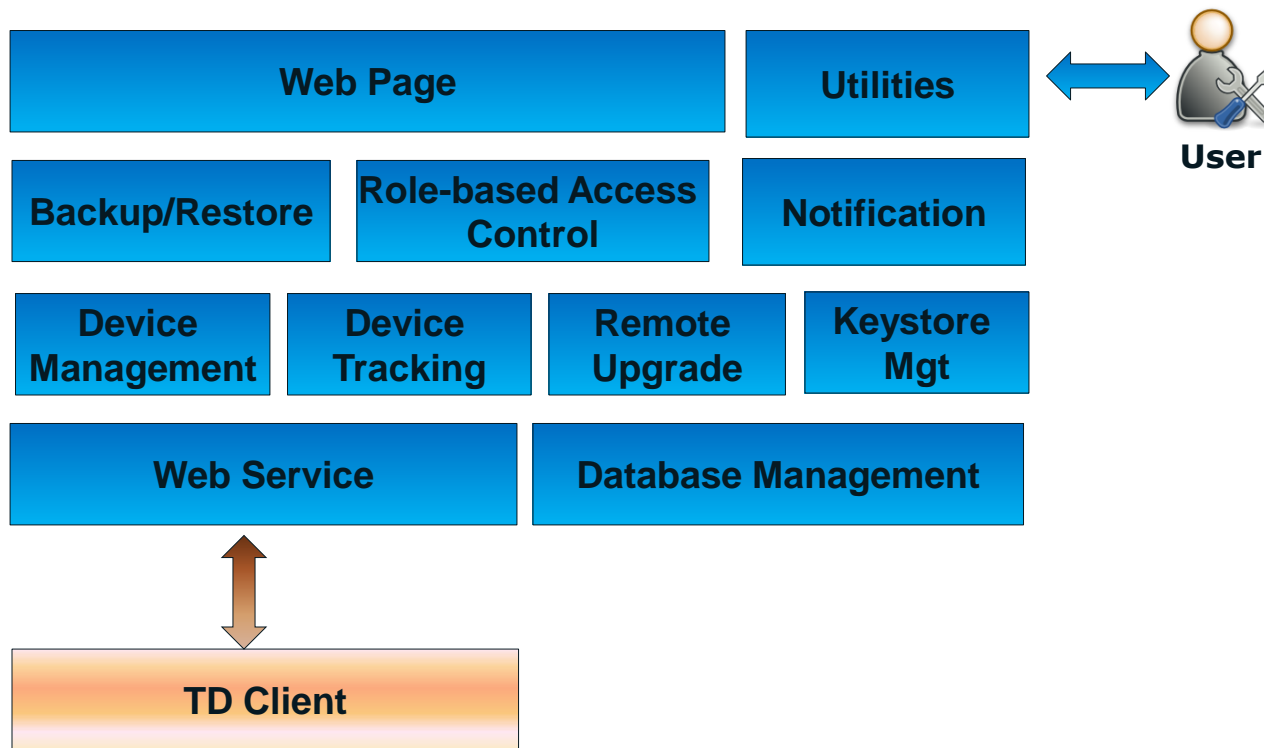
Revision	Comment
0.67	Revised on Sept 15, 2014

Agenda



Overview

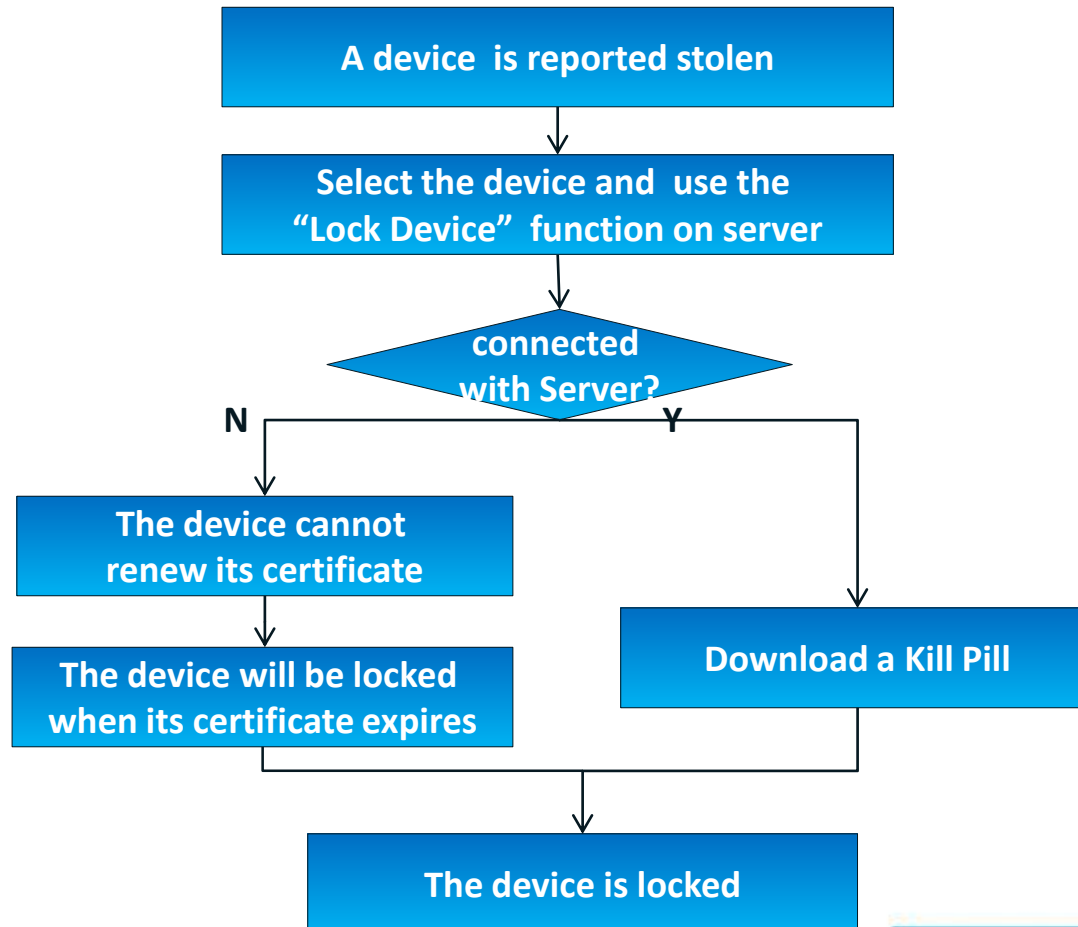
➤ TD server high level functionality



Overview

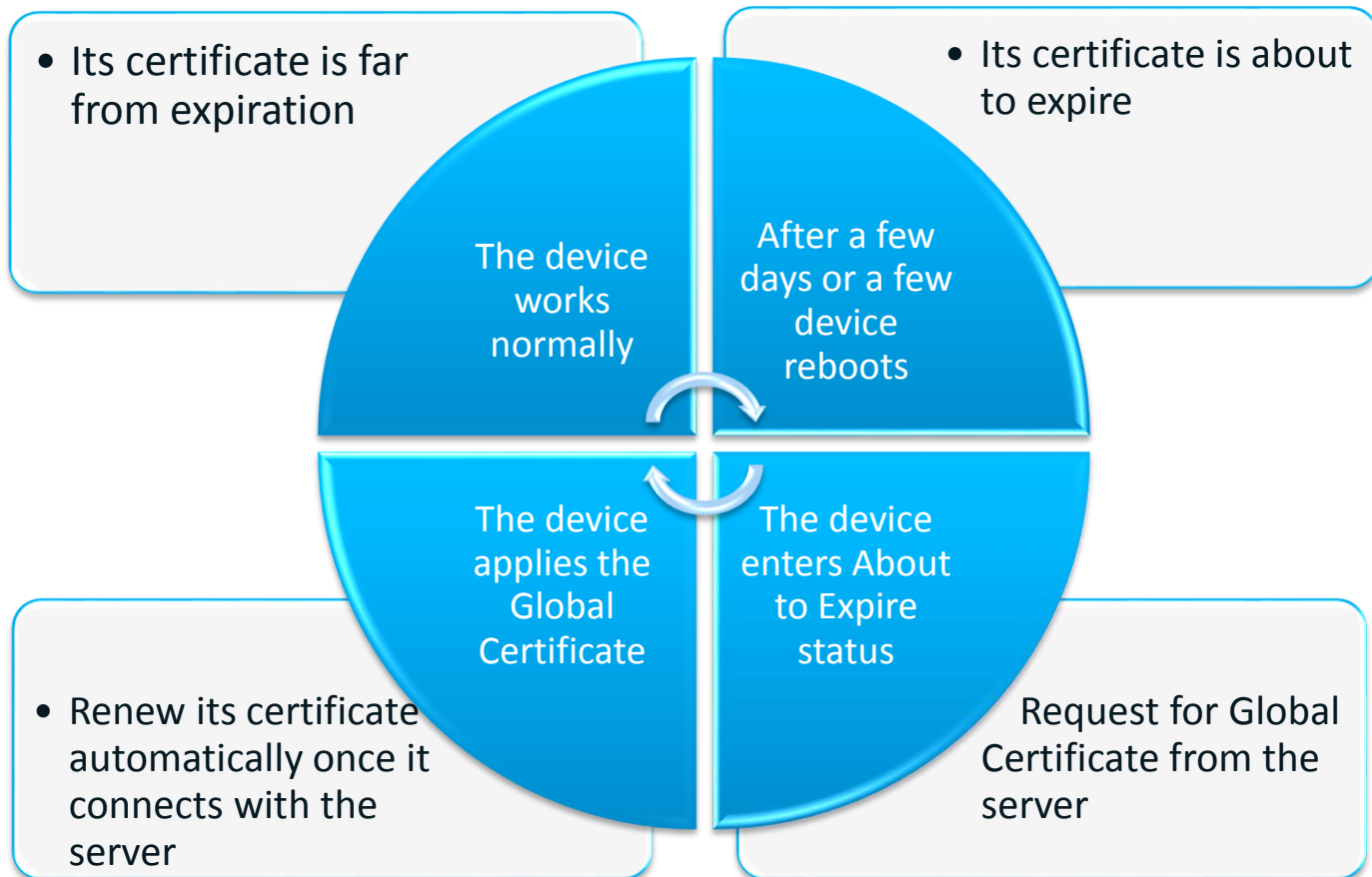
➤ Main TD working Scenarios

➤ Lock device scenario



Overview

➤ Normal status scenario



Overview

➤ Server Support Mode

<i>Server Support Mode</i>	<i>Description</i>
Stand-alone mode with Intel Root Public Key	<ul style="list-style-type: none">• No activation is required after the installation.
Stand-alone mode with your own Root Public Key	<ul style="list-style-type: none">• You can use the server without activation.• You can activate the server. (The server transforms to the Central Server supported mode)
Central Server supported mode	<ul style="list-style-type: none">• You must activate the server during pre-configuration after installation completes.

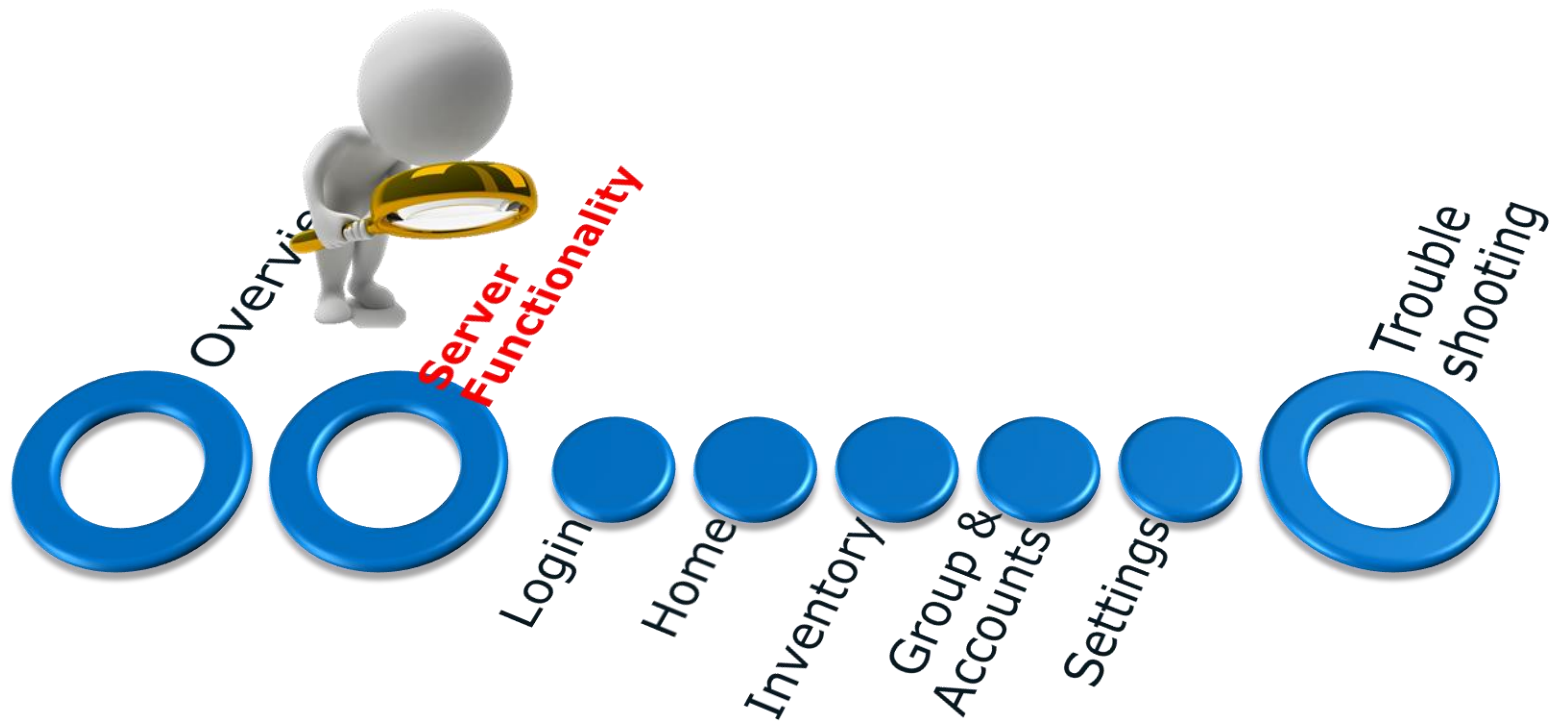
Overview

➤ User Account & Role

Server WebPages		Master Admin	Program Admin	Helpdesk / Call Centre	Custom
Home		✓	✓	✓	✓
Inventory		✓	✓	✓	✓
Groups & Accounts		✓	✓		
Settings	General	✓	✓	✓	✓
	Client	✓	✓		
	Server	✓	✓		
	Security	✓	✓		
	Advanced Account	✓		✓	✓

Account	Account Type	Available Functions	Groups
Master Admin	Admin	All functions.	All groups.
Program Admin	Admin	All functions except the Advanced page under Settings .	All groups.
Helpdesk / Call Center	Non-admin	Lock Device and Generate Unlock Code/Package .	The groups assigned.
Custom	Non-admin	The functions assigned.	The groups assigned.

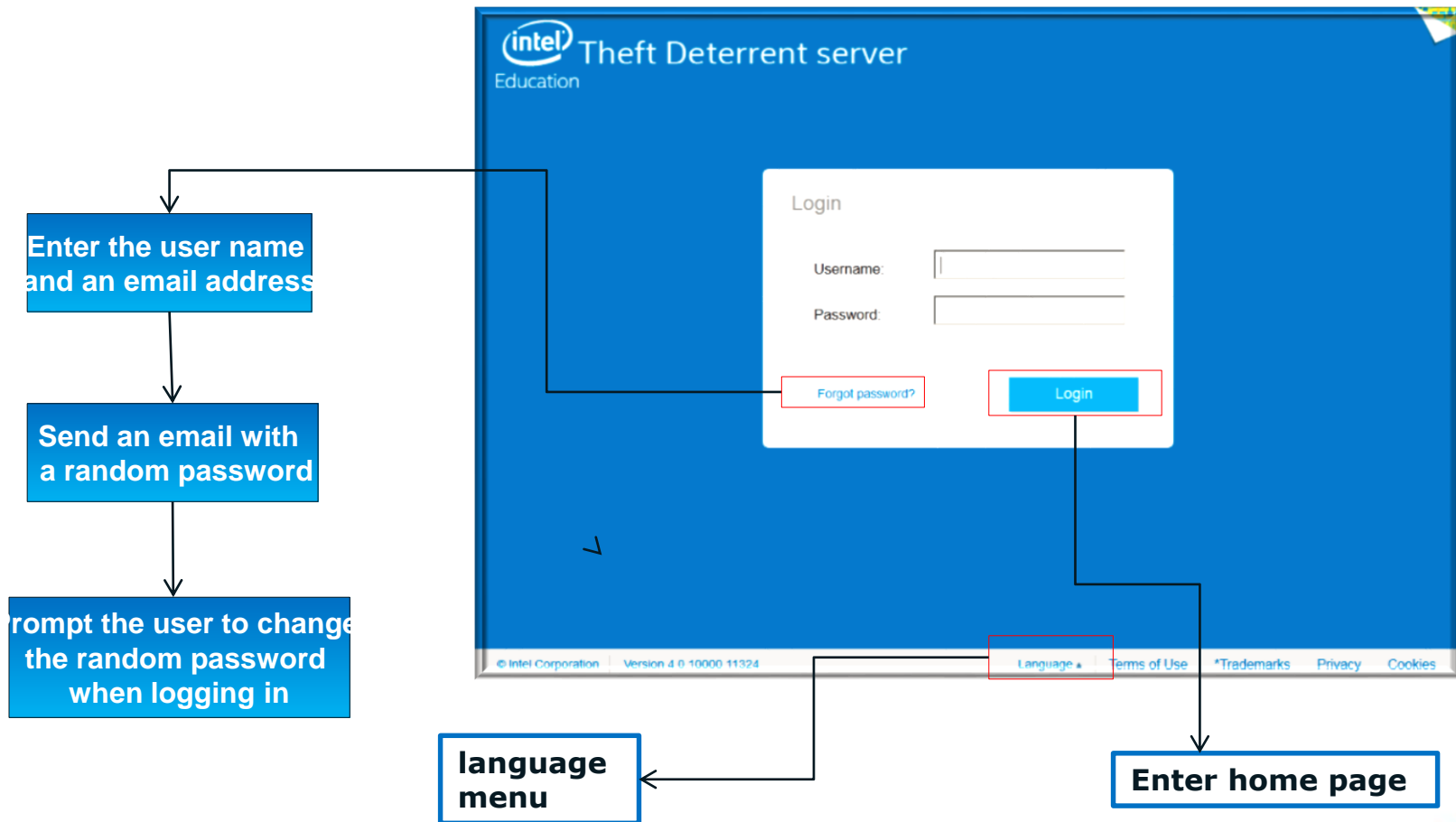
Agenda



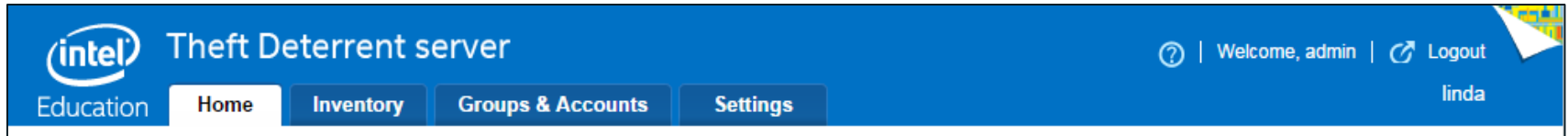
Login

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

Browser: IE 8 or above, Chrome, Firefox



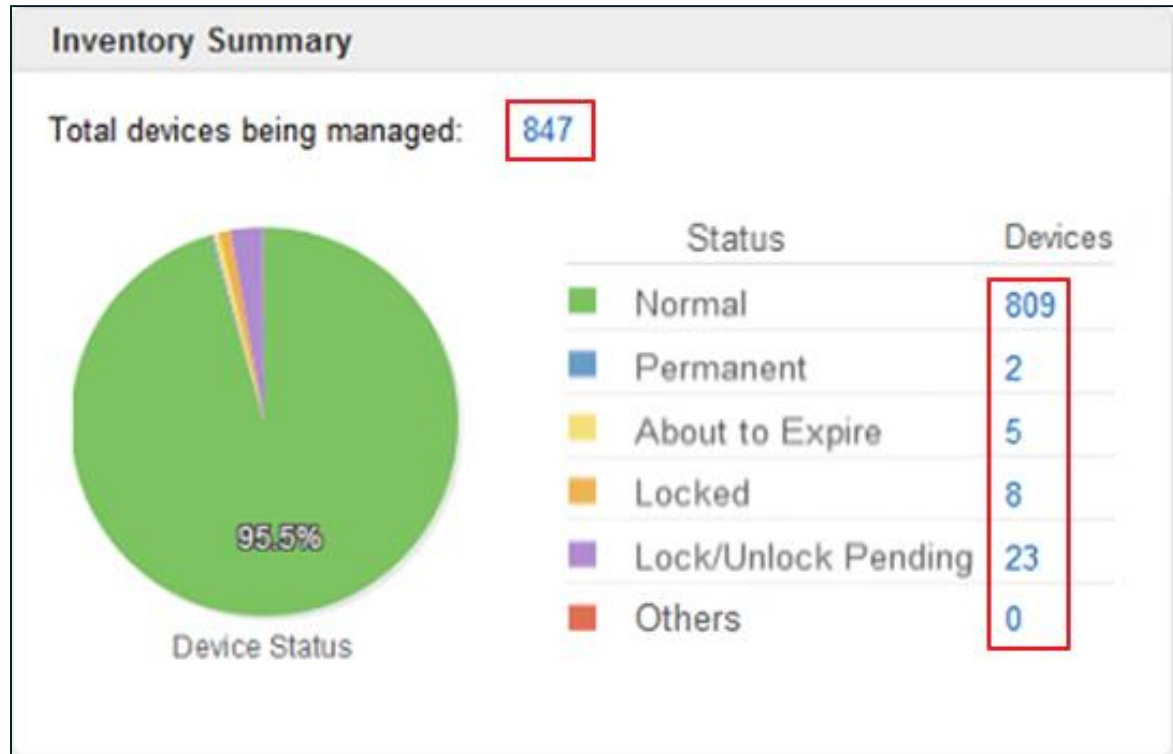
Home



Displays a statistical report:

- Inventory Summary
- Device Statistics
- Notifications

Home: Inventory Summary



Click blue
links to jump

Home: Device Statistics

Device Statistics				
Days	Last Check-in	Auto-locked	Manually Locked	Will Expire in
1-7	841	0	2	2
8-30	4	0	6	6
31-60	2	0	0	0
61-90	0	0	0	0
>90	0	0	0	0

Click blue
links to jump



Home: Device Statistics

The screenshot shows the 'Search & Filter' section of the Intel Management Console. It includes a search bar with the placeholder 'Enter criteria...' and a magnifying glass icon, and a dropdown menu with the placeholder 'Select a group...'. Below these is a table with two columns: 'Last login' and 'Last update'. The first row of the table shows '2014-01-23 13:42' and '2014-01-23 13:54' respectively. Blue arrows point from the search bar, the dropdown menu, and the 'Last login' and 'Last update' columns to callout boxes on the right.

Search & Filter

Search for devices:

Enter criteria... | 🔍

Or, filter devices by group:

Select a group... | ▼

Last login: 2014-01-23 13:42 | Last update: 2014-01-23 13:54

- Search for devices under management**
- Click to choose a specific group**
- User login time**
- Home page refreshed time**

Home: Notifications

The screenshot shows the 'Notifications' section of the Intel Education Solutions interface. It contains a list of notifications with icons indicating their severity: red 'X' for errors and yellow exclamation marks for warnings. Below the list are two buttons: 'Export Report' and 'View Logs'. At the bottom of the page is a footer menu with links for 'Language', 'Terms of Use', '*Trademarks', 'Privacy', and 'Cookies'. Blue arrows point from callout boxes to specific elements in the interface.

Error: Require your action.

Warning: Require your attention.

Export Report: Export some or all information of the dashboard

Language menu

View Logs: View, filter or export server operation logs

Notifications

- ✖ 28 device(s) has error.
- ✖ Failed to connect with the Central Server; last connection: 09:31 03-18-2014
- ✖ Theft Deterrent server Public Key was updated failed at 17:07 03-04-2014.
- ! 373 new device(s) has been approved under awaiting for check-in.
- ! 125 device(s) has been locked since your last login.
- ...

[View all notifications](#)


[Export Report](#) [View Logs](#)


[Language](#) [Terms of Use](#) [*Trademarks](#) [Privacy](#) [Cookies](#)


- The default language was selected during installation
- User's language preference will be saved


Home: Notifications


Notifications

 3 device(s) has error.

 Failed to connect with the Central Server; last connection: 15:27 02-07-2013

 5 device(s) will expire in 7 days.

 5 device(s) is being transferred to this server and requires your approval.

 1 new device(s) needs your approval.

...

View all notifications

Note: You can export device information as CSV file through the popup dialog of the **Device Error, Boot Tick Error, Unmatched Provision Number, or Exceed Download Limit** notification.

Type	Category	Description	Action
Error	Server Backup	Last automatic backup (to central server) failed at [date]: Backup now.	Check the status of the server and retry the server backup or restore
	Server Restore	Last restore failed at [date].	
	Device Error	XXX device(s) has error.	Refer to the device error code and find the device to debug. For managed device, the error can be cleared.
Warning	E-mail	Failed to send [email type] to [receiver] by e-mail at [date].	Check the email server availability.
	Device Transfer-in	XXX device(s) is being transferred to this server and requires your approval.	Approve or reject the transfer.
	Device Transfer-out	The transfer request(s) of XXX device(s) has been rejected by the destination server(s) since your last login.	Connect with the destination server admin.

Home: Notifications

Type	Category	Description	Action
Warning	Pending New Device	XXX new device(s) needs your approval.	Approve or reject the device.
	Awaiting check-in	XXX new device(s) has been approved under awaiting for check-in.	Wait for the device to check-in the server.
	Device Status	XXX device(s) has been locked since your last login.	<ol style="list-style-type: none"> If the device number is reasonable, generate unlock code for these device If the device number is not reasonable, check the server status and network connectivity.
	Device Status	XXX device(s) will expire in 7 days.	
	Device Status	XXX device(s): The Boot Tick at the client side is inconsistent with that in the server.	Reset the boot tick.
	Device Status	XXX device(s): The number of certificates downloaded has exceeded the boot certificate limit.	Reset the certificate download limit.
	Unmatched Provision Number	XXX device(s): provision number is unmatched.	Find the device(s) and change the server URL in client.
Information	Server Backup	Last automatic backup (to central server) was successful at [date].	No action is required.
	Server Restore	Last restore was successful at [date].	
	Server Update	Theft Deterrent server Public Key was updated successfully at [date].	
	New Device	XXX new device(s) has been added since your last login.	
	Device Transfer-out	XXX device(s) has been transferred to other server(s) successfully since your last login.	
	Device Transfer-out	XXX device(s) is pending to be transferred to other server(s).	

Inventory: Outline

Webpage

Pending New Devices

Device management

- Webpage layout
- Function
 - Assign Group
 - Lock and Unlock Devices
 - Provision new certificate
 - Transfer Device (optional)

Inventory: Webpage

Sub-Tab	Appearance Condition	Function	Comment
Device Management	Always appear	<ul style="list-style-type: none"> - View Device detail - Assign Group - Lock Device - Allow Unlocking - Generate Unlock Code - Provision New Certificate - Reject Device - View Blocked Devices - View Transfer History - Export Report 	Each user account can be assigned with different functions and the user will only be able to view and access to the functions that were assigned.
Pending New Devices	Appear only when there are some devices that require the manual approval or have device errors	<ul style="list-style-type: none"> - Approve Device - Reject Device - View Blocked Devices - Lock -Generate Unlock Code 	Only users that are assigned with any of the three functions can access to this page.
Transfer-In	Appear only when there are some devices that transfer to/from the Server (Central Server supported mode only)	<ul style="list-style-type: none"> - Accept Transfer - Reject Transfer - Export School Package 	Only the users that are assigned with any of the three functions can access to this page.
Transfer-Out		<ul style="list-style-type: none"> - Cancel Transfer - View History - Export School Package -Complete Offline Transfer 	Only users that are assigned with any of the three functions can access to this page.



Inventory: Pending new devices

➤ Approve new devices:

Step 1: Enter the Pending New Devices page

Device Management (166) | Transfer-in (6) | Transfer-out (8) | Pending New Devices

Devices Pending

Select all 9 devices

<input type="checkbox"/>	Hardware ID	Device Name	Group	IP Address	Approval Status
<input type="checkbox"/>	5EFC A30000CF	CMPC-01-196			Awaiting check-in
<input type="checkbox"/>	4089C40000BF	CMPC-00-183	Riverview Primary Scho		Awaiting check-in
<input type="checkbox"/>	4BAE910000CF	CMPC-01-195	MinHang Middle School		Awaiting check-in
<input type="checkbox"/>	4EFC A30000CF	CMPC-01-196	Applegate Primary Scho		Awaiting check-in
<input type="checkbox"/>	7EFC A30000CF	CMPC-01-196	Applegate Primary Scho		Awaiting check-in
<input type="checkbox"/>	D291520000B6	CMPC-00-185	MinHang Middle School		Awaiting check-in
<input type="checkbox"/>	83AF210000BE	CMPC-00-189	ShangHai Foreign Lang		Awaiting check-in
<input type="checkbox"/>	7F97B1000047	CMPC-01-71		10.216.245.170	Awaiting check-in
<input type="checkbox"/>	F50585000038	CMPC-00-56		10.216.71.126	Pending Approval

Selected Devices: 0 / 9

Page 1 of 1

Search & Filter

All status

Enter criteria...

Actions

Approve Device

Reject Device

View Blocked Devices

Lock

Generate Unlock Code

Inventory: Pending new devices

Step2 : Check status and take actions

Device Status	Color	Action	Next Status
Pending New devices	Black	<ul style="list-style-type: none">➤ Approve➤ Reject	<ul style="list-style-type: none">➤ "Awaiting check-in" status after approval➤ Moves to Block list after rejection
	Orange (TDv1 device)		
	Red (Hardware error)	Only reject	
Awaiting check-in	Black	No action needed	Changes to "Normal" status and moves to the Device Management page after its certificate is prepared
	Orange (TDv1 device)		



Inventory: Device Management

➤ Webpage Layout

Education Home Inventory Groups & Accounts Settings

Device Management Transfer-in (16) Transfer-out (17) Pending New Devices

All devices [Select all 428 devices](#)

<input type="checkbox"/>	Hardware ID	Group	Device Name	Student Name	Hardware Model	Gateway	Last Check	Expiration Date	Status
<input type="checkbox"/>	6FBD88000	Grant High School	CMPC-01-487		Tablet	61.71.160.59	2013-02-03	2013-06-01	
<input type="checkbox"/>	54788C000	Hoover High School	CMPC-01-486		Unknown classmate	211.102.145.10	2013-05-10	2014-05-10	
<input type="checkbox"/>	8D42CD000	Grant High School	CMPC-00-485	Zhang Qiu	Tablet	202.190.230.54	2013-02-03	2013-05-15	
<input type="checkbox"/>	05D957000	Grant High School	CMPC-00-483	Peter Pan	Tablet	61.1.236.88	2013-05-10	2014-05-10	
<input type="checkbox"/>	26FD30000	Hoover High School	CMPC-01-482	Tom Green	Convertible	211.199.136.23	2013-05-10	2013-09-11	
<input type="checkbox"/>	B584EC000	Wilson Elementary	CMPC-01-481		Unknown classmate	61.226.179.115	2013-05-10	2014-05-10	
<input type="checkbox"/>	BB38D9000	Wilson Elementary	CMPC-00-479		Not a classmate	61.218.235.138	2013-05-10	2014-05-10	
<input type="checkbox"/>	E65532000	Hoover High School	CMPC-01-478		Clamshell	211.160.129.24	2013-05-10	2013-07-02	
<input type="checkbox"/>	E63AC1000	Wilson Elementary	CMPC-01-477		Not a classmate	202.221.188.13	2013-05-10	2014-05-10	
<input type="checkbox"/>	D66A56000	Hoover High School	CMPC-01-476		Unknown classmate	211.12.245.9	2013-05-10	2013-06-16	
<input type="checkbox"/>	BD3526000	Hoover High School	CMPC-01-475		Unknown classmate	202.176.227.92	2013-05-10	2014-05-10	
<input type="checkbox"/>	663DA2000	Wilson Elementary	CMPC-01-474		Unknown classmate	202.10.230.61	2013-05-10	2013-06-27	
<input type="checkbox"/>	5BF770000		CMPC-00-473		Not a classmate	202.42.121.169	2013-05-10	2014-05-10	
<input type="checkbox"/>	2BB74F000		CMPC-00-472		Tablet	61.197.131.211	2013-05-10	2013-05-24	
<input type="checkbox"/>	D8000F000		CMPC-01-471		Not a classmate	61.80.127.137	2013-05-10	2013-07-12	

Selected Devices: 0 / 428

Page 2 of 29

15










Click to change column items

Click to enter Device Details

Click to change row numbers per page


Inventory: Device Management

Status and corresponding actions

Status	Icon	Action in Device Detail
Normal		<ul style="list-style-type: none"> • <input type="checkbox"/> Edit Device • <input type="checkbox"/> Lock Device • <input type="checkbox"/> Provision New Certificate • <input type="checkbox"/> Transfer Device (Central Server supported mode only)
Permanent		
About to Expire		
Manually Locked		Allow Unlocking
Automatically Locked		Generate Unlock Code
Lock Pending		Allow Unlocking
Unlock Pending		Generate Unlock Code
Awaiting check-in		No action is available
Error		No action is available

Inventory: Device Management

Row colors and corresponding actions

Row Color	Additional Action in Device Information Table							
Black	No addition action is required.							
Yellow	Global certificate download is blocked since the Boot Tick is inconsistent. <div><table><tr><td>Last Known Boot Tick</td><td>6</td><td>Reset</td></tr><tr><td colspan="3">The Boot Tick at the client side is inconsistent with that in the server.</td></tr></table></div>		Last Known Boot Tick	6	Reset	The Boot Tick at the client side is inconsistent with that in the server.		
Last Known Boot Tick	6	Reset						
The Boot Tick at the client side is inconsistent with that in the server.								
	Global certificate download is blocked since the download times has exceeded the limit. <div><div>Device status:</div><div> About to Expire</div><div>The number of certificates downloaded has exceeded the boot certificate limit. Reset</div></div>							
Red	Device Error with Error Code 0X***** inside. No action is available.							

Inventory: Device Management

Action Panel

Actions	Action	Device Status	Role Control
Assign to Group	Assign to Group	All	1. Privilege can be configured during create each Custom account. 2. Help desk/Call center can only access Lock and Generate Unlock Code
Lock	Lock	Normal/Permanent/About to Expire Automatically Locked Unlock Pending	
Allow Unlocking	Allow Unlocking	Manual Locked Lock Pending	
Generate Unlock Code	Generate Unlock Code	Normal/Permanent/About to Expire Automatically Locked Unlock Pending	
More Actions ▼	Provision New Certificate	Normal/Permanent/About to Expire	
Provision New Certificate	Reject Device	All	Binding with "Approve new device" privilege
Reject Device	View Blocked Devices	N/A	
View Blocked Devices	Export Report	All	Available for all accounts
Export Report			

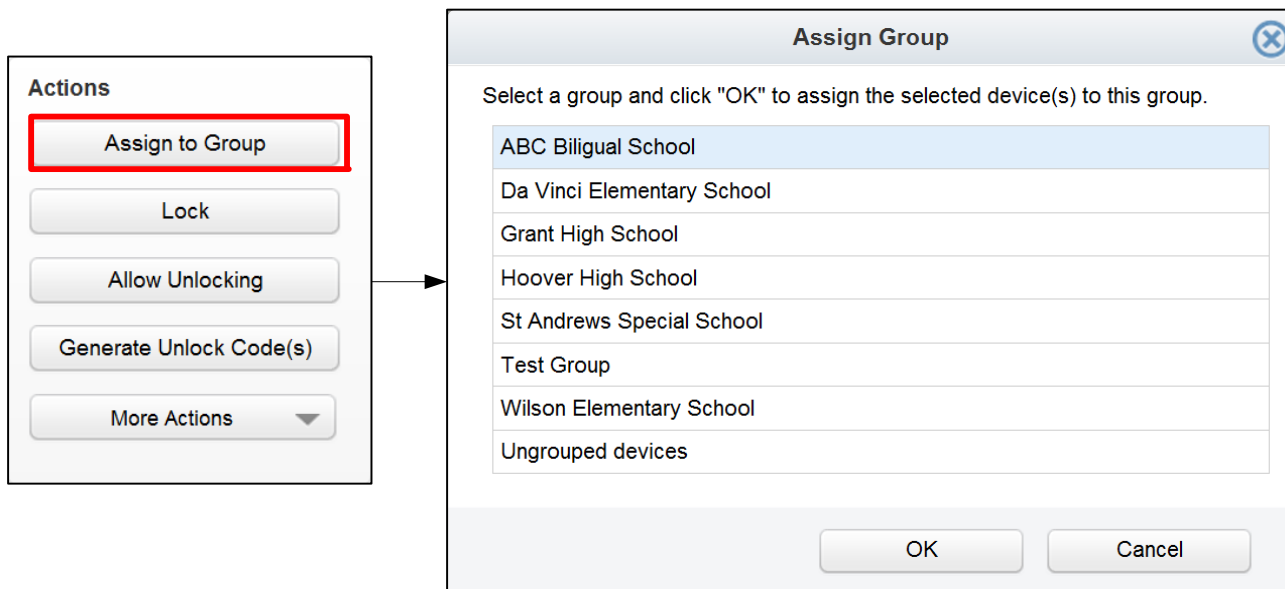
Action buttons are different according to the user role

Inventory: Device Management

➤ Function

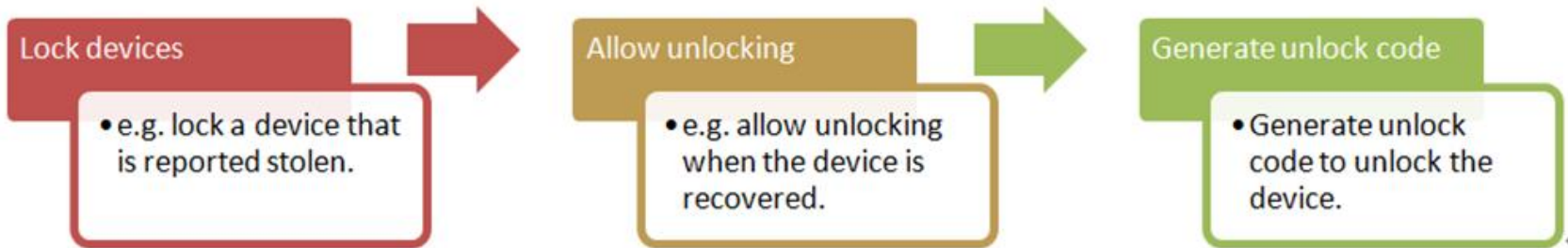
1. Assign Group

- Prerequisite: The master admin or program admin must create groups in the Groups & Accounts page in advance.



Inventory: Device Management

2. Lock and Unlock Devices



➤ Lock a device:

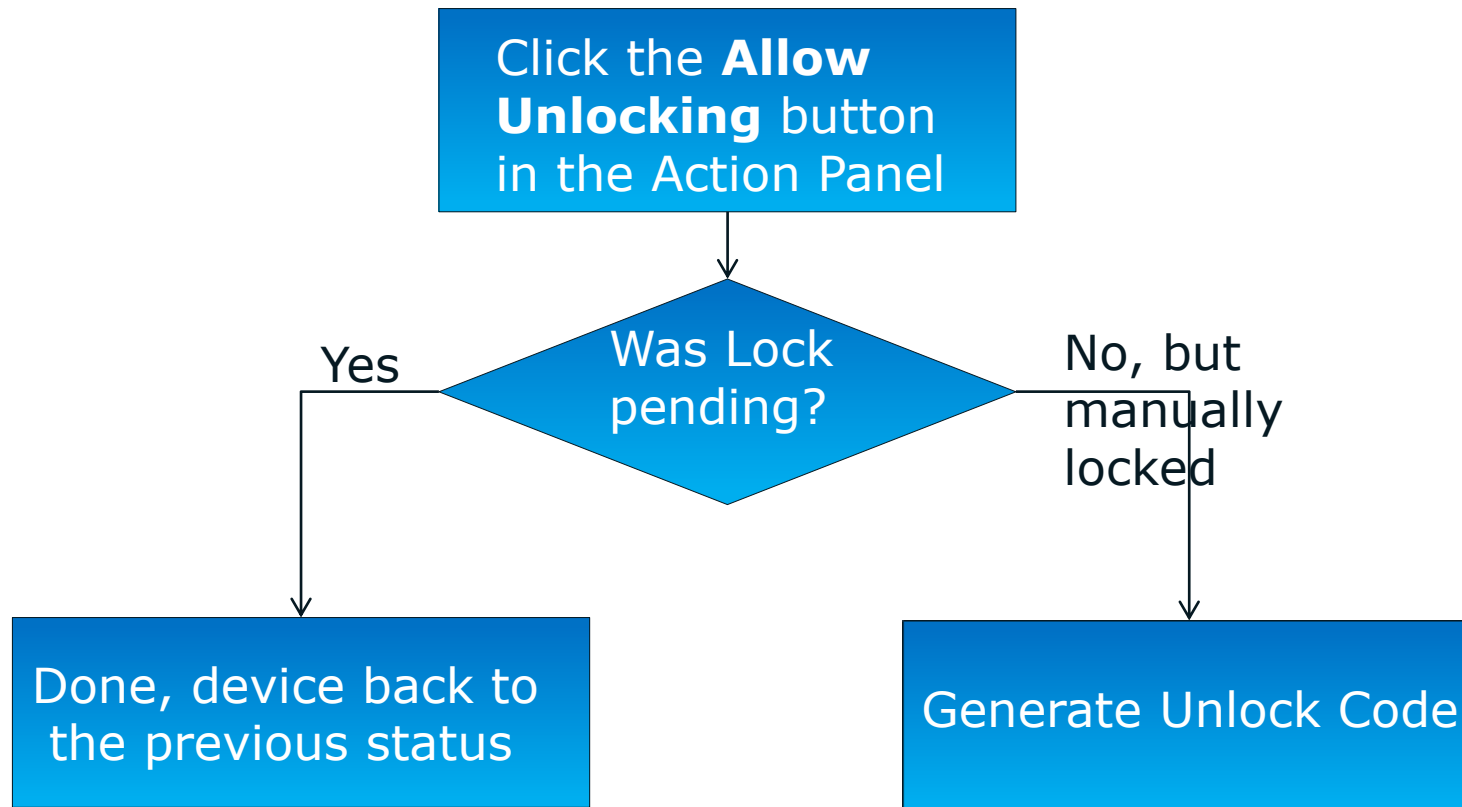
Step 1: Click the **Lock** button in the **Action** Panel.

Step 2: In the **Lock Device** window, input a lock comment and click **Lock Device**.

Step 3: Once connected to the server, the status changes from **Lock pending** to **Manually Locked** automatically.

Inventory: Device Management

➤ Allow Unlocking:



Inventory: Device Management

➤ Generate Unlock Code:

Hardware ID	Device Name	Boot Tick	Unlock Code
B0825348887B	android_92dc8390dc82016a	6	4016007013
49DCDD0001ED	CMPC-01-493	18	5122761142

Step 1: Click the **Generate Unlock Code** button in the panel.

Step 2: Check the **Boot Tick** number. Reset it if it's not identical to that displayed on the lock screen.

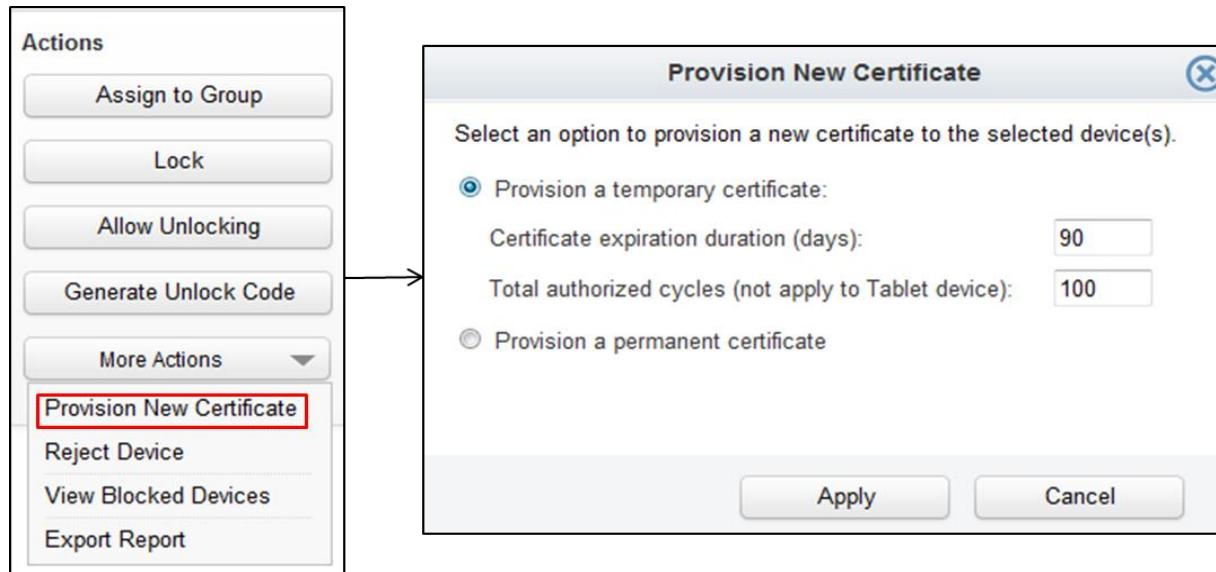
Step 3: Use the **Unlock Code** to unlock the device

Note: 1. Make sure Device Boot Tick -5 ≤ The Boot Tick you input on the server ≤ Device Boot Tick +1
2. This function can be achieved on the **Pending New Devices** page with the same steps as above



Inventory: Device Management

3. Provision New Certificates



Step 1: Click the **Provision New Certificate** button

Step 2: Input **Certificate expiration duration** and **Total authorized cycles** values(for a temporary certificate).

Inventory: Device Management

Threshold values for different certificates:

Certificate Type	Default	Expiration Day Limit		Remaining Cycle Limit (not applicable for Tablet)	
Warning Threshold	Day = 15 Cycle = 50	A1 Days	$1 \leq A1 < B1 \leq 30$	A2 cycles	$20 \leq A2 < B2 \leq 300$
Global Certificate	Day = 90 Cycle = 300	B1 Days	$A1 < B1 \leq 30$	B2 cycles	$(A2 + 10) \leq B2 \leq 20000$
Temporary Certificate		C1 Days	$A1 < C1 \leq 999$	C2 cycles	$(A2 + 10) \leq C2 \leq 20000$

Inventory: Device Management

4. Reject Devices

Step 1: Click the **Reject Device** button in the **Actions** panel

Step 2: Click **Yes** on the confirmation window

- Recover the device to its previous status:

Step1: Click **View Blocked Devices**

Step2: Click the **Restore** button

- Delete the rejected devices permanently:

Step1: Click **View Blocked Devices**

Step2: Click the **Remove** button

Note: The above actions can be accessed on the **Pending New Devices** page as well



Inventory: Device Management

5. Transfer Device (Central Server Supported Mode)

- Requirement: Between servers activated by one central server
- On the original server: transfer-out
- On the destination server: transfer-in



Devices pending to be transferred into or out of the server

Note: You can execute offline transfer function under any mode.



Inventory: Device Management

➤ Transfer-out:

Step 1: Click the **Transfer** button in the **Action** Panel

Step 2: In the **Transfer Device** window, select the destination server. Click **Transfer Device**.

Step 3: Device will be in **Transfer-out** page under **Inventory**, waiting for destination's acceptance.



Note: You can only request to transfer devices in **Normal**, **About to Expire**, or **Permanent** status.

Inventory: Device Management

➤ Transfer-in:

- Step 1: On the **Transfer-in** page under **Inventory**, select the device in **Pending Acceptance** status.
- Step 2: Click the **Accept Transfer** button in the **Action** Panel.
- Step 3: Connect the device to the server to prepare transfer package.
- Step 4: Connect again to complete.



Note: You can only accept or reject devices in Pending Acceptance status.

Inventory: Device Management

➤ Transfer locked device:

Step 1: On the **Transfer-in** or **Transfer-out** page under **Inventory**, select the locked device.

Step 2: Click the **Export School Package** button in the **Action** Panel and select a location to save the package.

Step 3: Copy the package to a removable disk and import it to the locked device.

Step 4: Connect the device to the destination to finish.



Note: You can only export school packages for one device in **Awaiting check-in** status at one time.



Group & Account

➤ Manage Groups

- Create Group

- Edit Group

- Delete Group

- Export Group

Export group information to .CSV file.

- Import Group

Import group information from .CSV file.

Group	E-mail	Phone No.	Description	Contact Person

Group & Account

➤ Manage Accounts

➤ Create Accounts

Step 1: Click the **Create User Account** button.

Step 2: Input a username.

Step 3: Select the role and assign functions.

Step 4: Complete user info, and assign a group.

➤ Edit Group

➤ Delete Group



Note: Assign devices pending for approval or transfer-in to the **Ungrouped** category.



Settings: Outline

General

- Offline Boot Certificate
- Import Device
- Email Notification Setting
- SMS Notification

Server

- Automatic Server Broadcast
- Automatic Device Approval
- Support E-mail Server
- Customized Columns

Client

- Global Certificate
- Check-in Interval
- Password Protection
- Student Unlock Code
- Unknown Device Remote Unlock

Security

- Update Public Key
- Update Shared Secret
- Export the Public Key
- Import Pre-activate Package
- Recover Crashed Server
- Offline Transfer

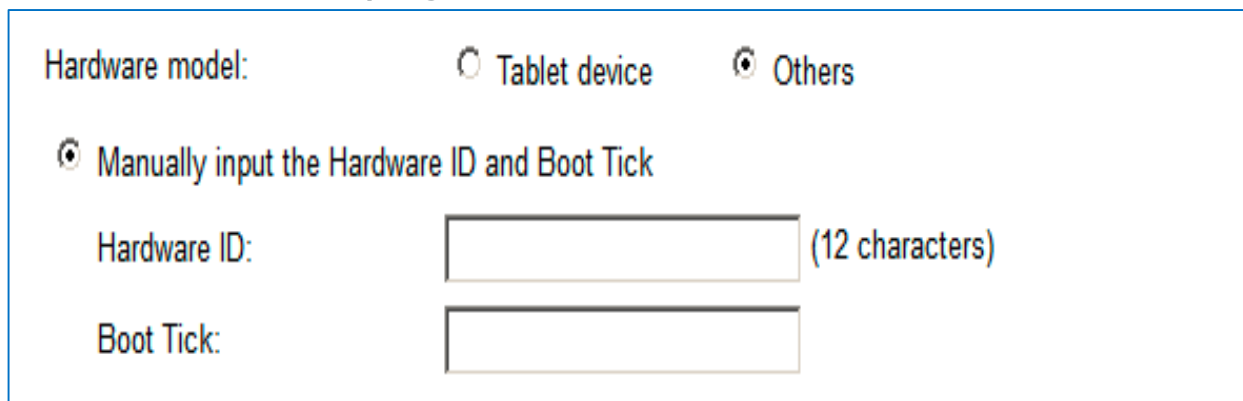
Advanced

- Set up Server
- Activate & Reactivate
- Server Backup
- Server Restore
- Set up Smart Update

Settings: General settings

➤ Offline Boot Certificate manually

Step 1: Find the **Offline Boot Certificate** area on the **General** page.



Hardware model: ☐ Tablet device ☒ Others

☒ Manually input the Hardware ID and Boot Tick

Hardware ID: (12 characters)

Boot Tick:

Step 2: Input information and click **Export** to get a certificate

Step 3: Copy the certificate(tpocc.bin) to a removable device and import it to the locked device.

Settings: General settings

➤ Offline Boot Certificate with CSV file

Step 1: Create a .csv containing the following columns with UTF-8 coding and the following formats:

<i>Hardware ID</i> <i>(Must have)</i>	<i>Boot Tick(must have)</i>
--	-----------------------------

<i>Id. de hardware</i> <i>(Must have)</i>	<i>Boot Tick(must have)</i>
--	-----------------------------

<i>ID do Hardware</i> <i>(Must have)</i>	<i>Boot Tick(must have)</i>
---	-----------------------------

<i>Donanım Kimliği</i> <i>(Must have)</i>	<i>Boot Tick(must have)</i>
--	-----------------------------

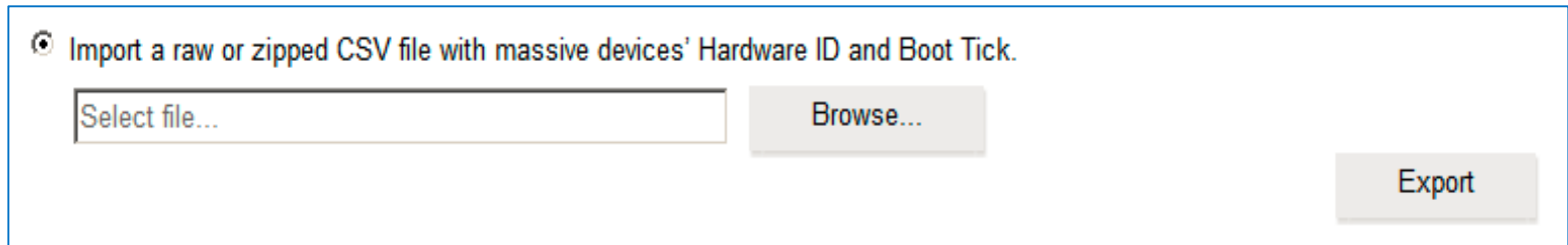
Settings: General settings

➤ Offline Boot Certificate with CSV file

Step 2: Select the **Hardware model** of your device(s).

Step 3: Choose **Import a raw or zipped CSV file with massive devices Hardware ID and Boot Tick.**

Step 4: Click **Browse** to choose this file and click the **Export** button to export the zip file with result and tcopp.bin under folder named as Hardware ID.



The screenshot shows a web interface for importing a CSV file. It features a radio button selected next to the text "Import a raw or zipped CSV file with massive devices' Hardware ID and Boot Tick.". Below this text is a text input field containing the placeholder "Select file...". To the right of the input field is a "Browse..." button. Further to the right is an "Export" button.

Note: Please split the CSV file if you want to export offline boot certificate for more than 50,000 devices.

Settings: General settings

➤ Import Device

Step 1: Export the .csv file from Device Management page or create one encoded in one of the following forms:

<i>Hardware ID (Must have)</i>	<i>Group (Optional)</i>	<i>Device Name (Optional)</i>	<i>Student Name (optional)</i>	<i>Serial No. (Optional)</i>	<i>Vendor (Optional)</i>	<i>Student ID No. (Optional)</i>	<i>Class No. (Optional)</i>
------------------------------------	-----------------------------	-----------------------------------	------------------------------------	----------------------------------	------------------------------	--------------------------------------	---------------------------------

<i>Id. de hardware (Must have)</i>	<i>Grupo (Optional)</i>	<i>Nombre de dispositivo (Optional)</i>	<i>Nombre de estudiante (optional)</i>	<i>N.º de serie (Optional)</i>	<i>Vendor (Optional)</i>	<i>Student ID No. (Optional)</i>	<i>Class No. (Optional)</i>
--	-----------------------------	---	--	------------------------------------	------------------------------	--------------------------------------	---------------------------------

<i>ID do Hardware (Must have)</i>	<i>Grupo (Optional)</i>	<i>Nome do Dispositivo (Optional)</i>	<i>Nome do Aluno (optional)</i>	<i>Número de Série (Optional)</i>	<i>Vendor (Optional)</i>	<i>Student ID No. (Optional)</i>	<i>Class No. (Optional)</i>
---------------------------------------	-----------------------------	---	-------------------------------------	---------------------------------------	------------------------------	--------------------------------------	---------------------------------

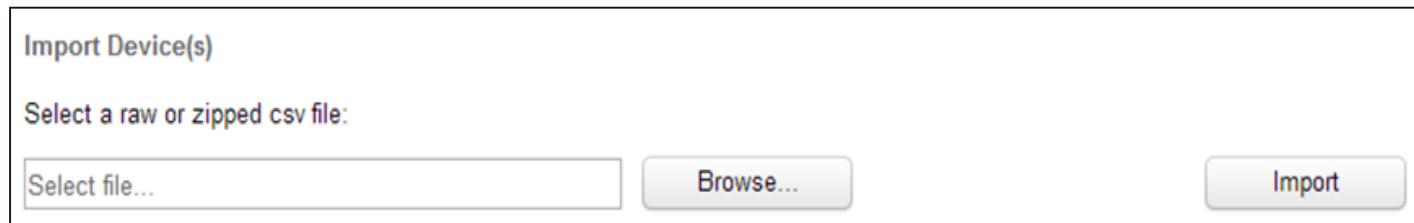
<i><u>Donanım Kimliği</u> (Must have)</i>	<i>Grup (Optional)</i>	<i>Cihaz Adı (Optional)</i>	<i>Öğrenci Adı (optional)</i>	<i>Seri No. (Optional)</i>	<i>Vendor (Optional)</i>	<i>Student ID No. (Optional)</i>	<i>Class No. (Optional)</i>
---	----------------------------	---------------------------------	-----------------------------------	--------------------------------	------------------------------	--------------------------------------	---------------------------------

Settings: General settings

➤ Import Device

Step 2: Zip or split the .csv file to make a single file < 50MB

Step 3: Find **Import Device(s)** on the **General** page



Import Device(s)

Select a raw or zipped csv file:

Select file... Browse... Import

Step 4: Test for import begins, with a summary report shown

Step 5: Click **Commit** to import



Note: Make sure you have the authorization to access the groups of the imported devices




Settings: General settings

➤ Email Notification Setting (for device info reports)

Step 1: Turn on the E-mail Notification function.

Step 2: Set addresses and sending frequency. Separate multiple addresses by a commas.

E-mail Notification



Send a summary report to my e-mail box regularly. You can input several e-mail addresses separated by commas.

E-mail:

Frequency: Every days

[Send a summary report now](#)

Save

Settings: General settings


➤ SMS Notification

Step 1: Turn on the SMS Notification function.

Step 2: Connect the server to an Android phone with TD SMS.

Step 3: Set receivers' phone numbers and sending frequency.
Separate multiple numbers by a comma.

SMS Notification



Send a summary report to mobile phone(s) regularly. The phone numbers can be separated by commas. Please refer to the [user manual](#) on how to setup the environment.

PIN Code :

Phone number:

Frequency: Every days

[Send a summary report now](#)

[Save](#)



Settings: Server settings

➤ Automatic Server Broadcast

Requirements:


Server Name & Address setup

Server and clients deployed in LAN.

Step 1: Turn on the **Automatic Server Broadcast** function.

Step 2: Input a frequency number (in minutes).

Step 3: Click the **Save** button.

Automatic Server Broadcast 

You can enable the server to broadcast its address so that the devices in the same network will be able to detect this server.

Broadcast frequency: every minutes

Save

Settings: Server settings

➤ Automatic Device Approval

Step1: Turn on the **Automatic Device Approval** function.

Step2: Select whether you want to always approve new devices automatically or approve new devices automatically till a certain date.

Step3: Click the **Save** button.

Automatic Device Approval

☒

You can enable the server to approve the pending devices automatically.

☒ Always approve automatically

☐ Approve automatically by: 

Save



AL

Note: Not for devices with hardware errors or installed with an earlier version of the client.


Settings: Server settings

➤ E-mail Server

Step1: Input the required information into the blanks.

Step2: Click the **Save** button

E-mail to Users



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

E-mail username:

admin@test.com

E-mail password:

••••••

SMTP server:

smtp.test.com

Port:

25

Security mode:

☐ None ☒ SSL support ☐ TSL support

Test...

Save

Settings: Server settings

➤ Support E-mail

Step 1: Turn on the Support E-mail function.

Step 2: Set e-mail addresses if any and sending frequency.
Separate multiple addresses by a commas.

Support E-mail

☒

The server configuration mail will be sent to Theft Deterrent support team (tdsupport@intel.com) regularly if turn on the feature. You can add your own support e-mail address(es) to receive the mail.

E-mail:

Frequency:

Every days

[Send a summary report now](#)

☒ Saved successfully.

Save



AL

Note: Make sure you have turned on the [E-mail server](#) function before using this function.

Settings: Server settings

➤ Customized Columns

Step 1: Turn on one or more customized column settings.

Step 2: Input the title of your customized column for each enabled setting. Make sure the name is different from existing ones.

Step 3: Click the **Save** button.

Customized Columns

You can add up to 3 customized columns for a device. Please avoid the use of existing column's title for your customized columns.

Column 1:	<input checked="" type="checkbox"/>	<input type="text" value="Vendor"/>
Column 2:	<input checked="" type="checkbox"/>	<input type="text" value="Student ID No."/>
Column 3:	<input checked="" type="checkbox"/>	<input type="text" value="Class No."/>


Save

Settings: Server settings

➤ Customized Columns

Step 4: On the **Inventory** page, you can display the customized column(s) by checking the customized column's title in the drop-down list.

Device Management | Transfer-in (9) | Transfer-out (17) | Pending New Devices (3)

All devices | [Select all 162 devices](#) 

<input type="checkbox"/>	Hardware ID	Vendor	Device Name	Hardware Model	Gateway	Last Check-in	Status
<input type="checkbox"/>	99C4330000C7	mobile	CMPC-01-199	Unknown classmate P	202.126.210.184	2014-06-28	✓
<input type="checkbox"/>	877C7D0000C3		CMPC-00-195	Clamshell	61.137.211.173	2014-01-23	✓
<input type="checkbox"/>	E8095F0000C2		CMPC-01-194	Clamshell	61.90.109.187	2014-01-12	⚠
<input type="checkbox"/>	210DB80000C1		CMPC-01-193	Clamshell	211.226.69.207	2013-12-27	✓
<input type="checkbox"/>	D256C50000BF		CMPC-00-191	Unknown classmate P	211.139.191.194	2013-12-29	✓
<input type="checkbox"/>	DD74E40000BE		CMPC-01-190	Clamshell	211.38.53.57	2014-04-30	✓
<input type="checkbox"/>	298B7C0000BD		CMPC-01-189	Tablet	211.151.252.225	2014-03-13	✓
<input type="checkbox"/>	9BB6890000BC		CMPC-01-188	Clamshell	211.247.252.52	2014-05-08	⚠
<input type="checkbox"/>	B3569C0000BB		CMPC-01-187	Not a classmate PC	202.176.43.95	2014-05-09	✓
<input type="checkbox"/>	1DA36E0000BA		CMPC-00-186	Unknown classmate P	61.5.253.234	2014-05-02	✓
<input type="checkbox"/>	44A0140000B9		CMPC-01-185	Unknown classmate P	61.221.40.20	2014-01-08	✓
<input type="checkbox"/>	FB4CBD0000B8		CMPC-01-184	Clamshell	61.10.161.167	2014-05-07	⚠
<input type="checkbox"/>	836A5D0000B7		CMPC-01-183	Convertible	211.171.38.38	2013-12-28	✓
<input type="checkbox"/>	C5135D0000B6		CMPC-00-182	Convertible	202.202.132.25	2014-05-02	✓
<input type="checkbox"/>	F7A76C0000B5		CMPC-01-181	Convertible	202.213.179.101	2014-06-21	✓

Selected Devices: 0 / 162

Page 1 of 11 | 15

☐ Show All
☒ Hardware ID
☐ Group
☒ Device Name
☐ Student Name
☐ Serial No.
☒ Hardware Model
☐ IP Address
☒ Gateway
☒ Last Check-in
☐ Expiration Date
☐ Remaining Cycles
☐ Client Version
☒ Status
☒ Vendor
☐ Student ID No.
☐ Class No.
[Reset to default](#)

Settings: Server settings

➤ Customized Columns

Step 5: You can modify the customized information for each device by viewing its Device Details and clicking **Edit Device** button. Or you can import the customized information in a batch through [importing devices](#) function.



AL

Settings: Client settings

➤ Configure Global Certificate

Step1: Input the required information into the blanks.

Step2: Click the **Save** button

Global Certificate

You can set up the global certificate for all devices. The devices that are about to expire will request for the global certificate automatically.

Certificate expiration duration:	<input type="text" value="90"/>	days
Total authorized cycles:	<input type="text" value="200"/>	(not apply to Tablet device)
Expiration warning threshold:	<input type="text" value="20"/>	days, and/or <input type="text" value="20"/> cycles remaining
Boot certificate limit:	<input type="text" value="3"/>	times within <input type="text" value="30"/> days

Save

Settings: Client settings

➤ Configure Check-in Interval

Step1: Input the check-in interval(in minutes) for devices in different status

Step2: Click the **Save** button

Check-in Interval

You can set up the interval for devices in different status to check-in with the server automatically.

Device is normal:	<input type="text" value="120"/>	minutes
Device is about to expire:	<input type="text" value="30"/>	minutes
Device cannot connect to server:	<input type="text" value="60"/>	minutes

Save

- Note:**
1. Modification works only after device checks in
 2. Devices in two status concurrently checks in with a shorter interval
 3. Quick check-in when system starts up or user changes the server address



Settings: Client settings


➤ Set Client Password Protection

Requirements:

Password length must be less than 30 characters

➤ Configure Student Unlock Code

Student Unlock Code



You can enable students to generate unlock code(s) from the Theft Deterrent server student webpage. Also, you can set the maximum number of times that a student can generate unlock code(s).

Unlock Code limit: times within days

☒ The Student Name and Email are mandatory.

Save

Note: The student name and email could be configured to be mandatory.




Settings: Client settings

➤ Unknown Device Remote Unlock

- For pre-activated tablet devices which supports remote unlocking
- For devices pre-activated with a Public Key in the server keystore. click **Unlock through network**.
- Otherwise, import the pre-activate or crash recovery package with a temporary boot certificate to unlock

Unknown Device Remote Unlock



You can enable the remote unlock function for tablet devices that are not managed by the server yet if the clients are pre-activated with a Public Key associated with the server.

☒ Enable the function for devices pre-activated with a Public Key not in the server keystore.

The maximum Boot Tick supported:

Save



Settings: Security settings

➤ Update Public Key

Step 1: Update key pair on the sever on the **Security** page

Public Key

You can update, export or import the Public Key of the server. Please follow the [detailed procedure](#).

Update the Public Key for security issues.

Update Public Key

Step 2: Connect unlocked device to server to finish update. For locked device, continue the following steps.

Step 3: Click **Synchronize Packages** to enter **Package Sync** page

Settings: Security settings

Step 4: Select the device and export a tcopp.bin file

Device Management (432)
Transfer-in (18)
Transfer-out (17)
Pending New Devices (9)
Package Sync ✖

Package Sync

Select all 432 devices

<input type="checkbox"/>	Hardware ID	Group	Device Name	Serial No.	IP Address	Last Check	Expiration Date	Remaining	Status
<input type="checkbox"/>	872AD80001F	Applegate Primary	CMPC-00-4524ddb2dc-0ed0-4		10.216.54.159	2013-06-01	2013-12-22	6381	✓
<input type="checkbox"/>	088B710001F	Grant High School	CMPC-01-4549f5fed4-00ea-4b		10.216.36.17	2013-04-14	2014-04-07	9375	✓
<input checked="" type="checkbox"/>	6C48C10001F	Grant High School	CMPC-01-45d852378d-a040-4		10.216.152.149	2013-03-20	2014-03-04	1990	✓
<input type="checkbox"/>	6569610001F	Grant High School	CMPC-01-4588947622-ea8b-4		10.216.105.66	2013-05-01	2013-08-19	1792	⚠
<input type="checkbox"/>	2CA2130001E	Grant High School	CMPC-00-4582143ca6-6c11-4		10.216.104.175	2013-05-04	2013-09-15	6892	✓
<input type="checkbox"/>	7FC3B80001E	Middle School 0010	CMPC-00-4581118765-35a0-4		192.168.220.79	2013-04-14	2014-01-22	4359	✓
<input type="checkbox"/>	6954370001E	Middle School 0010	CMPC-01-45cc74f331-5672-40		192.168.168.215	2013-07-11	2013-11-19	497	✓
<input type="checkbox"/>	3289D80001E	Grant High School	CMPC-00-4531e3c447-03f0-45		10.216.140.14	2013-06-22	2014-04-18	7499	?
<input type="checkbox"/>	FE6A390001E	Middle School 0010	CMPC-00-45c290e037-e532-4		10.216.30.149	2013-03-06	2013-09-27	6688	✓
<input type="checkbox"/>	ABC2900001E	Middle School 0010	CMPC-00-4547505bce-fd07-45		192.168.201.202	2013-01-08	2013-12-12	6344	⚠

Search & Filter

All devices
All status
Enter criteria...

Actions

Update Shared Secret
Export Shared Secret
Export Public Key Package

Step 5: Copy the file to a storage device, and import it to our device to update

Settings: Security settings

➤ Update Shared Secret

- Used when unlock code cannot be generated, or device cannot be unlocked by unlock code.

Step 1: Click the **Synchronize Packages** button to enter **Package Sync** page

Step 2: Select the device and click **Update Shared Secret**

Step 3: Connect unlocked device to server to finish update. For locked device, continue the following steps.

Settings: Security settings

Step 4: Select the device and click **Export Shared Secret** to export a tcopp.bin file

Device Management (432) | Transfer-in (18) | Transfer-out (17) | Pending New Devices (9) | Package Sync

Package Sync Select all 432 devices

<input type="checkbox"/>	Hardware ID	Group	Device Name	Serial No.	IP Address	Last Check	Expiration Date	Remaining	Status
<input type="checkbox"/>	872AD80001F	Applegate Primary	CMPC-00-4924ddb2dc-0ed0-4	10.216.54.159	2013-06-01	2013-12-22	6381		
<input type="checkbox"/>	088B710001F	Grant High School	CMPC-01-4949f5fed4-00ea-4b	10.216.36.17	2013-04-14	2014-04-07	9375		
<input checked="" type="checkbox"/>	6C48C10001F	Grant High School	CMPC-01-49d852378d-a040-4	10.216.152.149	2013-03-20	2014-03-04	1990		
<input type="checkbox"/>	6569610001F	Grant High School	CMPC-01-4988947622-ea8b-4	10.216.105.66	2013-05-01	2013-08-19	1792		
<input type="checkbox"/>	2CA2130001E	Grant High School	CMPC-00-4982143ca6-6c11-4	10.216.104.175	2013-05-04	2013-09-15	6892		
<input type="checkbox"/>	7FC3B80001E	Middle School 0010	CMPC-00-4981118765-35a0-4	192.168.220.79	2013-04-14	2014-01-22	4359		
<input type="checkbox"/>	6954370001E	Middle School 0010	CMPC-01-49cc74f331-5672-4	192.168.168.215	2013-07-11	2013-11-19	497		
<input type="checkbox"/>	3289D80001E	Grant High School	CMPC-00-4931e3c447-03f0-4	10.216.140.14	2013-06-22	2014-04-18	7499		
<input type="checkbox"/>	FE6A390001E	Middle School 0010	CMPC-00-49c290e037-e532-4	10.216.30.149	2013-03-06	2013-09-27	6688		
<input type="checkbox"/>	ABC2900001E	Middle School 0010	CMPC-00-4947505bce-fd07-4	192.168.201.202	2013-01-08	2013-12-12	6344		

Search & Filter

All devices

All status

Enter criteria...

Actions

Update Shared Secret

Export Shared Secret

Export Public Key Package

Step 5: Copy the file to a storage device, and import it to our device to update

Settings: Security settings

➤ Export the Public Key

- Used for crash recovery or pre-activation

Step 1: On the **Security** Page, click the **Export** button in the **Public Key** area.

Step 2: Select the **Server Public Key** and/or the **Root Public Key** you want to export .



Step 3: Click the **Export** Button to export the server Public Key (file named as Pub_Key.bin) and/or Root Server Public Key (file named as CmpcRoot.pubkey).

Settings: Security settings

➤ Import Pre-activate Package

- For pre-activated devices with a Public Key not in the keystore
- Automatically done if the server had been activated on the central server

Step 1: On the **Security** page, click **Export** in the **Public Key** area to export the server Public Key

Step 2: Obtain the pre-activated package from the central server admin by providing the server Public Key

Step 3: Import the pre-activate package by referring to the steps of importing offline Transfer-in Package.

Settings: Security settings

➤ Recover Crashed Server

- Used when the server key is lost permanently

Step 1: Install a new server

Step 2: Get crashed server's **Provision Number** from its client

Step 3: Request a **transfer-in package** from the central server or root CA server admin

Step 4: Import the crash recovery package by referring to the steps of importing offline Transfer-in Package.



Offline Transfer- Transfer-in

➤ Offline Transfer-in

Step1: In the **Transfer Packages** area, select **Transfer-in Package**

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☒ Transfer-in Package ☐ Transfer-out Package

Import Transfer-in Package:

[View Transfer-in Package](#)

Offline Transfer- Transfer-in

Step2: Click the Browse button to locate the **tcopp.bin** or **tcopp_XXXXXXXXXXXXXXXXXXXXX_XXXXXXXXXXXXXXXXXXXXX.b** in file.

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☒ Transfer-in Package ☐ Transfer-out Package

Import Transfer-in Package:

Provision Number:

(20 characters)

[View Transfer-in Package](#)



Note: For **tcopp.bin** file, input **Provision Number** in the blank area.

Offline Transfer- Transfer-in

Step3: Click the **Import** button.

Step4: You can view all imported transfer-in packages by clicking the **View Transfer-in Package**

Transfer-in Package		
Source Provision Number	Destination Provision Number	Package Name
040cf8ef1c85835c475a	80ddb6225f90e9f66727	tcopp_80ddb6225f90e9f66727_040cf8ef1c85835c475a.bin
f5f4186e85879aa1d8ba	80ddb6225f90e9f66727	tcopp_80ddb6225f90e9f66727_f5f4186e85879aa1d8ba.bin
Page 1 of 1		
Close		

Note: Note: If a device with unmatched provision number tries to connect with the server, TD server will check whether the transfer-in package applied to the device or not. After the device successfully downloads and applies the transfer-in package, the device will appear as a new device under **Inventory**.

Offline Transfer- Transfer-out

➤ Offline Transfer-out

- ✓ Import the transfer-out package

Step1: In the **Transfer Packages** area, select **Transfer-out Package**

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☐ Transfer-in Package ☒ Transfer-out Package

Import Transfer-out Package:

Provision Number: (20 characters)

[View Transfer-out Package](#)

Offline Transfer- Transfer-out

Step2: Click the **Browse** button to locate the **tcopp.bin** or **tcopp_XXXXXXXXXXXXXXXXXXXXX_XXXXXXXXXXXXXXXXXXXXX.bin** file.

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☐ Transfer-in Package ☒ Transfer-out Package

Import Transfer-out Package:

Browse...

Import

[View Transfer-out Package](#)

For **tcopp.bin** file, input **Provision Number** of the tcopp.bin in the blank area.

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☐ Transfer-in Package ☒ Transfer-out Package

Import Transfer-out Package:

Browse...

Source Provision Number:

(20 characters)

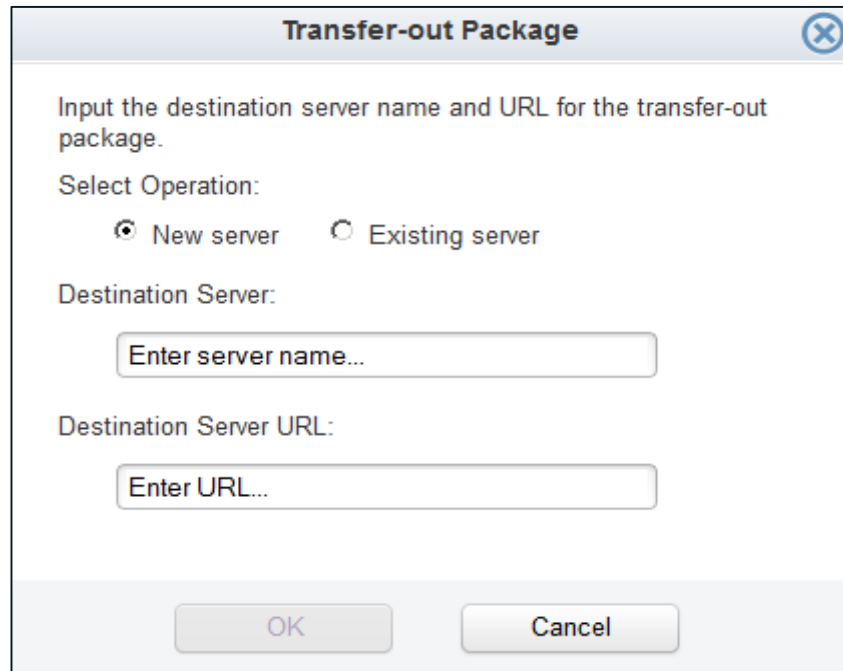
View Transfer-out Package

Import

Offline Transfer- Transfer-out

Step3: Click the **Import** button.

Step4: On the pop-up window, input the Destination server name and URL.



The screenshot shows a dialog box titled "Transfer-out Package" with a close button in the top right corner. Inside the dialog, there is a text label: "Input the destination server name and URL for the transfer-out package." Below this, there is a section labeled "Select Operation:" with two radio buttons: "New server" (which is selected) and "Existing server". Below the radio buttons, there is a label "Destination Server:" followed by a text input field containing the placeholder text "Enter server name...". Below this, there is a label "Destination Server URL:" followed by a text input field containing the placeholder text "Enter URL...". At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

Note: You can overwrite the transfer-out package for an existing destination server by selecting the **Existing Server** button in case of Public Key of the server was updated.



Offline Transfer- Transfer-out

Step5: You can view all imported transfer-out packages by clicking the **View Transfer-out Package**.

Transfer Packages

You can import the Transfer-in package for pre-activate or crash recovery, Transfer-out packages for offline device transfer. Please refer to the [detailed procedure](#).

Select Operation: ☐ Transfer-in Package ☒ Transfer-out Package

Import Transfer-out Package:

[View Transfer-out Package](#)

Transfer-out Package

Click a Destination Server Name or Destination Server URL to change the settings.

Source Provision Number	Destination Provision Number	Destination Server Name	Destination Server URL
abbc026871818b466fd7,45dd2a4902	75369d43713af78d8bca	1	https://1

Page 1 of 1

Note: You can click the **Destination Server Name** and **Destination Server URL** to change settings according to the destination server you choose. All the packages with the same destination provision number will be listed in one row



Offline Transfer- Transfer-out

- ✓ Select the devices you want to transfer out and complete the following steps:

Step1: On the **Device Management** page under **Inventory**, select the devices you want to transfer out and click the **Transfer** button.

The screenshot shows the Intel Theft Deterrent server interface. The top navigation bar includes 'Education', 'Home', 'Inventory', 'Groups & Accounts', and 'Settings'. The 'Inventory' tab is active, showing 'Transfer-in (4)', 'Transfer-out (11)', and 'Pending New Devices (3)'. The 'All devices' section displays a table of devices. The 'Transfer' button is highlighted in the 'Actions' panel on the right.

Hardware ID	Group	Device Name	Hardware Model	Gateway	Last Check-in	Status
EC67330000C7	Middle School 001	CMPC-01-199	Not a classmate PC	211.9.11.240	2014-02-06	✓
CDA5900000C6	ShangHai Foreign Lar	CMPC-00-198	Unknown classmat	211.222.11.238	2014-02-10	✓
412BB50000C5		CMPC-01-197	Convertible	211.5.215.89	2013-12-03	✓
2AE6890000C4	Grant High School	CMPC-01-196	Convertible	61.236.128.41	2014-03-11	✓
B355A50000C3		CMPC-00-195	Clamshell	202.251.162.240	2013-10-13	✓
8AC29B0000C2	Jupiter Space Institute	CMPC-00-194	Unknown classmat	211.196.104.126	2014-04-08	✓
8585D70000C0		CMPC-00-192	Unknown classmat	202.66.28.202	2013-11-22	✓
17D3090000BF	Hoover High School	CMPC-01-191	Clamshell	202.246.86.147	2014-03-25	✓
C4A4820000BE	ShangHai Foreign Lar	CMPC-00-190	Unknown classmat	211.118.26.86	2014-01-11	✓
B214E90000BD		CMPC-00-189	Convertible	202.110.56.116	2014-04-03	✓
FA8F760000BC	Jupiter Space Institute	CMPC-01-188	Convertible	61.58.39.218	2013-11-25	✓
07B0050000BB	Riverview Primary Sch	CMPC-00-187	Convertible	202.156.62.188	2013-12-25	✓
B306180000BA	Riverview Primary Sch	CMPC-01-186	Clamshell	202.71.32.209	2013-12-17	✓
B899D70000B9	Wilson High School	CMPC-01-185	Tablet	202.141.89.227	2014-02-13	✓
1A84790000B8	Applegate Primary Sch	CMPC-01-184	Clamshell	211.219.177.10	2014-04-09	⚠

Selected Devices: 2 / 171

Page 1 of 12

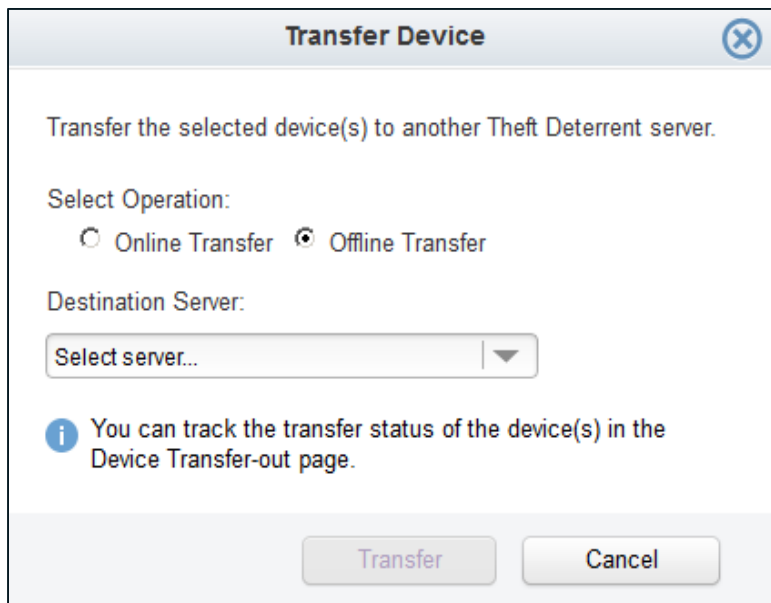
Actions:

- Assign to Group
- Lock
- Allow Unlocking
- Generate Unlock Code
- More Actions
- Provision New Certificate
- Transfer**
- View Transfer History
- Reject Device
- View Blocked Devices
- Export Report

Offline Transfer- Transfer-out

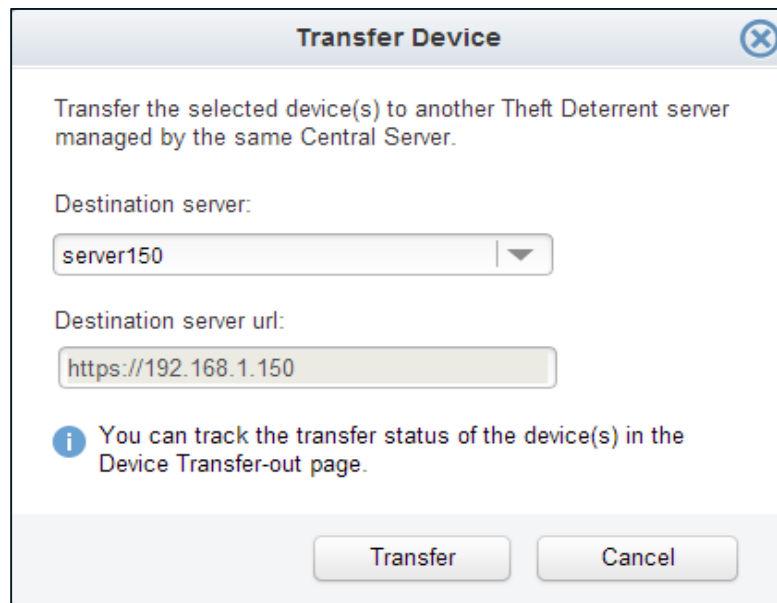
Step2: On the pop-up window, select **Offline Transfer** if your server is **Central Server Supported mode**. Then select the destination server name and URL, and click **Transfer** button.

With Central Server Supported Mode



The screenshot shows a 'Transfer Device' window with a title bar containing a close button. The main text reads: 'Transfer the selected device(s) to another Theft Deterrent server.' Below this, under 'Select Operation:', there are two radio buttons: 'Online Transfer' (unselected) and 'Offline Transfer' (selected). Under 'Destination Server:', there is a dropdown menu with the text 'Select server...'. At the bottom, there is an information icon followed by the text: 'You can track the transfer status of the device(s) in the Device Transfer-out page.' and two buttons: 'Transfer' and 'Cancel'.

Without Central Server Supported Mode



The screenshot shows a 'Transfer Device' window with a title bar containing a close button. The main text reads: 'Transfer the selected device(s) to another Theft Deterrent server managed by the same Central Server.' Below this, under 'Destination server:', there is a dropdown menu with the text 'server150'. Under 'Destination server url:', there is a text input field containing 'https://192.168.1.150'. At the bottom, there is an information icon followed by the text: 'You can track the transfer status of the device(s) in the Device Transfer-out page.' and two buttons: 'Transfer' and 'Cancel'.

Offline Transfer- Transfer-out

Step3: The selected devices will be moved to **Transfer-out** page under **Inventory** with status **Transferring**

Step4: Once devices connect with your TD server, they will automatically download the transfer-out packages and statuses will change to **Downloading**.

Step5: If the devices reboot and connect with your TD server again, the transfer-out process will be confirmed as complete and these devices will be moved out of device list.

Step6: Once the device(s) complete the transfer, you can click **View History** to view the transfer history.

Offline Transfer- Transfer-out

Education
Home
Inventory
Groups & Accounts
Settings
TD3server

Device Management (166)
Transfer-in (4)
Transfer-out
Pending New Devices (3)

Device Transfer-out
Select all 17 devices

<input type="checkbox"/>	Hardware ID	Destination Server	Original Group	Device Name	IP Address	Status
<input type="checkbox"/>	ECA86BE67725	td2server		android-1bf1dccc9	192.168.1.116	Downloading
<input type="checkbox"/>	2AE6890000C4		Grant High School	CMPC-01-196	192.168.198.83	Transferring
<input type="checkbox"/>	B355A50000C3			CMPC-00-195	10.216.120.91	Transferring
<input type="checkbox"/>	EF52830000C1	JiangSu East Edu Serv	Jupiter Space Institute	CMPC-00-193	192.168.59.33	Pending Acceptance
<input type="checkbox"/>	8585D70000C0			CMPC-00-192	192.168.180.4	Transferring
<input type="checkbox"/>	C4A4820000BE		ShangHai Foreign Lar	CMPC-00-190	10.216.139.10	Transferring
<input type="checkbox"/>	FA8F760000BC		Jupiter Space Institute	CMPC-01-188	192.168.246.102	Transferring
<input type="checkbox"/>	2E09EE0000A9	JiangSu East Edu Serv	Dunthrope Middle Sch	CMPC-01-169	192.168.239.81	Pending Acceptance
<input type="checkbox"/>	8BA7F1000089	JiangSu West Edu Sen	Hoover High School	CMPC-00-137	10.216.16.23	Awaiting check-in
<input type="checkbox"/>	3562FB00007C	JiangSu West Edu Sen	Jupiter Space Institute	CMPC-00-124	10.216.125.103	Awaiting check-in
<input type="checkbox"/>	F9AD8C000074	JiangSu West Edu Sen	Wilson High School	CMPC-00-116	10.216.145.97	Pending Acceptance
<input type="checkbox"/>	EE1E28000066	JiangSu East Edu Serv	Grant High School	CMPC-01-102	10.216.124.12	Awaiting check-in
<input type="checkbox"/>	D3F2E800005B	JiangSu East Edu Serv		CMPC-01-91	192.168.10.140	Pending Acceptance
<input type="checkbox"/>	057206000051	JiangSu West Edu Sen	MinHang Middle Scho	CMPC-00-81	10.216.8.153	Awaiting check-in
<input type="checkbox"/>	42885D00003F	JiangSu East Edu Serv	ShangHai Foreign Lar	CMPC-00-63	10.216.85.178	Pending Acceptance

Search & Filter

All status

Enter criteria...

Actions

Cancel Transfer

View History

Export School Package

Complete Offline Transfer

i Once the device(s) complete the transfer, you can click "View History" to view the transfer history.

Selected Devices: 0 / 17
Page 1 of 2
15

Offline Transfer- Transfer-out

You can manually finish transfer by clicking the **Complete Offline Transfer** button in case of any exception happened to block the process complete automatically. Devices with status **Transferring** or **Downloading** will be moved out of device list.

The screenshot displays the 'Theft Deterrent server' interface. The top navigation bar includes 'Education', 'Home', 'Inventory', 'Groups & Accounts', and 'Settings'. The 'Inventory' tab is active, showing 'Device Management (166)', 'Transfer-in (4)', 'Transfer-out', and 'Pending New Devices (3)'. The 'Device Transfer-out' section is selected, displaying a table of 16 devices. The table columns are: Hardware ID, Destination Server, Original Group, Device Name, IP Address, and Status. The 'Complete Offline Transfer' button is highlighted in the 'Actions' panel on the right. A search and filter panel is also visible on the right side of the table.

Hardware ID	Destination Server	Original Group	Device Name	IP Address	Status
<input type="checkbox"/> 2AE689000C4		Grant High School	CMPC-01-196	192.168.198.83	Transferring
<input type="checkbox"/> B355A5000C3			CMPC-00-195	10.216.120.91	Transferring
<input type="checkbox"/> EF5283000C1	JiangSu East Edu Serv	Jupiter Space Institute	CMPC-00-193	192.168.59.33	Pending Acceptance
<input type="checkbox"/> 8585D7000C0			CMPC-00-192	192.168.180.4	Transferring
<input type="checkbox"/> C4A482000BE		ShangHai Foreign Lar	CMPC-00-190	10.216.139.10	Transferring
<input type="checkbox"/> FA8F76000BC		Jupiter Space Institute	CMPC-01-188	192.168.246.102	Transferring
<input type="checkbox"/> 2E09EE000A9	JiangSu East Edu Serv	Dunthrope Middle Sch	CMPC-01-169	192.168.239.81	Pending Acceptance
<input type="checkbox"/> 8BA7F100089	JiangSu West Edu Ser	Hoover High School	CMPC-00-137	10.216.16.23	Awaiting check-in
<input type="checkbox"/> 3562FB00007C	JiangSu West Edu Ser	Jupiter Space Institute	CMPC-00-124	10.216.125.103	Awaiting check-in
<input type="checkbox"/> F9AD8C000074	JiangSu West Edu Ser	Wilson High School	CMPC-00-116	10.216.145.97	Pending Acceptance
<input type="checkbox"/> EE1E28000066	JiangSu East Edu Serv	Grant High School	CMPC-01-102	10.216.124.12	Awaiting check-in
<input type="checkbox"/> D3F2E800005B	JiangSu East Edu Serv		CMPC-01-91	192.168.10.140	Pending Acceptance
<input type="checkbox"/> 057206000051	JiangSu West Edu Ser	MinHang Middle Scho	CMPC-00-81	10.216.8.153	Awaiting check-in
<input type="checkbox"/> 42885D00003F	JiangSu East Edu Serv	ShangHai Foreign Lar	CMPC-00-63	10.216.85.178	Pending Acceptance
<input type="checkbox"/> 8F8A3F00002A	JiangSu West Edu Ser	ShangHai Foreign Lar	CMPC-00-42	192.168.50.11	Awaiting check-in

Selected Devices: 0 / 16

Page 1 of 2

Language: Copyright © 2013 Intel Corporation. All Rights Reserved. Version 4.0.30103.10698

Search & Filter

All status

Enter criteria...

Actions

Cancel Transfer

View History

Export School Package

Complete Offline Transfer

Once the device(s) complete the transfer, you can click "View History" to view the transfer history.

Settings: Advanced settings

➤ Setup Server Name and Address

- Server Name: Displayed in Server header and client
- Server Address: Broadcasted to clients in the same LAN
- Download Log: Download the compressed log file(s)



Note: You can also find log files from

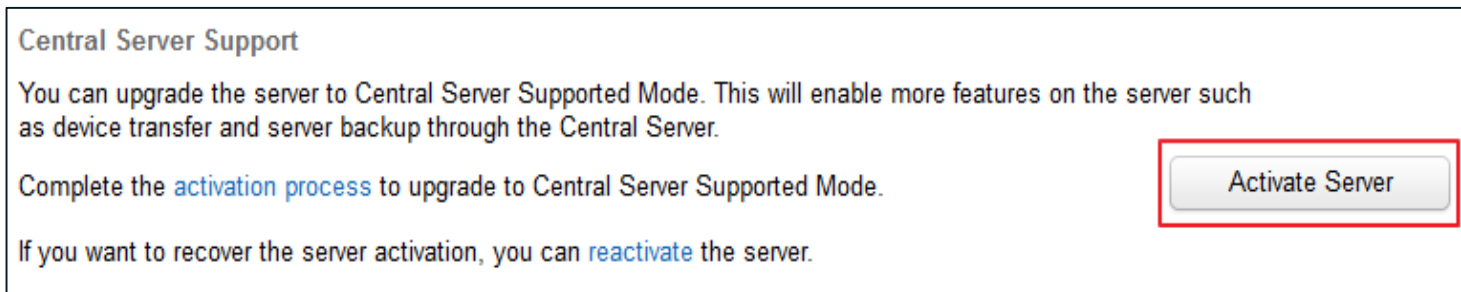
Linux: /var/log/theftdeterrentserver/opt/TheftDeterrentserver/Sites/logs

Windows: %systemdrive%\log\theftdeterrentserver

Settings: Advanced settings

➤ Activate Server

Step 1: On the **Advanced** page under **Settings**, click the **Activate Server** button



Step 2: Input information needed and click **Register Server**

Step 3: Receive an activation code to activate.

Settings: Advanced settings

➤ Reregister Server

Step 1: On the **Advanced** page under **Settings**, click the **Reregister** link

Step 2: Input information needed and click **Reregister Server** button

Central Server Support

The server is linked with the Central Server: 192.168.1.132

Update the server information registered on the Central Server.

If you want to register to a new Central server or recover the server activation, you can [reregister](#) or [reactivate](#) the server.

Update...

Step 3: Get approval and receive a re-registration code to reregister.

Settings: Advanced settings

➤ Reactivate Server

Step 1: Contact central server admin offline to request an activation code

Step 2: On the **Advanced** page under **Settings**, click the **reactivate** link

Central Server Support

You can upgrade the server to Central Server Supported Mode. This will enable more features on the server such as device transfer and server backup through the Central Server.

Complete the [activation process](#) to upgrade to Central Server Supported Mode.

Activate Server

If you want to recover the server activation, you can [reactivate](#) the server.

Central Server Support

The server is linked with the Central Server: 192.168.1.132

Update the server information registered on the Central Server.

Update...

If you want to register to a new Central server or recover the server activation, you can [reregister](#) or [reactivate](#) the server.

Step 3: On the **Activate Theft Deterrent Server** page, input information and click **Reactivate Server**

Settings: Advanced settings

➤ Server Backup(Stand-alone Mode)

➤ Auto backup

Step 1: On the **Advanced** page under **Settings**, select **Back up server data automatically**

Step 2: Input information needed, click **Save**

➤ Manual backup

Step 1: On the **Advanced** page under **Settings**, click **Back up**


Step 2: Input information needed and back up.

Server Backup

You can back up server data manually or set up automatic backup.

☒ Back up server data automatically every days

☒ Protect the backup file with password: [Show characters](#)

 Only the last 3 automatic backup files will be kept. Older backup files are deleted automatically.

[Back up server data manually.](#)

[Manage server backup files](#)

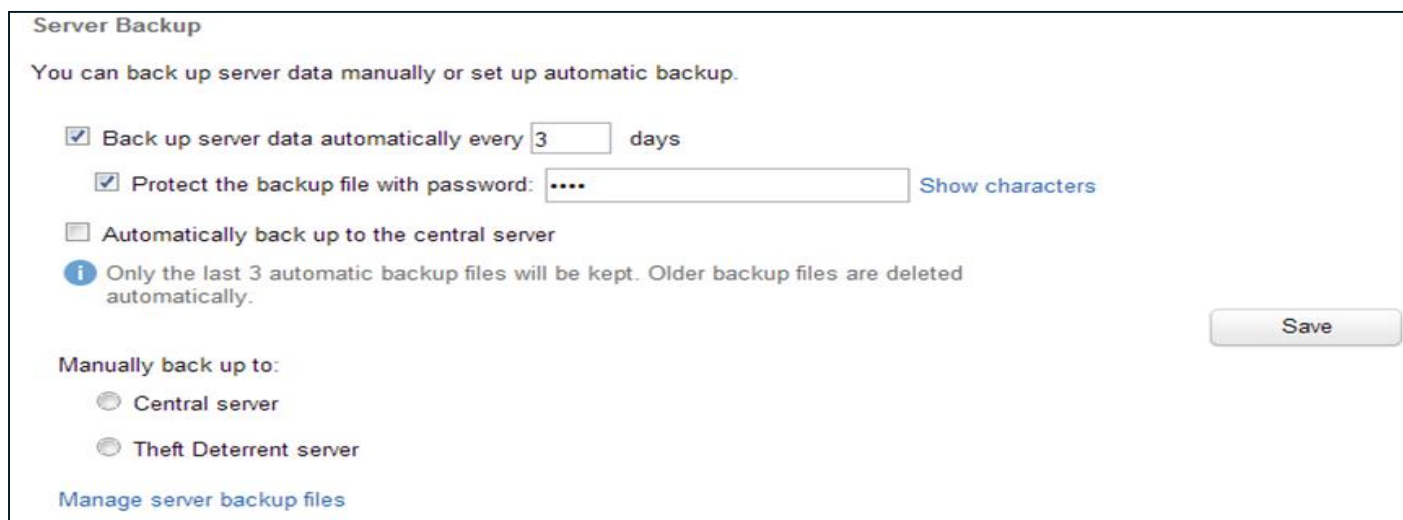
[Save](#)

[Back up](#)

Settings: Advanced settings

➤ Server Backup(Central Server Supported Mode)

➤ Auto backup



The screenshot shows a 'Server Backup' configuration window. At the top, it says 'You can back up server data manually or set up automatic backup.' Below this, there are three main sections. The first section, 'Automatic backup', has a checked checkbox for 'Back up server data automatically every 3 days'. The second checkbox, 'Protect the backup file with password', is also checked, with a password field containing four dots and a 'Show characters' link. The third checkbox, 'Automatically back up to the central server', is unchecked. An information icon and text state: 'Only the last 3 automatic backup files will be kept. Older backup files are deleted automatically.' A 'Save' button is on the right. The second section, 'Manually back up to:', has two radio button options: 'Central server' (selected) and 'Theft Deterrent server'. At the bottom left is a link 'Manage server backup files'.

➤ Manual backup

Step 1: On the **Advanced** page under **Settings**, select the backup location

Step 2: On the popup window, configure the backup settings

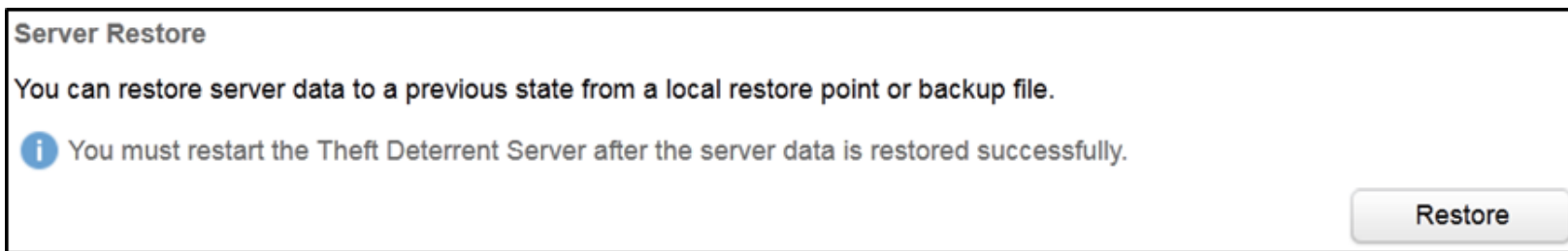
Settings: Advanced settings

➤ Server Restore

Step 1: On the **Advanced** page under **Settings**, click **Restore**

Step 2: Select the restoration source and click **Restore**

Step 3: Input the password and restart the server



Note: 1. Close database connection before restoration
2. After restoration, start the TD service manually.



Settings: Advanced settings

➤ Set up Smart Client Upgrade

Step 1: Turn on the Smart Client Upgrade function on the **Advanced** page under **Settings**

Step 2: Click the **Upload Package** button

Step 3: Select the uploaded package in the table to enable downloading



Note: For the separate download server, the client upgrade packages must be manually copied under download URL, with the same file name as the local download server in the location:

Debian: /opt/TheftDeterrentServer/Site/welcome-content/tdupdate

• **Windows:** C:\Program Files\Intel Education Software\Theft Deterrent server\Site\webapps\tdupdate

Setting: Advanced settings

Turn on/off the function

Smart Client Upgrade

The server can upgrade the Theft Deterrent clients automatically through the network. You can also use a separate download server(s). For more information about Smart Client Upgrade, please refer to the [user manual](#).

Enable	Enable 3G download	Package Name	Version	OS	Total #	Succeeded #	Failed #	Delete
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	client	4.0.20000.9512	Android	261	--	--	Delete
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	guardian	4.0.20000.9512	Android	261	--	--	Delete
<input checked="" type="checkbox"/>	<input type="checkbox"/>	client	4.0.30102.9512	Linux	--	--	--	Delete
<input checked="" type="checkbox"/>	<input type="checkbox"/>	client	4.0.10000.9512	Windows	239	--	--	Delete
<input checked="" type="checkbox"/>	<input type="checkbox"/>	guardian	4.0.10000.9512	Windows	239	--	--	Delete

Configure download server(s)...

Upload Package

Enable the corresponding package

Delete package from local service folder.

Configure 3rd party download server.

Enable 3G download for mandatory upgrade, only work for Android OS

Upload to local service folder.

Total #: The number of controlled devices of this type
Succeeded #: The number of successfully installed devices
Failed #: The number of devices with installation failure (only TDv2 client)

Setting: Advanced settings

➤ Configure download server

Configure Download Server

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

Enable	Server Name	URL	Concurrent Download Limitation	Client Speed Limitation	Delete
<input checked="" type="checkbox"/>	shwde6433	Local Address	100	200 KB/s	
<input checked="" type="checkbox"/>	Download Server 2	http://192.168.1.100/download/	300	200 KB/s	X

Add Server

Save

Cancel

Setting: Advanced settings

➤ Update package file name:

Version	OS	Display Name	File name
4.0.10000.XXXX	Windows	client	Theft_Deterrent_client_v4.0.10000.XXXX.release.zip
4.0.10000.XXXX	Windows	guardian	Theft_Deterrent_guardian_v4.0.10000.XXXX.release.zip
4.0.30X0X.XXXX	Linux	client	Theft_Deterrent_client_v4.0.3010X.XXXX.release.zip
4.0.30X0X.XXXX	Linux	guardian	Theft_Deterrent_guardian_v4.0.3010X.XXXX.release.zip
4.0.20000.XXXX	Android	client	Theft_Deterrent_client_v4.0.20000.XXXX.release.zip

➤ Version Naming Convention:

Version: **<Major Version>.<Minor Version>.<Platform Code>.<Build Number>**

Platform Code (5 digitals): **X(OS Major code) XX(OS Minor code) XX(OS version)**. The rule will be like below :

Platform code	OS Distri.	Platform Code	OS Distri.
10000	Windows Category	30101	Debian 6
10100	Windows 7	30102	Debian 7
10200	Windows 8	30200	Mint
10201	Windows 8 Legacy	40000	TDOS Category
10202	Windows 8 RT	40100	TDOS – Platform 1 (Yukka Beach)
20000	Android	40200	TDOS – Platform 2 (Salipta)
30000	Linux Category	40300	TDOS – Platform 3 (Sunny Hill)
30100	Debian Category		

Not all OS list supported

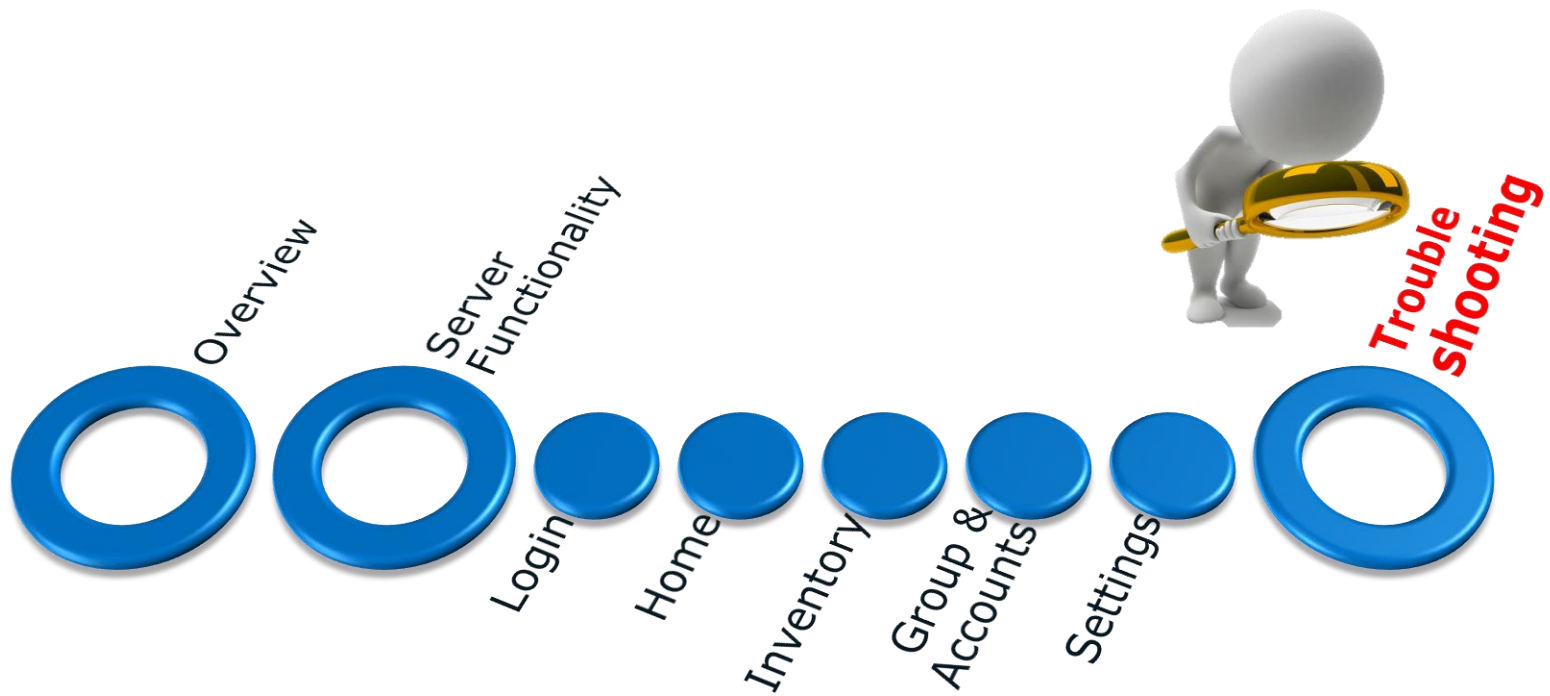
Settings: Account settings

- If you log in with a helpdesk/call center or customer account, edit information on the **Account** page under **Settings**



- If you log in as an admin, edit information on the Account page under **Groups & Accounts**

Agenda



Trouble shooting

Warning and Error Messages

Device Error Codes

Smart Client Upgrade Error Codes

Register/Activate Error Codes

Root Public Key file missing

Server keystore file corrupted

Fail to load configuration files

Fail to connect to the database

Error 404: Page not found

TD server activation problem

Trouble shooting

➤ Warning and Error Messages

Page	Issue	Warning/ Error	Solution
Device Management	Boot Tick inconsistent	Warning	Reset the Boot Tick on the Device Details page.
	Download limit expired	Warning	Reset the download limit on the Device Details page
	Hardware error	Error	Check the error codes.
Transfer-in	Transfer error	Error	Reject the device.
Pending New Devices	Client with an earlier version	Warning	If the client is in Inactive status or pre-activated with a Public Key related to this server, approve it. Else, reject it
	Hardware error	Error	Reject the device.

Trouble shooting

➤ Device Error Codes

Device Error Code	Description
0X02010001	The TPM device cannot be found.
0X02010002	The TPM is disabled.
0x02011006	
0X02010003	The TPM is deactivated.
0x02011007	
0X02010004	Errors occur during TPM initialization in the manufactory line. Possible reasons include: 1. The TPM does not have an Endorsement Key pre-installed. 2. The TPM NV partition or NV index creation failed. 3. The TPM status is incorrect.
0X02010005	
0X0201000A	
0X0201000C	
0X0201000E	
0X0201000F	
0X02011003	
0X0201EEEE	The TPM status error is reported by an old version of TD client (2.x)
0X0201FFFF	Internal error accessing the TPM.

Trouble shooting

➤ Smart Client Upgrade Error Codes

Error Codes	Descriptions
0x02050002	Fail to download the upgrade package. The error might be caused by network problems.
0x02050008	The upload package is corrupt.
0x02050010	Each upgrade package can only contain one file (.exe or .apk).
0x02050040	Fail to run the upgrade package. For example, the .exe file or the .apk file in the package is broken.

Trouble shooting

➤ Register/Activate Error Codes

Error Codes	Descriptions
0x05028001	Central server is under maintenance mode.
0x05068003	The activation code is invalid.
0x05068004	Retry to reactivate with the activation code used to activate in previous.
0x05068005	The central server cannot connect with Root CA server.
0x05068006	Cannot register again for the server already being registered and activated.

Trouble shooting

- Root Public Key file is missing
 - For Central Server supported mode:
Step: Re-install and then reactivate the server
 - For Stand-alone mode with your own Root Public Key:
Step 1: Rename the key to **td-cert-root.pubkey**
Step 2: Copy it to the following directory:

Windows: C:\Program Files\Intel Education Software\Theft
Deterrent server\Site\domain\data\security
Debian: /opt/TheftDeterrentserver/Site/domain/data/security

Trouble shooting

- For Stand-alone mode with the Intel Root Public Key:
 - Step 1: Install the server with the same mode on another machine.
 - Step 2: Copy the **td-cert-root.pubkey** file from the new server in the following directory:

Windows: C:\Program Files\Intel Education Software\Theft
Deterrent server\Site\domain\data\security
Debian: /opt/TheftDeterrentserver/Site/domain/data/security

Trouble shooting

➤ Server keystore file is corrupted

- Re-install and then restore the server with a backup file.
- Without backup files:
 - For **Central Server supported** mode, re-install and reactivate the server
 - For **Stand-alone mode**, re-install the server and import a crash recovery package

➤ Server fails to load configuration files

- Same with the solutions for corrupted server keystore file

Trouble shooting

- Server fails to connect to the database
 - Check the connection between web and database server
 - Restart the server:
 - Windows: **Start** menu -> **All Programs** -> **Intel Education Software** -> **Theft Deterrent server** -> **Start Server.**
 - Debian: Run the command “service theftdeterrentserver restart” with root privilege

Trouble shooting

➤ Error 404: Page not found

- Refresh the webpage or re-log in
- Make sure the URL is correct
- If trouble still exists, restart the server

➤ Theft Deterrent server activation problem

- Guarantee correct input and network connection
- In the registration step, contact the central server admin to make sure the server hasn't been activated
- In the activation step, for Stand-alone mode, make sure correct Root Public Key is imported

Exercise

Please try these tasks

1. Change Server settings for client heart-beat interval, email server setting etc.
2. Manual Approval of a Device
3. Manual lock the remote unlock of a classmate PC device
4. Manual lock then unlock by unlock for classmate PC device
5. Batch Lock and generate unlock code, send by email
6. Create group and account for different role of different schools

FAQ

How to start, stop, and restart the server as well as check its status?

Ans: 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 following commands with root privilege:

```
service theft deterrentserver start  
service theft deterrentserver stop  
service theft deterrentserver restart  
service theft deterrentserver status
```

FAQ

What is the priority of Online Certificate Packet?

Ans: Kill Pill (manual lock) > Global Certificate > other certificates

