



Intel® Education Solutions

Intel® Education Solutions Theft Deterrent Training – Client 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.

Version

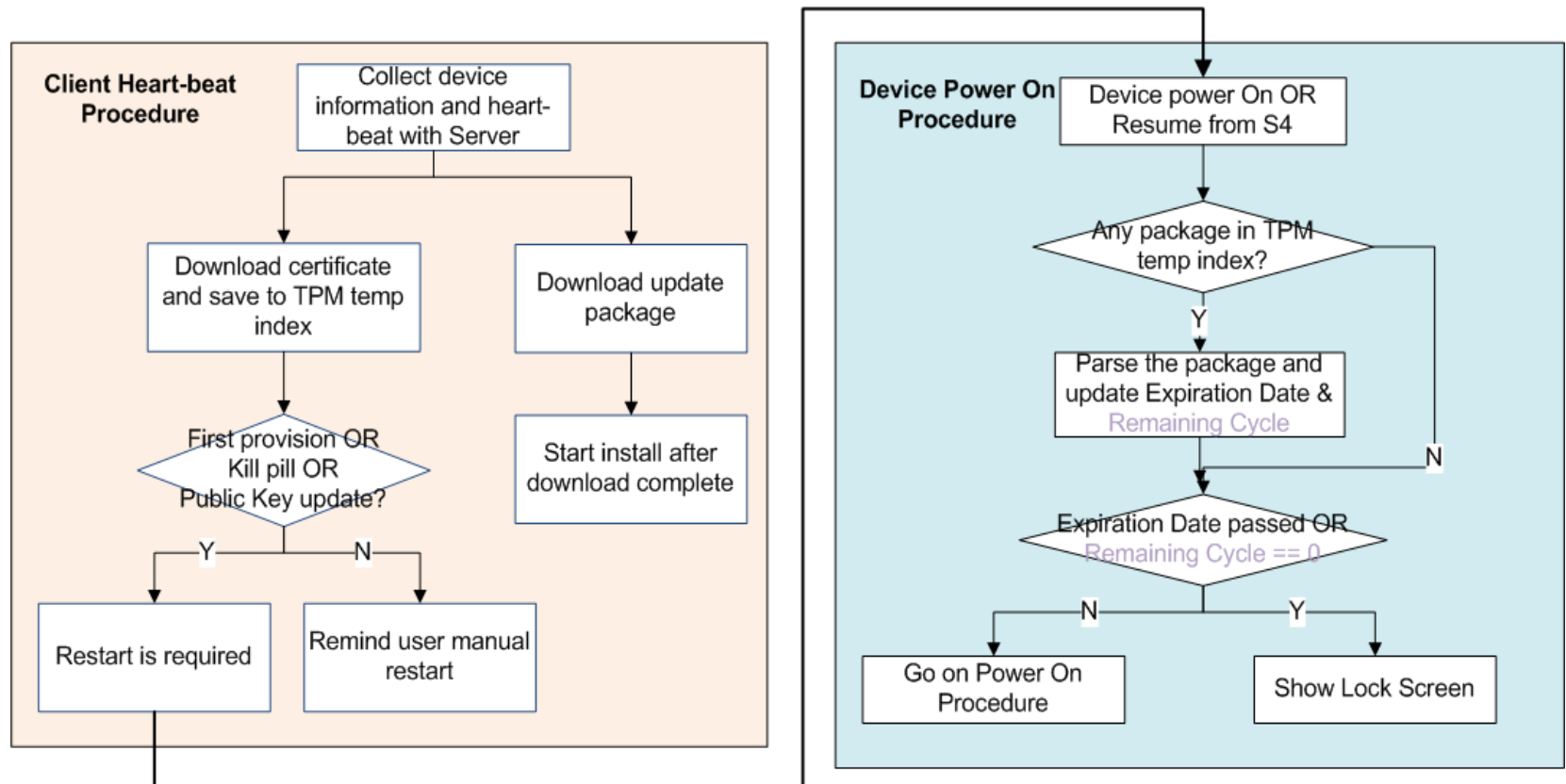
Version	Description
0.60	
0.61	Add quick heart-beat through Test . Add Export Log .

Agenda

- Overview
 - TD working mechanism in client
 - Client components
 - Client UI elements
- Function of Client
 - Dialog Detail
 - Network setting
 - First activation
 - Regular running job
 - Login to server
 - Export log file
- Unlock a device
 - Unlock an Intel® Education Tablet device
 - Unlock an Intel® classmate PC device

Overview

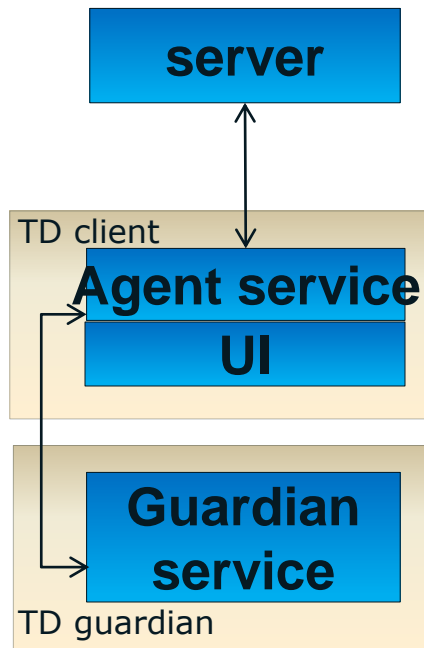
TD Working Mechanism in client



Note: Remaining Cycle is not applicable for Tablet device.

Overview

Client Components



Agent service: communicate with the server during each heart-beat:

- Check whether the server obtains any certificate or upgrade package for the client
- Download the certificate and update package from the server if available





UI: client network setting and TD status display, warning prompt

Guardian service: background service to protect the client

- Start the client service if it is stopped
- Install a built-in client if it is uninstalled
- Call system service to restart the system if required, like received kill pill from server.

Overview

Client UI Elements

Components	Windows	Android
Short-cut	Desktop short-cut  Start menu	Desktop short-cut in widget 
Tray Icon	Icon is different according to Device status 	N/A
Tooltip	Show different tool tip according to Device status.	N/A
Balloon/Notification	Warning + No package downloaded: Popup every heart-beat Package downloading: Pop up when you hover the mouse over the tray icon. Package update failed: Pop up if event happen.	Popup in system tray every heart-beat. 1. Warning + No package downloaded. Click the notification to open client UI. 2. Warning + Certificate downloaded. Click the notification to open restart dialog. Package downloading and Package update failed.
Dialog	2 tabs display: 1. Device Status & System Information 2. Settings	2 tabs and popup menu display 1. Device Status & System Information 2. Settings 3.  icon on the upper-right corner

Agenda

- Overview
 - TD working mechanism in client
 - Client components
 - Client UI elements
- **Function of Client**
 - Dialog Detail
 - Network setting
 - First activation
 - Regular running job
 - Login to server
 - Export log file
- Unlock a device
 - Unlock an Intel® Education Tablet device
 - Unlock an Intel® classmate PC device

Client Functionality

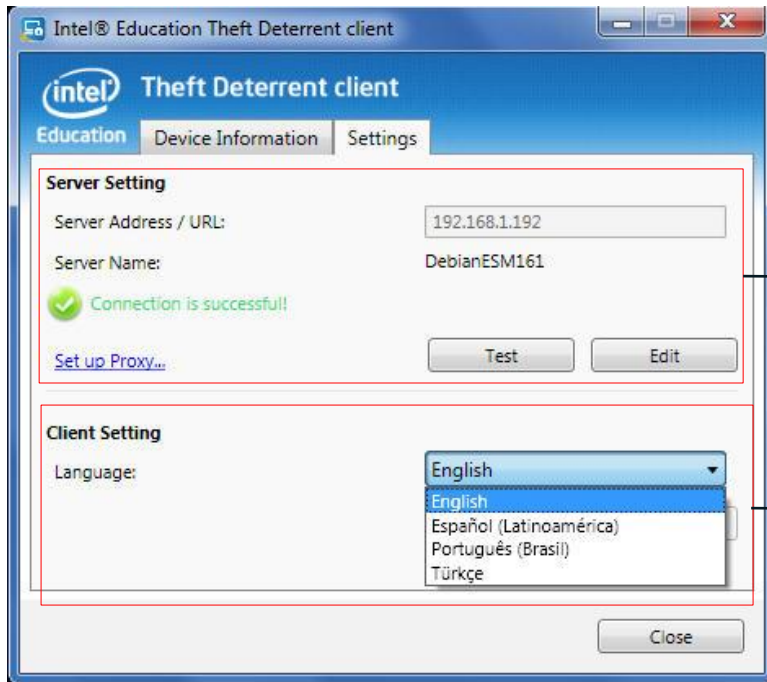
Dialog Detail

The screenshot shows the 'Intel® Education Theft Deterrent client' window. It has three tabs: 'Education', 'Device Information', and 'Settings'. The 'Device Information' tab is active. It contains two main sections: 'Device Status' and 'System Information'. The 'Device Status' section shows 'Device Status: About to expire', 'Boot Tick: 1', 'Expiration Date: 5/5/2013', and 'Remaining Cycles: 299'. To the right of this section is a 'Device status icon' (a laptop with a yellow warning sign). Below the 'Device Status' section is a warning message: 'The Device Status will be updated after you reboot the system.' The 'System Information' section shows 'Hardware ID: 1078D26A4D72', 'Device Name: ESMř-PC', and 'Group Name: ---'. A 'Close' button is at the bottom right. Annotations with arrows point to various parts of the dialog:

- [Detail status message with detail information](#) (points to the 'Device Status' section)
- Remind user to restart the device manually if a certificate has been downloaded (points to the warning message)
- Device information and group in the Server (points to the 'System Information' section)
- [Device status icon](#) (points to the laptop icon)
- [Warning / Error message](#) (points to the warning message)



Client Functionality

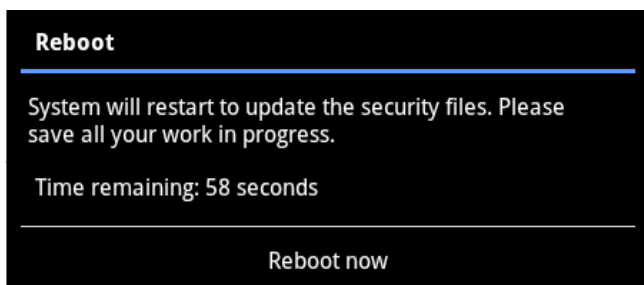
Dialog Detail





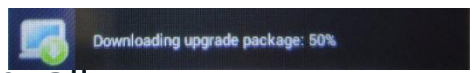
- Server address. Test in advance before you save the setting
- Set up Proxy if need
- Set client display language and Apply
- Not applicable for Android (which use Android language setting)

Client Functionality

- Network setting
 - Input correct Server address and Save
 - Select Proxy setting if needed
- First activation
 - TD can be activated in manufactory line (refer to Device deployment guide)
 - If not activated yet (Device status **Inactive** ). Steps:
 - Network setting
 - Wait for server approval, and a Reboot dialog will pop up
 - Wait for the device to restart and the Device status will be changed to **Normal** 



Client Functionality

- Regular running job
 - Client will work in background automatically. Device status is updated in every heart-beat
 - Maintain the connection between the server and the client, certificate will be downloaded
 - Kill Pill, Public Key and Share Secret update, the machine will be forced to restart
 - Global certificate, temporary certificate downloaded, reminder in UI to let user manual restart
 - Maintain the connection between the server and the client, remote update package will be downloaded
 - Download and upgrade in background, no user interaction.
 - Windows: Tray icon and tooltip will change to  (Downloading) and  (Upgrading).
 - Android: The notification for Downloading  appears and requires user to Accept the upgrading manually

Client Functionality

Heart-beat interval

1. Client will have 3 times of quick heart-beat (per 1 minutes) when it is just started or the server address is modified and saved.
2. After connected with server, client will use the server's heart-beat interval setting under Settings->client

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

Client Functionality

3. If it cannot connect with server, client will use the setting in local configuration file.

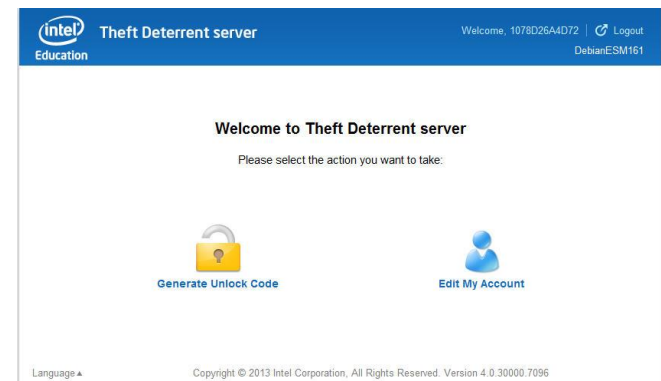
Client will try to connect with server every 10 minutes (4.0.x.10070 or higher) or 30 minutes (under 4.0.x.10070).

4. For version 4.0.x.10070 or higher, you can click **Test** to trigger a fast connection within 2 minutes.

Client Functionality

- Login to server
 - Setup student account
 - Select "Login to server" in popup menu
 - Setup student account with a 6~12 length password
 - Generate Unlock code
 - Select "Login to server" in popup menu
 - Log in with Hardware ID of the machine and the password pre-set
 - Click "Generate Unlock Code"
 - Input the Boot Tick and generate the Unlock Code.

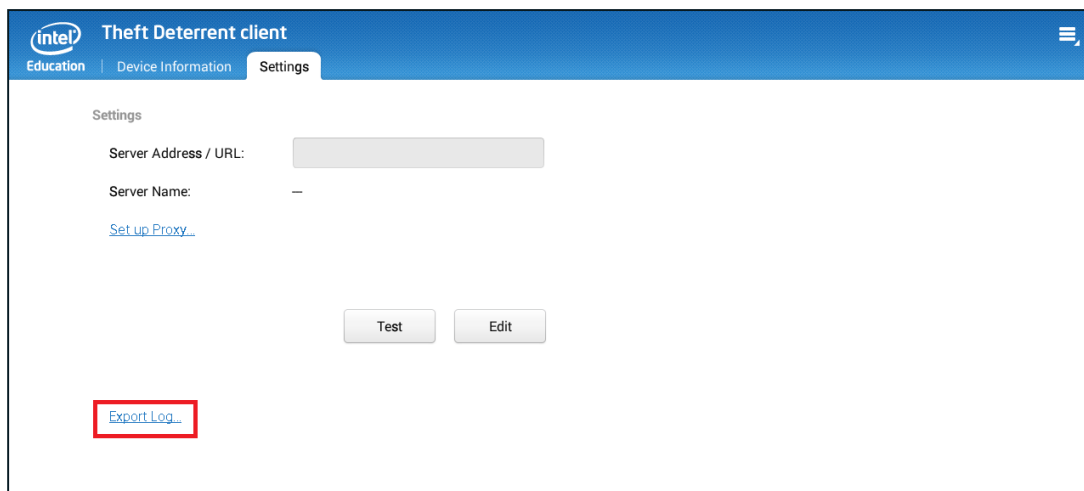
Note: Server can disable the generate unlock code function and set the times limitation under **Settings->Client-> Student Unlock Code** on the server webpage

A screenshot of a web form titled "Complete Account Information". The text below the title says: "Please create a password for login and provide an e-mail address which will be used for password reset." The form contains several input fields: "Hardware ID:" with the value "1078D26A4D72"; "Student name:" with an empty field and "(optional)" text; "New password:" with a red border and a black dot indicating a password character; "Confirm the password:" with an empty field; "E-mail:" with an empty field and "(optional)" text. Below the fields is a warning icon and text: "The password must be 6 to 12 characters in length." At the bottom right is a "Save" button.

Client Functionality

- Export log file

- You can click **Setting**->**Export Log** to export the log file named as "td.log" for trouble shooting.



OS	Export destination	Note
Windows/Linux	Specific destination path	The export folder name cannot contain any special character.
Android	/sdcard/td.log	

Agenda

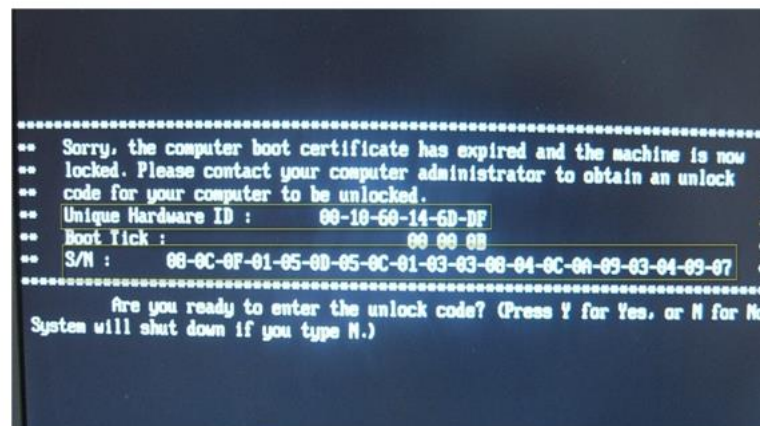
- Overview
 - TD working mechanism in client
 - Client components
 - Client UI elements
- Function of Client
 - Dialog Detail
 - Network setting
 - First activation
 - Regular running job
 - Login to server
 - Export log file
- **Unlock a device**
 - Unlock an Intel® Education Tablet device
 - Unlock an Intel® classmate PC device

Unlock a Device

If the device is locked, a lock screen is displayed as follows:



Tablet Lock Screen



Classmate PC Lock Screen

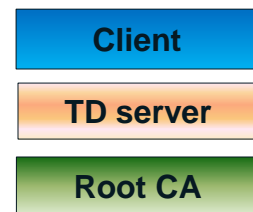
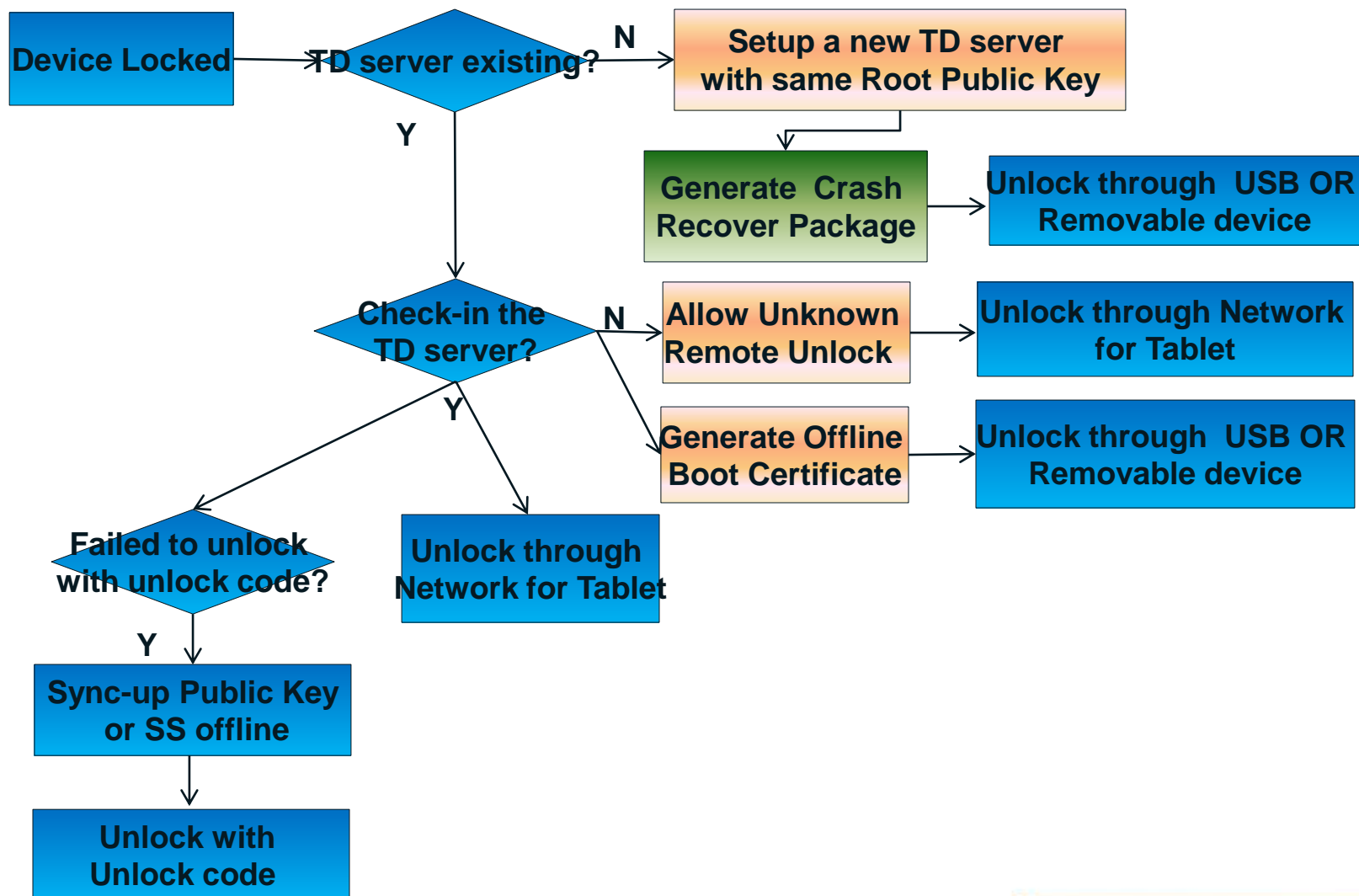
Hardware ID: Device's LAN/WLAN MAC address to identify a device for TD system. It is recorded in TPM during first provision and will not change in future.

Boot Tick: A hexadecimal number that increases by 1 after the client applies a certificate.

Provision Number or **S/N:** A 20-digit hexadecimal number generated from the Public Key of the server. It will be used to identify which TD server the device belongs to.

Unlock method		Classmate PC	Tablet
Unlock code		✓	✓
Removable device	USB	✓ (hot key Ctrl+Insert)	✓
	Mini-SD card		✓
Network			✓

Unlock a Device – Choose unlock method





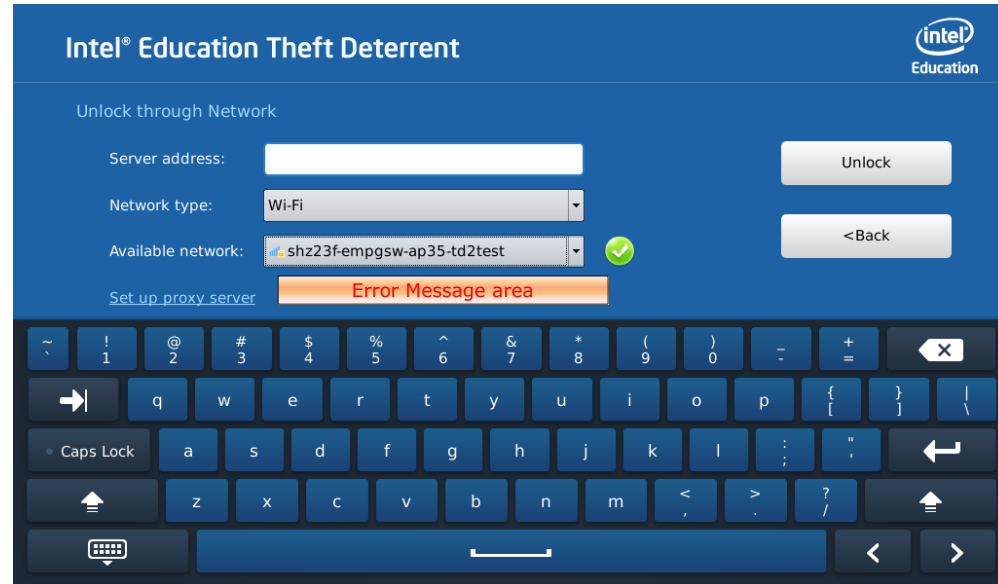
Unlock a Device – Unlock Package

Package	Generator	Input	Comment
Crash Recovery	Root CA	Provision Number Public Key of new TD server	
Advance Crash Recovery	Root CA	Provision Number Hardware ID Boot Tick Public Key of new TD server	Only applies to Beach Point/Pine Trail Peak and Tablet device
Offline Boot Certificate	TD server	Hardware ID Boot Tick	Device pre-provisioned with the TD server's key in manufactory line already
Shared Secret sync-up package	TD server	Export from server under Settings->Security->Sync Package button. Used to sync-up the Shared Secret or Public Key in device with a removable device if the unlock code is not applicable.	
Public Key sync-up package	TD server		
Unlock Code	TD server	Hardware ID Boot Tick Shared Secret	

Unlock a device – through network

Select **Unlock through Network** on the Lock Screen






- Input Server address
- Set up Proxy server if needed
- Select one AP from the drop-down list, then input AP's security key.
- If the network connection is successfully , the **Unlock** button will be enabled. If the network connection failed , the **Unlock** button is disabled.
- Click the **Unlock** button. If successful, the device will restart, otherwise error message will be displayed.



Unlock a device – through network

<i>Message</i>	<i>Error Code</i>	<i>Description</i>
The security key is incorrect. ...		AP's security file is not correct.
The port number of the proxy server is invalid.		Proxy server's port number is not 0-9 digital.
The unlock request is denied.		Device status in server is locked. Need Allow unlocking before remote unlock.
Failed to unlock the device. (Error Code: 0X-----)	0x01040001	Server has error.
	0x01040002	Cannot connect with the server.
	0x01040040	The server address is invalid because it is shorter than 4 characters.
	0x01040080	Cannot connect with the server because the proxy username or password is invalid.
	0x04020003	Server is busy. Please try again later.
	0x04020004	Server is under maintenance. Please try again later.
	0x04070001	Cannot unlock this device because it is not managed by the server yet.
	0x04070002	Cannot unlock this device because it is still waiting for the server's approval.
	0x04070003	Cannot unlock this device because it has been rejected by the server.
	0x04070005	The Root Public Key in the server is not the same as that in the device
	0x04070006	The server Public Key is not the same as that in the device
	0x04070007	Boot Tick in the client is inconsistent with that in the server.
	0x04070008	certificate download limit exceeded the threshold in the server.

Appendix - Device Status

Device Status Message	Device Status Icon	Warning/Error Message	Comment
Inactive		- Waiting for server approval...	
		- Cannot connect with the server - Cannot connected with the server because of invalid proxy - Rejected by the server	
Normal Permanent About to Expire		The warning message maybe display when: - Certificate download limit exceed - Boot Tick inconsistent - The Server is busy, please wait... - The Server is under maintenance - Server error	1. Remaining Cycle is not applicable for Tablet device. 2. Certificate download limit can be set in server Settings->Client->Boot certificate limit 3. In server, the device will display with orange and admin can manual reset the times for the 2 warning.
		- Cannot connect with the server - Cannot connected with the server because of invalid proxy - Connected with the wrong server - Rejected by the server	1. Server address is set correctly 2. Proxy is set correctly if need
Error(Error code)		Device Error	In server, the device will display with red and cannot approval in Pending approval Tab.

Appendix – Device Error Code Table

<i>client Error Code</i>	<i>Unlock Screen Error Code</i>	<i>Description</i>
0X02010001	0X01010001	The TPM device cannot be found.
0X02010002	0X01010002	The TPM is disabled.
0x02011006	/	
0X02010003	0X01010003	
0x02011007	/	The TPM is deactivated.
0X02010004	0X01010004	
0X02010005	0X01010005	
0X0201000A	0X0101000A	<p>Error occurred during TPM initialization in the manufactory line. The possible reasons include the following:</p> <ol style="list-style-type: none"> 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.
0X0201000C	0X0101000C	
0X0201000E	0X0101000E	
0X0201000F	0X0101000F	
0X0201FFFF	0X0101FFFF	Internal error accessing the TPM.

Trouble Shooting - client

1. Can I uninstall TD client?

Answer: For Android, it is pre-installed in image, so you cannot uninstall the client. For Windows, you need to uninstall the Guardian before uninstalling the client. And both the Guardian and the client can be protected by the password set by the server (**Settings->Client-> Password Protection**)

2. Can the useable time be extended by modifying the device's system time/date?

Answer: For Intel® Education Tablet, changing the system time will not affect the useable time of the device. For Intel® classmate PC, changing the system time can extend the usable time of the device. However, this will not impact the **Remaining Cycles** and the device will eventually be locked after the **Remaining Cycles** decreases to 0.

3. Why can't I enter the login page when I open the server webpage for student?

Answer: The login page is displayed only after the device owner completes the student account settings. Therefore, to generate an unlock code with a device borrowed from your classmate, ask your classmate to complete his or her account settings and then you can log in the server with your own **Hardware ID** and password.

Trouble Shooting – Unlock

1. What is the removable device format supported for unlocking?

Answer : The FAT file system. And for classmate PC, need

- FAT16:Support size up to 2GB (Recommend to use Size <2GB)
- FAT32:Support size up to 8GB

2. What is the network protocol supported for device unlocking through network?

Answer: The wireless encryption standards supported includes: WPA/WPA2/WEP (Hex Security Key only) or no encryption

