



# ThinkPad Tablet Deployment Guide





# ThinkPad Tablet Deployment Guide

**Note:** Before using this information and the product it supports, read the general information in Appendix A “Notices” on page 17.

**First Edition (August 2011)**

**© Copyright Lenovo 2011.**

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration “GSA” contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

---

# Contents

<b>Chapter 1. Overview. . . . .</b>	<b>1</b>	<b>Chapter 3. Using Microsoft Exchange</b>	
Lenovo Device Policy Manager Service . . . . .	2	<b>ActiveSync . . . . .</b>	<b>13</b>
<b>Chapter 2. Configuration . . . . .</b>	<b>5</b>	<b>Chapter 4. Lenovo Mobility</b>	
XML configuration files . . . . .	5	<b>Manager. . . . .</b>	<b>15</b>
Active Directory domain server . . . . .	11	<b>Appendix A. Notices. . . . .</b>	<b>17</b>
Configuration Profile Sign and Encrypt Utility. . .	11	Trademarks . . . . .	18
Lenovo Profile Manager . . . . .	11		



---

## Chapter 1. Overview

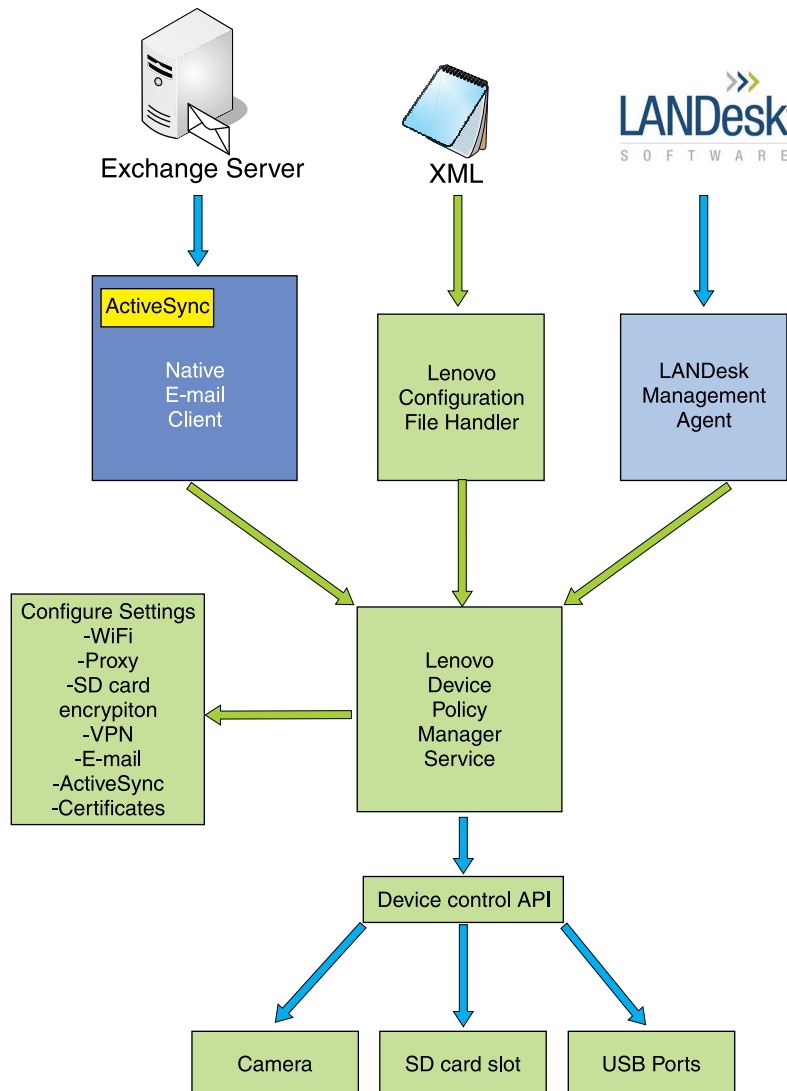
The Lenovo ThinkPad Tablet gives you the ability to configure and manage the tablet using regular tools such as you use within your enterprise. You can control tablet functions, enable corporate security, passwords, encryption and digital signatures.

You can push down configuration or policy settings to the ThinkPad Tablet in these ways:

- Microsoft Exchange ActiveSync
- An XML configuration file
- Lenovo Mobility Manager

Here is the information flow for the ThinkPad Tablet:

Figure 1. ThinkPad Tablet flow



Microsoft Exchange is used as the corporate email communication method.

You can create or modify an XML file using either a text editor or an XML editor to push down to the ThinkPad tablet through the Lenovo Configuration File Handler APK. Or you can use Lenovo Mobility Manager Suite to manage your user's ThinkPad tablets using the supplied Lenovo Mobility Manager APK. These methods then are passed through the Lenovo Device Policy Manager Service. For more information, see "Lenovo Device Policy Manager Service" on page 2.

---

## Lenovo Device Policy Manager Service

The Device Policy Manager Service handles the management of the ThinkPad Tablet. This component provides an interface that allows management tools, such as ActiveSync, an XML file, or Lenovo Mobility Manager to configure device features, such as WiFi profiles and device policies.



This interface allows you to push the following configurations to the ThinkPad Tablet:

- WiFi profiles
- WiFi access point filters
- WiFi radio power settings
- Microsoft Exchange E-mail server configuration
- VPN configuration
- ActiveSync server configuration
- Device feature disable, including:
  - Camera
  - USB port
  - SD card
  - Microphone
  - Pen
  - Bluetooth
  - WiFi
- Client certificates
- Web proxy
- SD card encryption
- Android Password policies



---

## Chapter 2. Configuration

The ThinkPad Tablet allows you to configure the corporate services that users need by specifying configuration settings in XML files. When these XML files are delivered to users and imported by the ThinkPad Tablet, the settings are applied by the ThinkPad Tablet. Configuring the ThinkPad Tablet with XML files helps make it easier for users to connect to their corporate networks and accounts, and quickly be productive.

---

### XML configuration files

The ThinkPad Tablet allows you to configure corporate services for users by specifying configuration settings in the XML file. When these XML files are delivered to users and loaded on the ThinkPad Tablet, the settings are automatically applied by the tablet. Configuring the ThinkPad Tablet with XML files makes it easier for the user to connect to corporate networks and accounts.

Using the XML file, you can configure the following:

- Microsoft Exchange e-mail server
- Virtual Private Network (VPN)
- Wireless Network Settings
- Digital certificates
- Active Directory domain server
- Device Policies

You can create a single, common XML configuration file for multiple users. The XML file may contain, for example, the configuration settings for the secure corporate wireless network, the CA certificate for the wireless network, and the address of the corporate Exchange server. You can make this XML file available to the user by sending it to the user's personal e-mail account, which the user can access using an unsecured visitor network connection, or the user's home internet connection. Or you can also put the XML configuration file on a Web server, making it accessible to any user that already has the proper intranet credentials.

Once the XML configuration file is received by the user, that user simply taps the file and the Lenovo Configuration Profile Handler is launched to import and apply the configuration settings on the device. The user may be prompted to enter personal logon credentials if they were not included in the configuration file, but all of the common server information and settings will be predefined for the user.

You can secure the XML configuration file by digitally signing and/or encrypting it. Encrypting helps ensure that sensitive data included in the configuration file, such as passwords, cannot be read by unauthorized users. Digital signatures helps ensure that the contents of the file are not changed in any way.

The Configuration Profile Sign and Encrypt Utility allows signing of the configuration profile with an embedded private key. The utility also allows the file to be encrypted using an encryption key derived from the password provided to the utility.

The XML configuration file naming convention always has a file extension of .lenovoconfig, so that the ThinkPad Tablet will recognize it as a configuration file. The file consists of three parts:

1. LenovoConfigSettings
2. LenovoPolicySettings
3. AndroidPolicySettings

The `LenovoConfigSettings` section provides control for the security and encryption for the ThinkPad Tablet. It imports configuration settings such as WiFi profiles, corporate domain servers, virtual private networks, and certificates. Once these are applied, they cannot be deleted.

The `LenovoPolicySettings` section allows you to set controls for the various functions of the ThinkPad tablet such as the camera, microphone, SD cards and Bluetooth, and Wifi radios. Any of these functions can be enabled or disabled depending on your corporate policy.

The `AndroidPolicySetting` section is used to set up policy settings supported natively by Android, including storage encryption, password length, number of numbers and letters required.

Note that a UUID is required for each XML file that you create. If you want to overwrite or remove any existing policies, you can send down a new file with the same UUID of the existing applied policy, and it will overwrite the existing file. Since multiple XML files (with different UUIDs) can be resident on the ThinkPad Tablet, the file with the strongest policies will be applied. For example, if you have an XML file that requires only a numeric password and another file with a different UUID that requires a longer, alphanumeric password, the file with the alphanumeric password will be applied.

The following tables provide information on settings for the XML file. The table headers are:

- **Setting** - The setting in the xml file that you can use require a user to log in to a corporate server or to allow or prevent user from using a certain function require of the device.
- **Parameter** - The fields in the setting that you assign a value for the user to fill in
- **Value** - The required value you need to enter for that field such as server address, user id, Yes/No and so on.
- **Notes** - Any special notes that apply to a setting.

Table 1. *LenovoConfigSettings*

Setting	Parameter	Values	Notes
Email Account	<ul style="list-style-type: none"> <li>• Type</li> <li>• SSL</li> <li>• AcceptAllCerts</li> </ul>	<ul style="list-style-type: none"> <li>• Exchange</li> <li>• Yes/No</li> <li>• Yes/No</li> </ul>	Microsoft Exchange is the only supported email type at this time.
Domain Server	<ul style="list-style-type: none"> <li>• ServerAddress</li> <li>• UserID</li> <li>• Password</li> </ul>	<ul style="list-style-type: none"> <li>• Server address</li> <li>• User ID</li> <li>• Password</li> </ul>	<ul style="list-style-type: none"> <li>• Server address is required</li> <li>• Optional</li> <li>• Optional</li> </ul>
Certificate Type	<ul style="list-style-type: none"> <li>• Type</li> <li>• Name</li> <li>• Filename/Encoded</li> </ul>	<ul style="list-style-type: none"> <li>• Root/User</li> <li>• Certificate Name</li> <li>• ?</li> </ul>	Certificates may be included in the XML file in a Base-64 encoded format.
VPN	<ul style="list-style-type: none"> <li>• PPTP <ul style="list-style-type: none"> <li>– Name</li> <li>– Server</li> <li>– OverwriteIfExists</li> <li>– DNSSearchDomain</li> <li>– DNSSearchDomain</li> <li>– Encryption</li> </ul> </li> <li>• L2TP <ul style="list-style-type: none"> <li>– Name</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Point-toPoint Tunneling Protocol <ul style="list-style-type: none"> <li>– Protocol names</li> <li>– Server IP address</li> <li>– Yes/No</li> <li>– Domain IP Address</li> <li>– Domain IP address</li> <li>– Yes/No</li> </ul> </li> <li>• Layer 2 Tunnel Protocol <ul style="list-style-type: none"> <li>– Name of the server</li> </ul> </li> </ul>	

Table 1. *LenovoConfigSettings (continued)*

Setting	Parameter	Values	Notes
	<ul style="list-style-type: none"> <li>– Server</li> <li>– OverwriteIfExists</li> <li>– DNSSearchDomain</li> <li>– Encryption</li> <li>• L2TPIPSecPSK <ul style="list-style-type: none"> <li>– Name</li> <li>– Server</li> <li>– OverwriteIfExists</li> <li>– Secret</li> <li>– IPSecPresharedKey</li> </ul> </li> <li>• L2TPIPSecCrt <ul style="list-style-type: none"> <li>– Name</li> <li>– Server</li> <li>– OverwriteIfExists</li> <li>– DNSSearchDomain</li> <li>– DNSSearchDomain</li> <li>– UserCertificate</li> <li>– CaCertificate</li> </ul> </li> <li>• AnyConnect <ul style="list-style-type: none"> <li>– Name</li> <li>– Host</li> <li>– OverwriteIfExists</li> <li>– UserCert</li> <li>– CertCommonName</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>– Server IP address</li> <li>– Yes/No</li> <li>– IP Address</li> <li>– Yes/No</li> <li>• Android PSK <ul style="list-style-type: none"> <li>– PSK name</li> <li>– Server URL</li> <li>– Yes/No</li> <li>– Password</li> <li>– Preshared Key</li> </ul> </li> <li>• L2TPIPSecCrt <ul style="list-style-type: none"> <li>– CRT Name</li> <li>– URL</li> <li>– Yes/No</li> <li>– Domain IP Address</li> <li>– Domain IP address</li> <li>– Certificate name</li> <li>– Certificate info</li> </ul> </li> <li>• AnyConnect <ul style="list-style-type: none"> <li>– VPN names</li> <li>– Host IP address</li> <li>– Yes/No</li> <li>– Yes/No</li> <li>– Certificate name</li> </ul> </li> </ul>	

Table 2. *LenovoPolicySettings*

Setting	Field	Values	Notes
DeviceControl	<ul style="list-style-type: none"> <li>• Camera</li> <li>• SDCardSlot</li> <li>• Mic</li> <li>• Bluetooth</li> <li>• DataRoaming</li> <li>• USBPort</li> <li>• MicroUSBPort</li> <li>• SDCardSlot</li> <li>• UnknownSources</li> <li>• USBDebugging</li> <li>• Wifi</li> <li>• HDMI</li> <li>• Tethering</li> </ul>	<ul style="list-style-type: none"> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> <li>• Allow/Block</li> </ul>	

Table 2. *LenovoPolicySettings* (continued)

Setting	Field	Values	Notes
	<ul style="list-style-type: none"> <li>Hotspot</li> </ul>	<ul style="list-style-type: none"> <li>Allow/Block</li> </ul>	
SecurityPolicy	<ul style="list-style-type: none"> <li>SDCardEncryption</li> <li>ADScreenLock</li> </ul>	<ul style="list-style-type: none"> <li>Not required/Required</li> <li>Not required/Required</li> </ul>	

Table 3. *AndroidPolicySettings*

Setting	Field	Values	Notes
StorageEncryption		<ul style="list-style-type: none"> <li>Required/Not required</li> </ul>	
Password	<ul style="list-style-type: none"> <li>maxFailuresForWipe</li> <li>maxTimeToLock</li> <li>expirationTimeout</li> <li>historyLength</li> <li>minLength</li> <li>minLetters</li> <li>minLowercase</li> <li>minNonletters</li> <li>minNumeric</li> <li>minSymbols</li> <li>minUppercase</li> <li>Quality</li> </ul>	<ul style="list-style-type: none"> <li>Number of failures before device is wiped</li> <li>Number in milliseconds</li> <li>Number in milliseconds</li> <li>Number of previous passwords</li> <li>Minimum character length</li> <li>Minimum number of letters</li> <li>Minimum number of lowercase letters</li> <li>Minimum number of nonletters</li> <li>Minimum numeric digits</li> <li>Minimum symbols</li> <li>Minimum Uppercase letters</li> <li>Set password restrictions such as numerics and alphanumerics</li> </ul>	

For more information on Android Policy Settings, see  
<http://www.google.com/support/a/bin/answer.py?answer=1056433&topic=14576>

Here is a sample XML file:

```
<?xml version="1.0" encoding="utf-8"?>

<lenovoconfig
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="lenovoconfig.xsd"
  uuid="2237f15e-1ce5-4e55-9fe6-767118c370c8">
  <Header>
    <DisplayName>Sample policy</DisplayName>
    <Author>David Rivera</Author>
    <Source>Manual</Source>
    <AllowUserRemove>yes</AllowUserRemove>
    <RebootOnApply>no</RebootOnApply>
  </Header>

  <LenovoConfigSettings>

    <Email Type="Exchange" SSL="yes" AcceptAllCerts="yes">
      <ServerAddress>gmail.com</ServerAddress>
      <UserID>t.cloud09@gmail.com</UserID>
    </Email>

    <DomainServer>
      <ServerAddress>dc.lenovo.com</ServerAddress>
    </DomainServer>
  </LenovoConfigSettings>
</lenovoconfig>
```

```

    <UserID>drivera</UserID>
  </DomainServer>

  <Certificate type="Root">
    <name>Corporate CA Cert</name>
    <encoded>
MIIDEzCCAnygAwIBAgIBATANBgkqhkiG9w0BAQQFADCBxDELMakGA1UEBhMCWkEx
FTATBgNVBAGTDFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBub3duMR0wGwYD
VQKExRUaGF3dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UECxMfQ2VydGhmaWNhdGlv
biBTZXJ2aWNlcycyBEaXZpc2lvbjEzMBCGA1UEAxMQVGhhZ3RlIFNlcnZlciBDQTE
mMCQGCSqGSIb3DQEJARYXc2VydmdVYlWNLcnRzQHRoYXdoZS5jb20wHhcNOTYwODAx
MDAwMDAwWhcNMjAxMjMxMjM1OTU5WjCBxDELMakGA1UEBhMCWkExFTATBgNVBAGT
DFdlc3Rlcm4gQ2FwZTESMBAGA1UEBxMJQ2FwZSBub3duMR0wGwYDVQKExRUaGF3
dGUgQ29uc3VsdGluZyBjYzEoMCYGA1UECxMfQ2VydGhmaWNhdGlvbiBTZXJ2aWNl
cyBEaXZpc2lvbjEzMBCGA1UEAxMQVGhhZ3RlIFNlcnZlciBDQTE
mMCQGCSqGSIb3DQEJARYXc2VydmdVYlWNLcnRzQHRoYXdoZS5jb20wZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGGAoGBAN0kUG7I/1Zr5s9dtuoMaHVHoqrC2oQL/Kj0R1HahbUgdJSGHg91
yekIYfUGbTBuFRKc6VLAYttNmZ7iagxEOM3+vuNkCXDF/rFrKbYvScg71CcEJRCX
L+eQbcAoQpnXTEPew/UhbVSfXcNY4cDk2VuwuNy0e9820sK1ZiIS1ocNAgMBAAGj
EzARMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAB/pMaVz7lcxG
7oWDTSEwjsrZgQ9JGubaUeNgcGyEYRGhGshIPLdFU+VPaGLtwtimHp1it2ITk6e
QNuoZDJ0uW8NxuQZRAvZim+aKZuZ6Cg70eNAKJpaPNW15yAbi8qkq43pUdniTCxZ
qdq5snUb9kLy78fyGPmJvKP/iiMucEc=
    </encoded>
  </Certificate>

  <VPN>
    <PPTP>
      <Name>MyPPTPVPN</Name>
      <Server>pptp.server.com</Server>
      <OverwriteIfExists>yes</OverwriteIfExists>
      <DNSSearchDomain>10.10.10.10</DNSSearchDomain>
      <DNSSearchDomain>11.11.11.11</DNSSearchDomain>
      <Encryption>no</Encryption>
    </PPTP>
    <L2TP>
      <Name>MyL2TPVPN</Name>
      <Server>l2tp.server.com</Server>
      <OverwriteIfExists>no</OverwriteIfExists>
      <DNSSearchDomain>12.12.12.12</DNSSearchDomain>
      <Secret>123456789A</Secret>
    </L2TP>
    <L2TPIPsecPSK>
      <Name>MyL2TPIPsecPSKVPN</Name>
      <Server>ipsecpk.server.com</Server>
      <Secret>FEDCBA987654</Secret>
      <IPSecPresharedKey>MyPreshardKey</IPSecPresharedKey>
    </L2TPIPsecPSK>
    <L2TPIPsecCRT>
      <Name>MyL2TPIPsecCRTVPN</Name>
      <Server>ipseccrt.server.com</Server>
      <DNSSearchDomain>13.13.13.13</DNSSearchDomain>
      <DNSSearchDomain>14.14.14.14</DNSSearchDomain>
      <UserCertificate>David Rivera Cert</UserCertificate>
      <CaCertificate>Corporate CA Cert</CaCertificate>
    </L2TPIPsecCRT>
    <AnyConnect>
      <Name>MyCiscoVPN</Name>
      <Host>20.20.20.20</Host>
      <UseCert>yes</UseCert>
      <CertCommonName>David Rivera Cert</CertCommonName>
    </AnyConnect>
  </VPN>

```

```

    </AnyConnect>
</VPN>

<WirelessProfile version="0.01" type="WLAN">
  <name>MyHomeNetwork</name>
  <SSID type="Normal">MyHome</SSID>
  <networktype>Infrastructure</networktype>
  <AuthenticationAlgorithm>Shared</AuthenticationAlgorithm>
  <keymgmt>None</keymgmt>
  <WEPKeys>
    <DefaultKeyIndex>1</DefaultKeyIndex>
    <key1>MyWEPKey</key1>
  </WEPKeys>
</WirelessProfile>

<WirelessProfile version="0.01" type="WLAN">
  <name>MyOfficeNetwork</name>
  <SSID type="Normal">MyOffice</SSID>
  <networktype>Infrastructure</networktype>
  <AuthenticationAlgorithm>Open</AuthenticationAlgorithm>
  <keymgmt>WPA_PSK</keymgmt>
  <presharedkey>somepresharedsecret</presharedkey>
  <protocol>RSN</protocol>
  <proxy type="HTTP" requiresauth="no">
    <address>10.10.10.34</address>
    <port>8080</port>
  </proxy>
</WirelessProfile>

<AccessPointFilter>
  <allow>
    <SSID>MyOffice</SSID>
  </allow>
  <allow>
    <SSID>MyHome</SSID>
    <Security>WEP</Security>
  </allow>
  <deny>
    <SSID>CoffeeShop</SSID>
  </deny>
</AccessPointFilter>
</LenovoConfigSettings>

<LenovoPolicySettings>
  <DeviceControl>
    <Camera>Allow</Camera>
    <SDCardSlot>Allow</SDCardSlot>
    <Mic>Allow</Mic>
    <Bluetooth>Allow</Bluetooth>
    <DataRoaming>Block</DataRoaming>
    <USBPort>Allow</USBPort>
    <MicroUSBPort>Allow</MicroUSBPort>
    <SDCardSlot>Allow</SDCardSlot>
    <UnknownSources>Block</UnknownSources>
    <USBDebugging>Allow</USBDebugging>
    <Wifi>Allow</Wifi>
    <HDMI>Allow</HDMI>
    <Tethering>Block</Tethering>
    <Hotspot>Block</Hotspot>
  </DeviceControl>

```



```

<SecurityPolicy>
  <!-- <SDCardEncryption>Required</SDCardEncryption> -->
  <SDCardEncryption>Not required</SDCardEncryption>
  <ADScreenLock>Not required</ADScreenLock>
</SecurityPolicy>
</LenovoPolicySettings>

<AndroidPolicySettings>
  <storageEncryption>Not required</storageEncryption>
  <Password>
    <maxFailuresForWipe>10</maxFailuresForWipe>
    <maxTimeToLock>5000</maxTimeToLock>
    <expirationTimeout>7776000000</expirationTimeout>
    <historyLength>5</historyLength>
    <minLength>8</minLength>
    <minLetters>2</minLetters>
    <minLowercase>1</minLowercase>
    <minNonLetters>1</minNonLetters>
    <minNumeric>3</minNumeric>
    <minSymbols>1</minSymbols>
    <minUppercase>1</minUppercase>
    <quality>393216</quality>
  </Password>
</AndroidPolicySettings>

</lenovoconfig>

```

The ThinkPad Tablet XML schema can be found on the Lenovo Website at [www.lenovo.com/support](http://www.lenovo.com/support).

---

## Active Directory domain server

An exclusive feature of the Lenovo ThinkPad tablet is that you can use Microsoft Active Directory to allow the user to unlock the ThinkPad Tablet using corporate credentials. You set the XML file to require an Active directory logon, and the user touches **Settings->Location & Security->Configure lock screen->Corporate logon**. The user enters the domain name or IP address, user name, and password. After this, the user can only use the Active Directory domain credentials to unlock the machine.

---

## Configuration Profile Sign and Encrypt Utility

IT administrators can secure the XML configuration file by digitally signing and/or encrypting it. Encrypting helps ensure that sensitive data included in the configuration file, such as passwords, cannot be read by unauthorized parties. Digital signatures help ensure that the contents of the file are not tampered with.

The Configuration Profile Sign and Encrypt Utility allows signing of the configuration profile with an embedded private key. The utility will also allow the file to be encrypted using an encryption key derived from the password provided to the utility.

This component is intended only for the preparation of the XML configuration file for deployment to devices. It is available at [www.lenovo.com/support](http://www.lenovo.com/support) and click Download Drivers & Software

---

## Lenovo Profile Manager

The Lenovo Profile Manager is an Android application (APK) that is preloaded on the ThinkPad Tablet. This APK takes XML configuration files and has the configuration and policy settings applied, and displays information about new and installed configuration profiles.

A configuration file received by the ThinkPad Tablet must have a specific file extension (.lenovoconfig). The Lenovo Profile Manager is registered as the handler for files with this extension. When a file with this extension is received on the device and tapped by the user, the XML Configuration Profile Handler will run.

The Lenovo Profile Manager calls into the Lenovo Device Policy Manager Service to perform an initial parse of the contents of the file. The initial parse:

- Verifies that the XML file contents are valid against the schema
- Determines what settings are included in the file

The Lenovo Profile Manager is registered as an Android Device Administration Receiver using the native Android capabilities.

The Lenovo Profile Manager also displays information about the installed profiles to the user. When the user touches **Settings->Location & security->Configuration profiles**, a list of installed profiles will be displayed using the “DisplayName” property of the configuration file. If no profiles are installed, the application will display the message “No configuration profiles have been applied.” If multiple profiles are installed, the user will see a list of them. The device will show which policy is the applied policy at the bottom of the page.

If the user selects an installed profile from the list, the details of the configuration settings in that list will be displayed. All installed profiles are displayed by the Configuration Profile Handler. This allows the user to view all configuration settings that have been applied.

The profile display also allows the user to remove selected profiles. Only configuration profiles that were installed by the Lenovo Profile Manager can be removed by the user, as long as you did not set the property indicating that the policy cannot be removed. Configuration settings that were not set by the Lenovo Profile Manager will be displayed, but cannot be removed by the user.

The Lenovo Profile Manager also calls into the Lenovo Device Policy Manager Service to receive a list of installed profiles, and receives the list of installed profiles, their source, and whether the profile is allowed to be installed from the Lenovo Device Policy Manager Service.

---

## Chapter 3. Using Microsoft Exchange ActiveSync

The ThinkPad Tablet includes support for Microsoft Exchange ActiveSync. The ThinkPad Tablets can be managed with Microsoft Exchange ActiveSync in the same way as other mobile devices.

Microsoft Exchange ActiveSync offers pushmail capability for mobile devices. In addition to pushing e-mail and calendar entries, ActiveSync allows the you to push device policies.

The ThinkPad Tablet supports the following Exchange ActiveSync controls:

- Remote wipe
- Password policies
- Device encryption
- Camera
- Wi-Fi
- Bluetooth
- Sync from PC
- Removable storage
- SD card encryption

Once a ThinkPad Tablet is configured to connect to the Exchange server, policy settings pushed to the device from the Exchange server are automatically applied, ensuring that the device maintains the security settings that your IT department requires.

The ThinkPad tablet e-mail client includes support for Exchange ActiveSync policies. These policies are for password enforcement and for device encryption. Those settings natively supported by Android, including password and device encryption, are supported without change by Lenovo.

This component extends the native ActiveSync capability built into the e-mail client to support additional device policies not natively supported by Android. The additional ActiveSync policies supported on the ThinkPad Tablet include:

- Removable storage (USB port and SD card enable/disable)
- Camera
- WiFi
- Desktop synchronization (micro USB enable/disable)
- Bluetooth (only Bluetooth enable/disable is supported. If the you set Bluetooth to “Handsfree only” in the ActiveSync console, it disables the Bluetooth radio).



---

## Chapter 4. Lenovo Mobility Manager

Lenovo has a mobility management plug-in that enables you to:

- Discover devices, without an agent at the point of data access, through Microsoft Exchange ActiveSync systems
- Know which users are consuming corporate data and what devices they are using
- Push down corporate management and security settings to out-of-policy devices
- Wipe data using a single user-based policy from devices that are lost or stolen or when someone leaves your organization
- Improve business processes for reclaiming corporate IT assets and proprietary information as in the case of employee termination

The Lenovo Mobility Manager requires the user to log in to the configuration server using a PIN, which the user retrieves by logging in to a PIN server from a PC. The user authenticates to the PIN server using corporate credentials, and supplies that PIN when logging on to the Lenovo Mobility Manager configuration server from his ThinkPad Tablet. After connecting to the configuration server, the IT-provided configuration information is pushed to the device and the device is automatically configured.

To use the Mobility management tools, the following prerequisites are required:

- Lenovo ThinkManagement Console Version 9.0 with SP2 or later.
- For Exchange-enabled devices, you must have installed the Exchange Management Tools, available as an option from within the Microsoft Exchange installation.
- Windows Communication Foundation (WCF) and Internet Information Services (IIS) must be installed and registered.

When a mobile device logs in to synchronize e-mail, contact, and calendar information, it does so using an existing Outlook mailbox account. Once the device has logged in, the Exchange server stores identifying information in its database, including the Device ID, owner, the date/time it logged in, and so on. That information can then be retrieved from the Exchange server and displayed in the Mobility management tool.



---

## Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

*Lenovo (United States), Inc.  
1009 Think Place - Building One  
Morrisville, NC 27560  
U.S.A.  
Attention: Lenovo Director of Licensing*

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

---

## Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

- Lenovo
- The Lenovo logo
- ThinkPad
- ThinkVantage

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft, Active Directory, ActiveSync, and Windows are trademarks of the Microsoft group of companies.

Other company, product, or service names may be trademarks or service marks of others.





Part Number:

Printed in USA

(1P) P/N:

