APPENDIX A

Central Configuration Using File Server

This appendix contains information about configuring thin clients using a central file server as an alternative to Cisco VXC Manager.

Cisco VXC Manager is the standard tool for central management. As an alternative method for thin client management, you can configure a local file server from which the thin clients can obtain INI files for their configuration.

Caution Central configuration using a file server provides fewer capabilities for hands-on client management, and is therefore recommended only in test environments or for troubleshooting. Cisco VXC Manager is the standard tool for thin client management.

For information about configuring thin clients using Cisco VXC Manager, see Central Configuration Using Cisco VXC Manager, page 1-1 and the *Administration Guide for Cisco Virtualization Experience Client Manager*.

This appendix includes:

For detailed information on constructing and using INI files, see the *Cisco Virtualization Experience Client 6215 INI Files Reference Guide*.

How INI Files Are Employed

INI files (created and maintained by the network administrator) determine how the thin client is configured and updated. The thin client accesses INI files from the server during the initialization process. Typically, INI files are accessed through FTP, HTTP, or HTTPS; if no protocol is specified, the default is anonymous FTP.

INI files are employed as follows:

- wlx.ini—This is the global INI file. One wlx.ini file is available to all users. It contains global parameters for all thin clients accessing the server.
- $MAC.ini—This file can be used for device-specific configuration. If the thin client locates this INI file (it is stored in the same directory as wlx.ini), wlx.ini is not accessed, unless you use the include=wlx.ini parameter.

When a thin client is initialized, it accesses the global wlx.ini file.

How to Set Up Central Configuration Using a File Server

For the thin client to successfully access INI files and update itself from a server, you must set up the server with the correct folder structure (where the INI files and other update files are located), direct the thin client to the server, and then reboot or start the thin client.

After DHCP and servers are configured and available, the thin client checks (at each bootup) to see whether or not any updates are available on a predefined server (DCHP Option 161 specifies the server URL; DCHP Option 162 specifies the root path to the server). If updates are available, the updates are automatically installed.

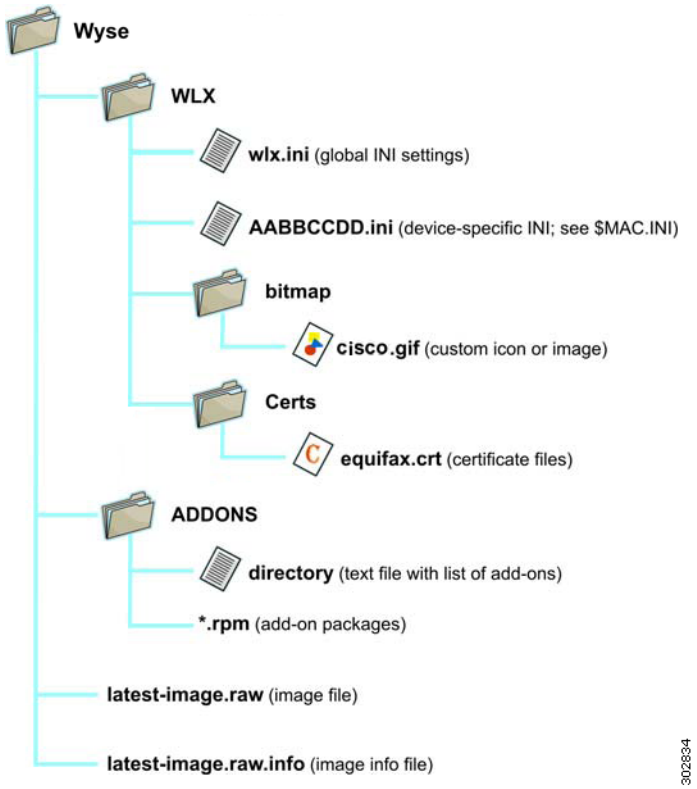
Step 1: Prepare the Root Directory and Folder Structure on the File Server

Set up the following folder structure on your server under the C:/inetpub/ftproot folder (for FTP) or C:/inetpub/wwwroot folder (for HTTP or HTTPS) and place your INI files and other necessary files inside the structure as noted (this list describes the folder structure, starting with the root directory).

/wyse/	The root directory. It stores the wlx folder and the add-ons folder. It also stores the following files, which are used for imaging and updating devices: • Latest-image.raw • Latest-image.raw.info
/wyse/wlx	The main INI configuration folder. It stores the following: • wlx.ini file or $MAC.ini file • bitmap folder • certs folder
/wyse/wlx/bitmap	The folder where you can place custom images you plan to use.
/wyse/wlx/certs	The folder where you can place the CA certificates that can be imported to a thin client. **Note** Use the Certs and ImportCerts INI parameters in the wlx.ini file to import the certificates to thin clients.
/wyse/addons	The folder where you can place the add-ons you want to use. It also stores the directory file and the *.rpm packages available to be installed on the thin client. The directory file should list all available add-ons. The directory file is required in the add-ons folder to guarantee that add-ons are properly located.

The following figure shows how to set up the folder structure on your file server and where to place INI files and other necessary files inside the structure.

Figure A-1 Folder Structure



Be sure to create/activate the required MIME Types (.ini, .raw, .info, .rpm, and .) under IIS (on a per site basis) to enable downloading. Also be sure your web server can identify the file types used by Cisco thin clients.

To create/activate a MIME Type:

Step 1 On your IIS server, use the File Types menu to add a New Type.

Step 2 In the File Type dialog box, enter the Associated extension: (.ini, .raw. .info, .rpm, or .). and Content type.

Step 3 Click **OK** to apply the settings.

Repeat the steps above for each required MIME type, specifying the appropriate extension and content type.

Step 2: Direct the Thin Client to the Server

After you set up the folder structure and populate it with the correct files, you must then direct the thin client to the location of the server using DHCP.

Using DHCP

With the DHCP method of configuring the file server location (recommended), the thin clients obtain information about the server and root directory using the following DHCP options:

- 161—Specifies the server
- 162—Specifies the root path to the server (ftp/http/https)
  - If no root path is defined, /wyse is assumed.
  - If a root path is defined, the additional path is appended to the URL supplied by Option 161.
- 184—(Optional) Specifies the server username (for the server specified in Option 161)
- 185—(Optional) Specifies the server password (for the server specified in Option 161.

Tip The thin clients perform the check-in for firmware updates early in the boot process. For that reason, a unit may not receive changes in DHCP information until it completes a full boot. However, you can avoid this scenario by forcing a renewing of the DHCP lease, which ensures that the unit has the latest file-server location before the next firmware check.

Use the guidelines shown in Table A-1 when you create and add the DHCP options you need.

Table A-1 DHCP Option Tags

Option	Description	Notes
001	Client identifier	Always sent
002	Time Offset	Optional
003	Router	Optional but recommended. It is not required unless the appliance must interact with servers on a different subnet.
006	Domain Name Server (DNS)	Optional but recommended
012	Host Name/Terminal Name	Optional string. The hostname or terminal name to be set.
015	Domain Name	Optional but recommended. See Option 6.
028	Broadcast Address	Optional
044	WINS servers IP Address	Optional
051	Lease Time	Optional but recommended
052	Option Overload	Optional
053	DHCP Message Type	Recommended
054	DHCP Server IP Address	Recommended
055	Parameter Request List	Sent by appliance
057	Maximum DHCP Message Size	Optional (always sent by appliance)
058	T1 (renew) Time	Optional but recommended
059	T2 (rebind) Time	Optional but recommended
061	Client identifier	Always sent

Table A-1 DHCP Option Tags

Option	Description	Notes
161	Server (ftp/http/https)	Optional string. If this is an IP address or resolvable hostname, the protocol is assumed to be FTP; however, it may be the leading portion of a URL that specifies another protocol. If the URL form is used, it should not include a trailing slash (for example, http://server.example.com or ftp://192.168.0.1).
162	Root path to the server (ftp/http/https)	Optional string. The relative directory starting from the root directory must be given. For example, on an FTP server, the full directory may be C:/Inetpub/ftproot/wyse, where wyse is the directory that contains the firmware. In this example, the correct string value for this DHCP option is /wyse. On a Linux server, an FTP user-based directory might be /home/test/wyse. In this example, if the FTP user is test, then the FTP root path is /wyse and not the full path (/home/test/wyse). This value should use URL path notation (start with a forward slash, /, and use a forward slash as folder separators).
181	PN Server	Optional string. IP address or FQDN of the PNLite server.
182	Admin List	Optional string. DHCP equivalent of the DomainList INI file parameter.
184	Server Username	Optional string. Username to use when authenticating to the server specified in Option 161.
185	Server Password	Optional string. Password to use when authenticating to the server specified in Option 161.
186	Cisco VXC Manager	Optional binary IP address of the Cisco VXC Manager server. This option can specify up to one Cisco VXC Manager server.
191	XenDesktop DDC URL	Optional string. You can connect to your XenDesktop URL by using DCP Option tag 191 to specify the XenDesktop DDC URL.
194	Cisco VXC Manager FQDN	Optional FQDN of the Cisco VXC Manager server. This option can specify up to one Cisco VXC Manager server.

Step 3: Rebooting

To reboot your thin client, click **Computer > Shutdown** and choose **Restart**.

Note To reboot the client, use the Restart option to ensure the client performs a full boot sequence. This step is especially important when you are upgrading client firmware or configurations; otherwise, the upgrades may not take effect.

After you reboot (or start the thin client), the thin client searches in the defined root path for the latest available image and updates if necessary. Additionally, it checks the directory file in the add-ons folder to determine whether any updates for installed add-ons are defined. Add-ons that exist in the add-ons folder but are not listed in the directory file are ignored during update check-in.