CHAPTER 4

Cisco VXC Firmware and Configuration Upgrade Procedures

This chapter provides information on the procedures required to upgrade firmware images and configurations on Cisco VXC 6215 clients (running SUSE Linux firmware), Cisco VXC 2211/2211 PCoIP clients (running ThreadX firmware), and Cisco VXC 2112/2212 ICA clients (running WTOS firmware) using Package Manager.

It contains the following information:

Cisco VXC 6215 Upgrade Procedures

You can use Cisco VXC Manager to manage Cisco VXC 6215 clients using similar procedures as those required for the management of the Cisco VXC 2112/2212 ICA-protocol clients.

Management Architecture

The following sections provide a brief overview of the features of the Cisco VXC 6215 that are relevant for its management. For more information on the Cisco VXC 6215, see *Cisco Virtualization Experience Client 6215 Administration Guide*.

Operating System: Cisco-Enhanced SUSE Linux

Cisco VXC 6215 clients run a Cisco-enhanced version of SUSE Linux that is optimized to run Internet browsers, virtualization clients, remote desktop protocols, and other productivity software like unified communications.

Cisco VXC Manager Agent: HAgent for SUSE Linux

The Cisco VXC Manager Agent, also referred to as the HAgent, is installed on the Cisco VXC 6215 for communicating management messages with the Cisco VXC Manager.

INI files for Client Configuration

Cisco VXC 6215 uses INI files for configuration of the device. See *Cisco Virtualization Experience Client 6215 INI Files Reference Guide* for details.The INI settings are applied at boot time or when a user logs out of a device.The INI files can be automatically deployed to Cisco VXC 6215 using an FTP server (see "Appendix A: Central Configuration: Automating Updates and Configurations" of the *Cisco Virtualization Experience Client 6215 Administration Guide*) or using the Default Device Configuration (DDC) mechanism of Cisco VXC Manager (see Updating the Cisco VXC 6215 Operating System Image, page 4-2).

Device Discovery

Upon boot up, the Cisco VXC 6215 clients follow the automated discovery process described in Adding and Automatically Discovering Devices, page 2-13. Administrators can also run the manual discovery process described in Adding Devices Manually, page 2-15. After a client has checked in (or registered) with Cisco VXC Manager, it appears in the Cisco VXC Manager interface and can then be managed. During the first check-in, the Cisco VXC Manager Agent for the client also provides a complete hardware and software inventory. To refresh this information, right-click a device in the details pane of the Device Manager and choose **Refresh Device Information**.

Heartbeats and Health Status

Cisco VXC Manager Agents on the Cisco VXC 6215 send heartbeat check-ins according to the interval specified in the Configuration Manager preferences. The default check-in time is one hour.

Updating the Cisco VXC 6215 Operating System Image

To update the firmware image on the Cisco VXC 6215, perform the following procedure.

Note If the Cisco VXC 6215 is running the Voice and Video Firmware Add-on, after you upgrade the Base VDI firmware, you must install the compatible release of the Voice and Video Firmware Add-on. See Register a Package to Enable a Cisco Add-On, page 4-6.

Procedure

Step 1 Download or copy the OS image from the Cisco Software Download page at the following URL: http://www.cisco.com/cisco/software/navigator.html

Choose **Products > Voice and Unified Communications > IP Telephony > Virtualized Endpoints > Cisco Virtualization Experience Client 6000 Series > Cisco Virtualization Experience Client 6215**.

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped OS image files to a local folder.

Step 3 In the extracted wlx.ini file, do not modify the existing parameters, but add any additional INI configurations you require.

Note If you have existing INI configurations on your clients, you must copy and paste these parameters into the wlx.ini that you push with the update; otherwise, the clients will lose the pre-existing configurations.

Step 4 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Step 5 To upgrade the Cisco VXC 6215, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35)

Note If you downgrade a Cisco VXC 6215 thin client from a newer Image DDC (for example, DDC_10) to any older Image DDC (for example, DDC_09), and then try to re-apply the newer image DDC to the client, the operation fails. To successfully re-apply the newer image DDC (DDC_10) to the thin client after a downgrade, you must first rename the newer image DDC using Cisco VXC Manager (for example, to DDC_10a).

Packaging and Deploying Cisco VXC 6215 Add-On Packages

This section describes how to perform additional Cisco VXC Manager package management tasks for the Cisco VXC 6215 add-on packages.

Note This section contains additional Package Manager procedures that are applicable only to the Cisco VXC 6215 add-ons.

Cisco VXC 6215 Default Add-Ons

The Cisco VXC 6215 firmware includes default add-ons that provide increased security for the thin client and minimize the exposure of the SUSE Linux base operating system to users, while still providing users with useful functionality.

Add-ons are feature-specific software components that provide additional customized functionality on the Cisco VXC 6215 thin clients without affecting the underlying operating system files.

The Cisco add-on applications bundled by default on the Cisco VXC 6215 include the following:

Autologin

The Autologin (autologin-1.0-2.sletc11sp1.rpm) add-on allows the Cisco VXC 6215 to boot using the thin user credentials without requiring the user to provide the credentials.

After the thin client boots up, the login screen initially appears, and after approximately 10 to 15 seconds, the thin client automatically logs the user into the thin client using thinuser/thinuser as the default username and password.

Caution For proper operation of the Cisco VXC 6215, the Autologin add-on must always be enabled and running on the thin client (the default configuration). Do not remove or disable the Autologin add-on as this is an unsupported configuration. Operation with the Autologin add-on enabled is the only supported mode of operation. If you do remove the Autologin add-on, you must reinstall it by reinstalling the latest Base VDI Firmware Release available on cisco.com.

CiscoConfig

The CiscoConfig add-on (ciscoconfig-1.0-2.sletc11sp1.rpm) provides additional functionality to the user beyond that provided by the Autologin add-on. With the CiscoConfig add-on, the Cisco VXC 6215 provides access to additional applications including system information, display settings, Cisco VXC Manager settings, and the Firefox Browser though the Application Browser (**Computer > More Applications**).

Caution As the CiscoConfig add-on is required for proper functioning of the Autologin add-on, the CiscoConfig add-on must always be enabled and running on the thin client (the default configuration). If you do remove the CiscoConfig add-on, you must reinstall it by reinstalling the latest Base VDI Firmware Release available on cisco.com.

Ssh_opt

The Cisco VXC 6215 can support remote connections to the thin client using SSH. To provide increased security, the ssh_opt add-on (ssh_opt-1.0-1.0.sletc11sp1.rpm) disables SSH functionality by default. To allow remote SSH access to the client, the administrator can disable this add-on.

Note To enable the SSH functionality on the Cisco VXC 6215 devices using Cisco VXC Manager, in the Device Manager, right-click the device and choose **Execute Command**. In the Execute Command dialog box, type **/etc/init.d/sshd start** to enable the SSH functionality. If the Ssh_opt add-on is installed on the Cisco VXC device, then the Ssh_opt add-on sets the OpenSSH idle timeout to 30 mins and the maximum timeout to 60 mins. (These default SSH idle timeout values cannot be modified.)

Optional Voice and Video Firmware Add-On

To support Unified Communications on the Cisco VXC 6215, you must purchase and install the Voice and Video Firmware add-on. The optional Voice and Video Firmware add-on provides Unified Communications functionality for Cisco UC Integration for Microsoft Lync and Cisco Unified Personal Communicator.

With the Voice and Video Firmware add-on, users in a virtual environment can use Cisco UC Integration for Microsoft Lync or Cisco Unified Personal Communicator from their thin clients. The Voice and Video Firmware runs on the thin client, and Cisco UC Integration for Microsoft Lync or Cisco Unified Personal Communicator runs on the Windows hosted virtual desktop.

Power Management Settings with Voice and Video Firmware Add-On

By default, the Cisco VXC 6215 supports a power management setting (EnergyWise) whereby the clients enter the sleep mode after a specified period of time. When the Voice and Video Firmware add-on is enabled, this power management setting is disabled, and the clients do not enter the sleep mode.

For more information on the optional Voice and Video Firmware add-on, see the *Deployment Guide for Voice and Video Firmware for Cisco Virtualization Experience Client 6215.*

Downloading the Cisco VXC Add-On Software Packages

To download the Cisco VXC 6215 add-on software packages, follow these steps:

Procedure

Step 1 From your workstation, access http://www.cisco.com/cisco/software/navigator.html.

Step 2 Sign in with your Cisco.com user ID and password.

Step 3 On the Download Software page:

a. Choose **Products > Voice and Unified Communications > IP Telephony > Virtualized Endpoints**.

b. When the next page appears, choose **Cisco Virtualization Experience Client 6000 Series**.

c. Choose **Cisco Virtualization Experience Client 6215**.

d. In the the Add Ons folder, choose the add-on you require.

e. Click the **Download** button next to the WinZip file to launch a window with detailed information about the selected release and to add it to the Download Cart.

Step 4 Verify that the software and image information are what you want, and click **Proceed With Download**.

Step 5 Accept the conditions by entering the appropriate information into the User Details section and by clicking **Accept**.

Step 6 Read the Cisco End User License Agreement, and click **Agree**.

Step 7 Download and save the Cisco VXC 6215 add-on zip file to your workstation.

Step 8 Locate the saved file on the host or workstation, and unzip the file to your local drive or disk.

Managing Cisco VXC Manager Add-On Packages

Click **Package Manager** in the tree pane of the Cisco VXC Manager Administrator Console to open the Package Manager. The Package Manager allows you to quickly view and manage the Cisco VXC Manager packages that can be distributed to the devices within your Cisco VXC Manager environment.

Before using the Package wizard to create and register Cisco VXC Manager packages, you must understand the update distribution process and the contents of Cisco VXC Manager packages, know the location of the existing Cisco VXC Manager packages that you want to register, know the location of the base image, and know the add-ons you want to add to it when you create the bundled images. You must also ensure that the devices from which you will be getting images or configurations already have the Cisco VXC Manager Agent installed. After Cisco VXC Manager packages are registered, you can distribute the packages as updates to the devices within your Cisco VXC Manager network (see Update Manager, page 5-29).

Register a Package to Enable a Cisco Add-On

Use the following procedure to enable a Cisco add-on.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, extract the add-on files to a local folder (see Downloading the Cisco VXC Add-On Software Packages, page 4-5).

Note Assuming an add-on named ciscoaddontest1, the extracted add-on folder structure appears as follows:
~/ciscoaddontest1/wlx/wlx.ini
~/ciscoaddontest1/ADDONS/<rpmfilename>.rpm
~/ciscoaddontest1/ADDONS/directory
~/ciscoaddontest1.rsp

Step 2 In the extracted wlx.ini file, do not modify the existing parameters, but add any additional INI configurations you require.

Note If you have existing INI configurations on your clients, you must copy and paste these parameters into the wlx.ini that you push with the add-on; otherwise, the clients will lose the pre-existing configurations.

Step 3 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 4 Click the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 5 Enter the file path to the Cisco VXC Manager script file (RSP) file for the Cisco VXC Manager package (for example, ciscoaddontest1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 6 To have the Cisco VXC Manager package active for distribution, check the **Active** check box.

Step 7 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 8 Click **Next** to create and register the Cisco VXC Manager package.

Step 9 After the Cisco VXC Manager package is created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Register a Package to Disable a Cisco Add-On

There are two methods that you can use to disable a Cisco add-on, using either a remove-packages.sh file or a RemoveAddons INI parameter, as described in the following procedures.

Note You can uninstall add-ons using Cisco VXC Manager; however, when you upgrade the device to a new version of firmware, these add-ons may be reenabled in the updated firmware.

Disabling an Add-On Using the remove-packages.sh File

Use the following procedure to disable a Cisco add-on using the remove-packages.sh file.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, create a new folder for the add-on.

Step 2 Within this folder, create an RSP file with a name that starts with the ciscoaddon prefix, for example, ciscoaddon-remove1.rsp.

Step 3 To disable an add-on package, verify that the content of the RSP file is as follows:

```
[Version]
Number=ciscoaddon-remove1
Description=Remove sample Cisco Add-on package
OS=SLX
Category=Other Packages
USE_Pxe=NO

[Script]
CO "SLC"
LU
SF "<regroot">/*" "/tmp/"
EX "dos2unix /tmp/remove=packages.sh"
EX 'sh /tmp/remove-packages.sh"
EL
RB
```

Step 4 In the RSP script, ensure that the "Number=" segment has the exact same value as the RSP filename.

Step 5 In the add-on folder, create a subfolder with a name that matches the RSP file name, for example, ciscoaddon-remove1.

Step 6 Within the subfolder you created, create the remove-packages.sh file.

The contents of the remove-packages.sh file must be as follows:

```
#!/bin/bash
for addon in ciscoaddon-remove1
do
/usr/sbin/addon-remove $addon
done
```

Note The folder structure and the corresponding files for the add-on deployment must be as follows:
~ /ciscoaddon-remove1.rsp
~ /ciscoaddon-remove1/remove-packages.sh

Step 7 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 8 Click the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 9 Enter the file path to the Cisco VXC Manager script (RSP) file for the Cisco VXC Manager package (for example, ciscoaddon-remove1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 10 Depending on whether you want to have the Cisco VXC Manager package distributed (active for distribution), check or uncheck the **Active** check box.

Step 11 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 12 Click **Next** to create and register the Cisco VXC Manager package.

Step 13 After the Cisco VXC Manager package has been created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Disabling an Add-On Using the RemoveAddons INI Parameter

Use the following procedure to disable a Cisco add-on using the RemoveAddons INI parameter.

Procedure

Step 1 On the server on which you have Cisco VXC Manager installed, create a new folder for the add-on.

Step 2 Within this folder, create an RSP file with a name that starts with the ciscoaddon prefix, for example, ciscoaddon-remove2.rsp.

Step 3 If you want to disable an add-on package, verify that the content of the RSP file is as follows:

```
[Version]
Number=ciscoaddon-remove2
Description=Push and parse wlx.ini and image update package
OS=SLX
Category=Other Packages
USE_Pxe=NO

[Script]
EX "/bin/regset --persist System IniFileSource server"
RP "<regroot>"
EX "/usr/bin/perl /etc/addons.d/dispatcher.d/60.fetchIni eth0 up"
EX "/usr/bin/perl /sbin/dhcp2registry"
EX "/usr/sbin/thinclient-config --set-update-mode addons"
```

```
EX "sync"
EX "sleep 2"
RB
```

Step 4 In the RSP script, ensure that the “Number=” segment has the exact same value as the RSP filename and folder name.

Step 5 Within the add-on folder, create a subfolder with a name that matches the RSP file name, for example, ciscoaddon-remove2.

Step 6 Within this folder, create a subfolder named **wlx**.

Step 7 Within the wlx folder, create a wlx.ini file.

Note The folder structure and the corresponding files for the add-on deployment must be as follows:
`~/ciscoaddon-remove2/wlx/wlx.ini`
`~/ciscoaddon-remove2.rsp`

Step 8 Verify that the content of the wlx.ini file is as follows:

```
Update.Preserve_changes=Yes
Update.Mode=Addons
RemoveAddons=ciscoaddon-remove2.rpm
```

Step 9 In the wlx.ini file, ensure that the “RemoveAddons=” segment has the exact same value as the RPM filename of the add-on to remove.

Note If you are removing multiple add-ons, then you must specify all the RPM files in a comma-separated list in the RemoveAddon segment. For example:
RemoveAddons=ciscoaddon-remove2.rpm,ciscoaddon-remove3.rpm,ciscoaddon-remove4.rpm

Step 10 In the tree pane of the Administrator Console, right-click **Package Manager** and choose **New > Package** to open the Package wizard.

Step 11 Choose the **Register a Package from a Script File (.RSP)** option and click **Next**.

Step 12 Enter the file path to the Cisco VXC Manager script (RSP) file for the Cisco VXC Manager package (for example, ciscoaddontest1.rsp) you want to register (you can use Browse to find and choose a file), and then click **Next** to open the Software Package Information dialog box.
The wizard obtains and displays the name, description, and category of the Cisco VXC Manager package.

Step 13 Depending on whether you want to have the Cisco VXC Manager package distributed (active for distribution), check or uncheck the **Active** check box.

Step 14 Click **Next**.
The wizard notifies you that it is ready to create and register the new Cisco VXC Manager package.

Step 15 Click **Next** to create and register the Cisco VXC Manager package.

Step 16 After the Cisco VXC Manager package is created and registered, click **Finish**.
The Cisco VXC Manager package is copied to the Master Repository and is displayed under the appropriate category. The Cisco VXC Manager package is now ready for distribution (see Managing the Schedules for Device Updates, page 5-29).

Updating the Cisco VXC 6215 Client Configuration

Use this procedure to create a SUSE Linux package to upgrade the Cisco VXC 6215 client configuration.

Procedure

Step 1 Create a folder to contain the client configurations, for example 6215Configs.

Step 2 In the 6215Configs folder, create an RSP file named SLE1.rsp with the following content:

```
[Version]
Number=SLE1
OS=SLX
Category=Other Packages
USE_Pxe=NO
[Script]
RP "<regroot>"
EX "/usr/bin/perl /sbin/dhcp2registry"
EX "/usr/sbin/thinclient-config --set-update-mode both"
EX "/usr/sbin/thinclient-config --set-force-image-update no"
EX "sync"
EX "sleep 2"
RB
RB
```

where the "Number=" segment must have the exact same value as the RSP file name.

Note This RSP script is provided as an example; you may need to reconfigure the parameters depending on your environment.

Step 3 Also in the 6215Configs folder, create a subfolder using the same name as the RSP file name, for example SLE1.

Step 4 In the SLE1 folder, create a subfolder named wlx.

Step 5 In the wlx folder, create a file named wlx.ini that contains the required configuration. (See *Cisco Virtual Experience Client 6215 INI Files Reference Guide* for more information.) For example:

- Location and name of .rsp image:

  C:\VXC-M\6215Configs\SLE1.rsp
- Location and name of wlx directory:

  C:\VXC-M\6215Configs\SLE1\wlx
- Location and name of wlx.ini file in wlx directory:

  C:\VXC-M\6215Configs\SLE1\wlx\wlx.ini

Step 6 In the tree pane of the Administrator Console, expand **Package Manager**.

Step 7 In the details pane, right-click **Other Packages** and choose **New > Package**.

Step 8 Choose **Register a Package from a Script file (.RSP)** and click **Next**.

Step 9 Click **Browse** to choose the file path of the .rsp package file you want to register (For example: C:\VXC-M\6215Configs\SLE1.rsp) and click **Open**.

Step 10 Click **Next** to display the Package Wizard summary.

Step 11 Click **Next** to see the Package Registration Progress screen.

Step 12 Click **Next** to create the package.

Step 13 After the package is created and registered, click **Finish**.

Step 14 To upgrade the Cisco VXC 6215, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Cisco VXC 2111/2211 PCoIP Client Upgrade Procedures

The following sections describe how to update the PCoIP firmware image and client configurations:

- Updating the PCoIP Firmware Image, page 4-11
- Updating the PCoIP Client Configuration (Building and Registering a ThreadX Package), page 4-11

Updating the PCoIP Firmware Image

To update the firmware image on a Cisco VXC PCoIP client, perform the following procedure.

Procedure

Step 1 Download the PCoIP image package from the Cisco Software Download page at the following URL:

http://www.cisco.com/cisco/software/navigator.html?mdfid=283759601&i=rm

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped firmware files to a local folder.

Step 3 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Note To upgrade the image on PCoIP devices, the Category parameter in the RSP file must be set to Images (Category=Images).

Step 4 To upgrade the Cisco VXC 2111/2211, you can use Default Device Configuration or use the Drag-and-Drop method (see Managing Default Device Configurations, page 7-66 and Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35)

Updating the PCoIP Client Configuration (Building and Registering a ThreadX Package)

You can configure the following configuration packages for mass deployment to ThreadX devices:

- **VMwareView Packages**: You can deploy a VMwareView package to the ThreadX devices to configure the VM server settings.
- **Video Packages**: You can deploy a video package to ThreadX devices to configure global video settings such as minimum and maximum image quality settings.

- **RDP Packages**: You can deploy an RDP package to ThreadX devices to configure global RDP settings.

Note Cisco does not provide support for RDP network implementations with the Cisco VXC 2111/2211 PCoIP clients running ThreadX firmware.

- **Additional configuration packages**: You can also deploy additional configuration packages including: timezone and international language settings.

After configuring these packages, you can use DDC or drag and drop to schedule the deployment of the packages to the devices you want (for more information on scheduling packages, see Update Manager, page 5-29).

Tip You can use the sample ThreadX packages that are bundled with Cisco VXC Manager. To create customized packages, modify these sample ThreadX packages, which you can then deploy to ThreadX devices. The sample ThreadX packages are located in the ThreadX Configuration folder (under the Package Manager node).

Customizing the Existing Sample ThreadX Packages

Use the following guidelines to customize the existing sample ThreadX packages.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Package Manager > ThreadX Configuration**.

Step 2 In the details pane, right-click the desired sample package and choose **View Package Script** to open the Package Script dialog box displaying the script of the Cisco VXC Manager package.

Step 3 Check the **Edit and Save Script to Database ONLY** check box and then configure the parameters as desired.

Step 4 After completing your changes, click **OK**.

Step 5 Schedule the package update using Default Device Configuration (see Managing Default Device Configurations, page 7-66) or using the Drag-and-Drop method (see Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Creating New ThreadX Packages

Use the following guidelines to configure additional customized ThreadX packages based on the existing ThreadX packages.

Procedure

Step 1 Create a folder to contain the new package (for example, VMwareViewTest1).

Step 2 In the tree pane of the Administrator Console, expand **Package Manager > ThreadX Configuration**.

Step 3 In the details pane, right-click the desired package and choose **Export Package Script**.

Step 4 Browse to the folder you created in Step 1, and click **OK**.

Step 5 Rename the exported RSP file to match the name of the folder you created in Step 1 (for example, VMwareViewTest1.rsp).

Step 6 Use a text editor to edit the RSP file script for the requirements of your environment.

The following shows an example VMwareView script:

```
[Version]
Number=VMWareViewTest1
Description=ThreadX VMWareView Configuration
OS=TDC
Category=ThreadX Configuration
[Script]
IP=10.10.10.1
SSL=0
AutoLaunchIfOnlyOneDesktop=0
AutoConnect=0
Enable Kiosk Mode=1
Enable custom username=1
Username=user123
Password=
```

Be sure that the Number= segment has the exact same value as the RSP file name and folder name (this naming convention applies to all packages).

Step 7 Register the package (see Register a Package from a Script File (.RSP), page 3-35).

Step 8 Schedule the package update using Default Device Configuration (see Managing Default Device Configurations, page 7-66) or using the Drag-and-Drop method (see Scheduling Device Updates Using the Drag-and-Drop Method, page 5-35).

Supported Parameters for ThreadX VMware View Packages

You can use a VMware View package to configure View Connection Server settings on ThreadX devices. To configure a VMware View package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following table describes the parameters supported in the script of a VMware View package.

Table 4-1 VMWare View Package Parameter Definitions

Parameter	Definition
IP=	Connection server IP address
Port=	Port number (integer value between 1 and 65535).
SSL=	Use secure connection (SSL). Enter 0 for no, 1 for yes.
AutoLaunchIfOnlyOneDesktop=	Auto Launch if only one desktop. Enter 0 for no, 1 for yes.
AutoConnect=	Always connect to this server at startup. Enter 0 for no, 1 for yes.
Enable Kiosk Mode=	Enter 0 for no, 1 for yes.
Enable custom username=	Enter 0 for no, 1 for yes.

Table 4-1 VMWare View Package Parameter Definitions

Parameter	Definition
Username=	User name if enable custom username is true (Enable custom username=1)
Password=	Specifies the password for the specified username.

VMware View Package Example

The following shows an example script for a VMware View package.

```
[Version]
Number=VMWareView_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
IP=10.100.5.5
Port=999
SSL=1
AutoLaunchIfOnlyOneDesktop = 1
AutoConnect=1
Enable Kiosk Mode=1
Enable custom username = 1
Username=Tester
Password=PW
```

Supported Parameters for ThreadX Language Packages

You can use a Language package to configure language and keyboard settings on ThreadX devices. To configure a Language package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following sections describe the parameters supported in the script of a Language package.

Language=

The Language= parameter allows you to set the language for the On Screen Display GUI on the device.

Table 4-2 Language Parameter Values

Language	Parameter Value
Chinese-Simplified	zh_CN
Chinese-Traditional	zh_TW
English	en
French	fr
German	de
Greek	el
Italian	it
Japanese	ja

Table 4-2 Language Parameter Values

Language	Parameter Value
Korean	ko
Portuguese	pt
Spanish	es

Keyboard Layout=

The Keyboard Layout= parameter sets the layout and language of the keyboard according to the language selected.

Table 4-3 Keyboard Layout Parameter Values

Keyboard Layout Language	Parameter Value
Belgian ISO-8859-1	be.iso
Belgian ISO-8859-1 (accent keys)	be.iso.acc
Danish Codepage 865	danish.cp865
Danish ISO-8859-1	danish.iso
Danish ISO-8859-1 (accent keys)	danish.iso.acc
Dutch ISO-8859-1 (accent keys)	dutch_iso.acc
Finnish Codepage 850	finnish.cp850
Finnish ISO-8859-1	finnish.iso
Finnish ISO-8859-1 (accent keys)	finnish.iso.acc
French Canadian ISO-8859-1 (accent keys)	fr.ca.iso.acc
French Dvorak-like	fr.dvorak
French Dvorak-like (accent keys)	fr.dvorak.acc
French ISO-8859-1	fr.iso
French ISO-8859-1 (accent keys)	fr.iso.acc
German Codepage 850	german.cp850
German ISO-8859-1	german.iso
German ISO-8859-1 (accent keys)	german.iso.acc
Greek ISO-8859-7 (104 keys)	el.iso07
Italian ISO-8859-1	it.iso
Japanese 106/109	jp.106
Japanese 106x (ctrl and shift swapped)	jp.106x
Korean Dubeolsik ISO-8859-1	kr.iso
Latin American	latinamerican
Latin American (accent keys)	latinamerican.iso.acc
Lithuanian	lt.iso
Norwegian Dvorak	norwegian.dvorak

Table 4-3 Keyboard Layout Parameter Values (continued)

Keyboard Layout Language	Parameter Value
Norwegian ISO-8859-1	norwegian.iso
Norwegian ISO-8859-1 (accent keys)	norwegian.iso.acc
Polish ISO-8859-2 (Programmers)	pl.iso2.pro
Portuguese ISO-8859-1	pt.iso
Portuguese ISO-8859-1 (accent keys)	pt.iso.acc
Russian	ru.iso
Spanish ISO-8859-1	spanish.iso
Spanish ISO-8859-1 (accent keys)	spanish.iso.acc
Spanish ISO-8859-15 (accent keys)	spanish.iso15.acc
Swedish Codepage 850	swedish.cp850
Swedish ISO-8859-1	swedish.iso
Swedish ISO-8859-1 (accent keys)	swedish.iso.acc
Swiss-French Codepage 850	swissfrench.cp850
Swiss-French ISO-8859-1	swissfrench.iso
Swiss-French ISO-8859-1 (accent keys)	swissfrench.iso.acc
Swiss-German Codepage 850	swissgerman.cp850
Swiss-German ISO-8859-1	swissgerman.iso
Swiss-German ISO-8859-1 (accent keys)	swissgerman.iso.acc
Turkish Q ISO-8859-9	tr.iso9.q
Turkish Q ISO-8859-9 (accent keys)	tr.iso9.q.acc
United Kingdom Codepage 850	uk.cp850
United Kingdom Codepage 850 (ctrl and caps swapped)	uk.cp850.ctrl
United Kingdom ISO-8859-1	uk.iso
United Kingdom ISO-8859-1 (ctrl and caps swapped)	uk.iso.ctrl
United States of America dvorak	us.dvorak
United States of America dvorakx	us.dvorakx
United States of America Emacs optimized layout	us.emacs
United States of America ISO-8859-1	us.iso
United States of America ISO-8859-1 (accent keys)	us.iso.acc
United States of America ISO-8859-1 (ctrl and caps swapped)	us.pc.ctrl
United States of America lefthand dvorak	us.dvorakl

Table 4-3 Keyboard Layout Parameter Values (continued)

Keyboard Layout Language	Parameter Value
United States of America righthand dvorak	us.dvorakr
United States of America Traditional Unix Workstation	us.unix

Language Package Example

The following shows an example script for a ThreadX Language package.

```
[Version]
Number=Language_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
Language=en
Keyboard Layout=us.iso
```

Supported Parameters for ThreadX TimeZone Packages

You can use TimeZone packages to specify the time zone on ThreadX devices. To configure a TimeZone package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12.

The following tables describe the parameters supported in the script of a TimeZone package.

Table 4-4 TimeZone Package Parameter Definitions

Parameter	Definition
NTP Server=	NTP Host DNS Name (IP Address or FQDN)
Query Interval=	NTP Query Interval (integer value - number of seconds) Valid range is: 900–60480000.
Port=	NTP Host Port (integer value between 1 and 65535)
Enable Daylights Saving=	Enable Daylight Saving Time. Enter 0 for no, 1 for yes.
Time Zone=	See the following table for possible values.

Table 4-5 Time Zone Parameter Values

Time Zone	Parameter Value
(GMT-12:00) International Date Line West	gmt_minus_1200_international_date_line_west
(GMT-11:00) Midway Island, Samoa	gmt_minus_1100_midway_island
(GMT-10:00) Hawaii	gmt_minus_1000_hawaii
(GMT-09:00) Alaska	gmt_minus_0900_alaska
(GMT-08:00) Pacific Time (US & Canada)	gmt_minus_0800_pacific_time
(GMT-08:00) Tijuana, Baja California	gmt_minus_0800_tijuana

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT-07:00) Arizona	gmt_minus_0700_arizona
(GMT-07:00) Chihuahua, La Paz, Mazatlan - New	gmt_minus_0700_chihuahua_new
(GMT-07:00) Chihuahua, La Paz, Mazatlan - Old	gmt_minus_0700_chihuahua_old
(GMT-07:00) Mountain Time (US & Canada)	gmt_minus_0700_mountain_time
(GMT-06:00) Central America	gmt_minus_0600_central_america
(GMT-06:00) Central Time (US & Canada)	gmt_minus_0600_central_time
(GMT-06:00) Guadalajara, Mexico City, Monterrey - New	gmt_minus_0600_guadalajara_new
(GMT-06:00) Guadalajara, Mexico City, Monterrey - Old	gmt_minus_0600_guadalajara_old
(GMT-06:00) Saskatchewan	gmt_minus_0600_saskatchewan
(GMT-05:00) Bogota, Lima, Quito, Rio Branco	gmt_minus_0500_bogota
(GMT-05:00) Eastern Time (US & Canada)	gmt_minus_0500_eastern_time
(GMT-05:00) Indiana (East)	gmt_minus_0500_indiana
(GMT-04:30) Caracas	gmt_minus_0430_caracas
(GMT-04:00) Atlantic Time (Canada)	gmt_minus_0400_atlantic_time
(GMT-04:00) La Paz	gmt_minus_0400_la_paz
(GMT-04:00) Manaus	gmt_minus_0400_manaus
(GMT-04:00) Santiago	gmt_minus_0400_santiago
(GMT-03:30) Newfoundland	gmt_minus_0330_newfoundland
(GMT-03:00) Brasilia	gmt_minus_0300_brasilia
(GMT-03:00) Buenos Aires, Georgetown	gmt_minus_0300_buenos_aires
(GMT-03:00) Greenland	gmt_minus_0300_greenland
(GMT-03:00) Montevideo	gmt_minus_0300_montevideo
(GMT-02:00) Mid-Atlantic	gmt_minus_0200_mid_atlantic
(GMT-01:00) Azores	gmt_minus_0100_azores
(GMT-01:00) Cape Verde Is.	gmt_minus_0100_cape_verde_is
(GMT) Casablanca, Monrovia, Reykjavik	gmt_plus_0000_casablanca
(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	gmt_plus_0000_greenwich_mean_time
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	gmt_plus_0100_amsterdam
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	gmt_plus_0100_belgrade
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris	gmt_plus_0100_brussels
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb	gmt_plus_0100_sarajevo
(GMT+01:00) West Central Africa	gmt_plus_0100_west_central_africa
(GMT+01:00) Windhoek	gmt_plus_0100_windhoek
(GMT+02:00) Amman	gmt_plus_0200_amman

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT+02:00) Athens, Bucharest, Istanbul	gmt_plus_0200_athens
(GMT+02:00) Beirut	gmt_plus_0200_beirut
(GMT+02:00) Cairo	gmt_plus_0200_cairo
(GMT+02:00) Harare, Pretoria	gmt_plus_0200_harare
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius	gmt_plus_0200_helsinki
(GMT+02:00) Jerusalem	gmt_plus_0200_jerusalem
(GMT+02:00) Minsk	gmt_plus_0200_minsk
(GMT+03:00) Baghdad	gmt_plus_0300_baghdad
(GMT+03:00) Kuwait, Riyadh	gmt_plus_0300_kuwait
(GMT+03:00) Moscow, St. Petersburg, Volgograd	gmt_plus_0300_moscow
(GMT+03:00) Nairobi	gmt_plus_0300_nairobi
(GMT+03:30) Tehran	gmt_plus_0330_tehran
(GMT+04:00) Abu Dhabi, Muscat	gmt_plus_0400_abu_dhabi
(GMT+04:00) Baku	gmt_plus_0400_baku
(GMT+04:00) Caucasus Standard Time	gmt_plus_0400_caucasus_standard_time
(GMT+04:00) Yerevan	gmt_plus_0400_yerevan
(GMT+04:30) Kabul	gmt_plus_0430_kabul
(GMT+05:00) Ekaterinburg	gmt_plus_0500_ekaterinburg
(GMT+05:00) Islamabad, Karachi, Tashkent	gmt_plus_0500_islamabad
(GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi	gmt_plus_0530_chennai
(GMT+05:30) Sri Jayawardenepura	gmt_plus_0530_sri_jayawardenepura
(GMT+05:45) Kathmandu	gmt_plus_0545_kathmandu
(GMT+06:00) Almaty, Novosibirsk	gmt_plus_0600_almaty
(GMT+06:00) Astana, Dhaka	gmt_plus_0600_astana
(GMT+06:30) Yangon (Rangoon)	gmt_plus_0630_yangon
(GMT+07:00) Bangkok, Hanoi, Jakarta	gmt_plus_0700_bangkok
(GMT+07:00) Krasnoyarsk	gmt_plus_0700_krasnoyarsk
(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi	gmt_plus_0800_beijing
(GMT+08:00) Irkutsk, Ulaan Bataar	gmt_plus_0800_irkutsk
(GMT+08:00) Kuala Lumpur, Singapore	gmt_plus_0800_kuala_lumpur
(GMT+08:00) Perth	gmt_plus_0800_perth
(GMT+08:00) Taipei	gmt_plus_0800_taipei
(GMT+09:00) Osaka, Sapporo, Tokyo	gmt_plus_0900_osaka
(GMT+09:00) Seoul	gmt_plus_0900_seoul
(GMT+09:00) Yakutsk	gmt_plus_0900_yakutsk
(GMT+09:30) Adelaide	gmt_plus_0930_adelaide

Table 4-5 Time Zone Parameter Values (continued)

Time Zone	Parameter Value
(GMT+09:30) Darwin	gmt_plus_0930_darwin
(GMT+10:00) Brisbane	gmt_plus_1000_brisbane
(GMT+10:00) Canberra, Melbourne, Sydney	gmt_plus_1000_canberra
(GMT+10:00) Guam, Port Moresby	gmt_plus_1000_guam
(GMT+10:00) Hobart	gmt_plus_1000_hobart
(GMT+10:00) Vladivostok	gmt_plus_1000_vladivostok
(GMT+11:00) Magadan, Solomon, Is., New Caledonia	gmt_plus_1100_magadan
(GMT+12:00) Auckland, Wellington	gmt_plus_1200_auckland
(GMT+12:00) Fiji, Kamchatka, Marshal Is.	gmt_plus_1200_fiji
(GMT+13:00) Nuku'alofa	gmt_plus_1300_nukualofa

TimeZone Package Example

The following shows an example script for a TimeZone package.

```
[Version]
Number=TimeZone_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
NTP Server=10.100.5.5
Query Interval=3600
Port=9999
Enable Daylights Saving=1
Time Zone=gmt_minus_1000_hawaii
```

Supported Parameters for ThreadX Video Packages

You can use a Video package to configure video image quality settings on ThreadX devices. To configure a Video package, see Customizing the Existing Sample ThreadX Packages, page 4-12 and Creating New ThreadX Packages, page 4-12. The following table describes the parameters supported in the script of a Video package. A lower image quality allows a higher frame rate when network bandwidth is limited.

Table 4-6 Video Package Parameter Definitions

Parameter	Definition
Cursur_enable=	Enable Local Cursor. Enter 0 for no, 1 for yes.
Min_Img_Qty=50	Minimum Image Quality. Range: 30 to 100.
Max_Img_Qty=80	Maximum Image Quality. Range: 30 to 100.

Video Package Example

The following shows an example script for a Video package.

```
[Version]
Number=Video_Test
Description=Test Script
OS=TDC
Category=ThreadX Configuration
[Script]
Cursur_enable=1
Min_Img_Qty=50
Max_Img_Qty=80
```

Cisco VXC 2112/2212 ICA Client Upgrade Procedures

The following sections describe how to update the ICA firmware image and client configurations:

- Updating the ICA Firmware Image, page 4-21
- Updating the ICA Client Configuration (Building and Registering a WTOS package), page 4-22

Note When Cisco VXC Manager deploys packages to Cisco VXC 2112/2212 ICA devices, it notifies the devices to download the updated firmware or configuration from a specific folder location on the server. The ICA devices then update themselves but do not notify the Cisco VXC Manager server.

Updating the ICA Firmware Image

To update the firmware image on a Cisco VXC ICA client, perform the following procedure.

Procedure

Step 1 Download the OS image from the Cisco Software Download page at the following URL:

http://www.cisco.com/cisco/software/navigator.html?mdfid=283759601&i=rm

Step 2 On the server where you have Cisco VXC Manager installed, extract the zipped firmware files to a local folder.

Step 3 Register the package (see Register a Package from a Script File (.RSP), page 3-35). When you are prompted for an RSP file during the package registration process, browse and choose the RSP file that is contained in the unzipped package.

Note To upgrade the image on ICA devices, the Category parameter in the RSP file must be set to Images (Category=Images).

Step 4 Configure the following WTOS preferences:

a. In the tree pane of the Preferences dialog box, click **WTOS**.

b. Ensure that the WTOS Root Path field contains **WNOS**.

c. Click **OK**.

Step 5 To upgrade the Cisco VXC 2112/2212, use Default Device Configuration (see Managing Default Device Configurations, page 7-66).

Note ICA Clients only support the Default Device Configuration method for upgrades. They do not support drag and drop.

Updating the ICA Client Configuration (Building and Registering a WTOS package)

Use this procedure to update the ICA client configuration using a WTOS package.

Procedure

Step 1 Create a folder to contain the client configurations, for example **ICAConfigs**.

Step 2 In the ICAConfigs folder, create an RSP file named ICA1.rsp with the following content:

```
[Version]
Number=ICA1
Description=Package for ICA client upgrade
OS=BL
Category=Images
Imagetype=Merlin
Mediasize=128
[Script]
```

where the "Number=" segment must have the exact same value as the RSP file name.

Step 3 Also in the ICAConfigs folder, create a subfolder using the same name as the RSP file name, for example **ICA1**.

Step 4 In the ICA1 folder, create a subfolder named **WNOS**.

Step 5 In the WNOS folder, create a file named wnos.ini that contains the required configuration. (See *Cisco Virtual Experience Client 2112/2212 WTOS INI Files Reference Guide* for more information, including sample .ini files.)

For example:

- Location and name of RSP image:

  C:\VXC-M\ICAConfigs\ICA1.rsp
- Location and name of WNOS directory:

  C:\VXC-M\ICAConfigs\ICA1\WNOS
- Location and name of wnos.ini file in WNOS directory:

  C:\VXC-M\ICAConfigs\ICA1\WNOS\wnos.ini

Step 6 Register the package (see Register a Package from a Script File (.RSP), page 3-35).

Step 7 Ensure the following additional WTOS preferences are configured appropriately:

a. In the tree pane of the Preferences dialog box, click **WTOS**.

b. Ensure that the WTOS Root Path field contains **WNOS**.

c. Click **OK**.

Step 8 To upgrade the Cisco VXC 2112/2212, use Default Device Configuration (see Managing Default Device Configurations, page 7-66).

Note In the Default Device Configuration wizard, on the Primary Definition tab, choose the name of the package you just registered in the Qualifying OS Image field to update the ICA client configuration.

Upgrading Clients Using a Remote Repository

Cisco VXC Manager supports a built-in scalability feature in the form of remote repositories. In order to preserve bandwidth and perform upgrades more efficiently, you can configure a remote repository that is closer to the physical location of your devices. The configuration of a remote repository involves setting up the remote repository, registering the repository in Cisco VXC Manager, syncing packages with the remote repository, and specifying which subnet is associated with which repository.

In the current release, the only method of assigning devices to a remote repository is by device subnet.

For more information, see Understanding Cisco VXC Manager Repositories, page 7-86, Scheduling a Remote Repository Synchronization, page 5-38, and Adding Subnets to Cisco VXC Manager Manually, page 7-91.

Understanding the Cisco VXC Manager Package Structure

A Cisco VXC Manager Package structure consists of two components:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

In order for a Package to function properly, these two components must adhere to the following structural rules:

- The Package script file must have an .rsp extension. You can create and edit an RSP file using Notepad.
- The Package folder must have the same name as the Package script file.
- The Number= parameter in the [Version] section of the Package script file should match the value reported by the device to the Client Manager. This becomes extremely important when using the Default Device Configuration feature.
- All the files referenced by the Package script file must be within the Package folder or a subfolder within.
- All command arguments should be enclosed in double-quotes and are separated by spaces ONLY.
- All registry paths are delimited with backslashes (‘\’) and are within quotes.
- Do not use abbreviations for the root registry keys (e.g. use HKEY_LOCAL_MACHINE, not HKLM).
- All filenames are delimited with backslashes (‘\’) and are within quotes.
- Neither path names nor registry branches should ever end with a backslash.

- In general, a script is aborted if a command fails. If you do not want the script to abort if a command fails, then appended the command with and asterisk (*). (Note not all commands support this).
- <REGROOT> (e.g. <regroot>\sourcefile.txt) points to the root directory of the registered package (e.g. c:\inetpub\ftproot\rapport\<packagename>).

Tip <regroot> is a pointer that tells the Cisco VXC Manager Service to look in a specific location on the Cisco VXC Manager server (not the device) for Package application files. <regroot> finds the Cisco VXC Manager Master Repository and identifies the folder contained within that is holding the needed Package files.

Understanding the Script File Structure

A Cisco VXC Manager script (RSP) file is one of two components that make up a Cisco VXC Manager Package:

- The Package script (RSP) file (ImgXL24.rsp)
- The Package folder that contains the required application or image files (ImgXL24)

The Package script (RSP) file must conform to a specific structure and should contain two sections:

- Version
- Script

Version

The Version section contains information required for package registration and distribution purposes. The following describes each of the elements of the Version section:

[Version] - Required section header

Number= - Must be the same as the Package Script File name

Description= - A brief description of what the Package is to achieve

OS= -The Operating System the Package is intended for

USE_REMOTE= - YES/NO, specifies whether or not a Remote Repository (if it exists) should be used. Default is YES. (OPTIONAL)

DEPLOYEDSW= - YES/NO defines whether package should be added to the Cisco VXC Manager deployed package table for device. Default is YES. (OPTIONAL)

Category= - The Cisco VXC Manager Package Manager category in the Administrator Console where the package will reside. Note if the category does not exist it will be created.

Image Category Special Tags

[Version] - Required section header

ImageSize= - size of image in Megabytes

BootFloppy= - name of bootfloppy; default is RAPPORT

IMAGE= - name of image file to be used; by default Cisco VXC Manager uses the first file found in the package folder (excluding CRC.text)

Command= - the image operation to be performed

Script

The Script section contains the commands that are carried out when the script is distributed. Each command is executed in order as they appear within the [Script] section.

Recommended Scripting Template

```
[Version]
Number=Script name (matching the RSP_ file name and Package folder name)
Description=Detailed description with version number and valid images
OS=XX
Category=Other Packages
[Script]
Written by: Your Name and Company
; ..........................................................................
; >Check the Operating System
; >Check the Image Version
; ..........................................................................
CO "NT"
CI “XXXX”
; ..........................................................................
; >Check Free Space
; >Check Minimum Memory, if necessary
; >Check User, if necessary
; ..........................................................................
CF “X” “XXX”
CR “XXXX”
CU “XXXXXXXX”
; ..........................................................................
; > Query User then lock Workstation
; ..........................................................................
QU
LU*
; ..........................................................................
; >Add Commands Here
; ..........................................................................
;SF “<regroot>\files\x.xxx” “c:\yyyy\zzzz”
;EX “c:\yyyy\zzzz”
;DF “c:\yyyy\zzzz”
;MR “<regroot>\xxxx.reg”
;SP "c:\windows\system.ini" "DISPLAY" "screen-size" "640"
; ..........................................................................
; >End Lockout
; ..........................................................................
EL*
; ..........................................................................
; >Reboot, if necessary
; ..........................................................................
RB
---------------------------------------------------------------------------
```

Version

The Version section contains information required for package registration and distribution purposes.

BootFloppy=

Specifies the boot floppy Cisco VXC Manager uses during the imaging process:

- Rapportitf.0 (Cisco VXC Manager Imaging agent for imaging)

Category=

Defines the category for the Package. If you type a different category name in Category=, and then register the Package using Cisco VXC Manager, a folder is created under the Package Manager with that name.

Tip A package can be moved from one category to another by changing Category= and re-registering the package.

Command=

The image operation to be performed.

Example: Command=%ImageWrite%

Possible Values:

- %ImageWrite% (This value writes to the DiskOnChip)
- %ImageRead% (This value reads from the DiskOnChip)

DeployedSW=

This defines whether the package should be added to the Cisco VXC Manager deployed package table for the device.

DEPLOYEDSW=Yes or No - Default is Yes if not specified or specified incorrectly. This option is used primarily in conjunction with DDC. If a DDC has Enforce Sequence enabled any package sent to the device will trigger the DDC to re-image the device (thereby removing all packages). Using DeployedSW=No allows the user to send packages to devices without logging their distribution, thereby not triggering a DDC operation.

Description=

Allows the script developer to add a short description about the Package. The description is a comment line and is not parsed by Cisco VXC Manager when the script is executed.

Image=

This defines the file name to be used when reading or writing an image.

Image=filename - The default is the first file found in <regroot> excluding CRC.txt.

ImageSize=

Identifies for Cisco VXC Manager the size of image being sent to a client.

Values: 8, 16, 24, 32, 48, 64, 72, 80, 96, 128, 144, 192, 256, 512, 1024

Number=

Identifies for Cisco VXC Manager the name of the Package. The name of the Package script (RSP) file must match the Number= parameter. For example, if the Package script name is ImgXL24.rsp, you must have Number=ImgXL24 in the [Version] section of ImgXL24.rsp.

Example:

```
[Version]
Number=[Number reported by device in Device Manager under Image]
Description=Image to Write to Device
OS=NT
Category=Images
USE_PXE=YES
USE_REMOTE=NO
DEPLOYEDSW=YES
IMAGE=[xyz24xl.img]
IMAGESIZE=24
```

OS=

Defines the Operating System the device is running.

Values:

- BL WTOS
- SLX SUSE Linux
- TDC ThreadX

Use_Remote=

This defines whether the package should use a Remote Repository assigned to its subnet or if it should always use the Master.

Use_Remote=Yes or No - Default is Yes, if not specified or specified incorrectly.