Cisco VXC 6215 Firmware Release 9.0 setup

Cisco thin clients are designed to be centrally managed and configured using INI files and the Cisco VXC Manager. This chapter describes the Cisco VXC Manager procedures required to apply client configurations on Cisco VXC 6215 devices running Firmware Release 9.0. For detailed information about using Cisco VXC Manager, see *Administration Guide for Cisco Virtualization Experience Client Manager*.

Note This chapter describes the steps required to manage devices that are already running Firmware Release 9.0. For information about upgrading Cisco VXC 6215 devices from Release 8.6 or 8.7 to Release 9.0, see Upgrading to Firmware Release 9.0.

This chapter contains the following topics:

High-level steps for initial setup

The following are the high-level steps required to set up your Cisco VXC 6215 environment.

Note To interoperate with Cisco VXC 6215 Firmware Release 9.0, you must run Cisco VXC Manager 4.9.1. If you are running a previous release of Cisco VXC Manager, you can still discover and manage Cisco VXC 6215 devices running Firmware Release 9.0, but real-time commands are not supported.

For upgrades, Cisco recommends that you first upgrade your Cisco VXC Manager management server to release 4.9.1, and then upgrade your Cisco VXC 6215 devices to Firmware Release 9.0.

Procedure

Step 1 Set up your virtualization server (see your virtualization server documentation).

Step 2 Install or upgrade to Cisco VXC Manager 4.9.1 (see *Installation Guide for Cisco Virtualization Experience Client Manager*).

Step 3 Connect at least one Cisco VXC 6215 to your network and power it on.

Step 4 Set up device discovery in Cisco VXC Manager (DHCP is the recommended method—see Client discovery using Cisco VXC Manager, on page 5).

Step 5 Create the INI files to centrally configure the thin clients (see Create a wlx.ini file for client configuration, on page 10).

Step 6 Set up a configuration package in Cisco VXC Manager referencing the desired INI configuration (see Create a Cisco VXC Manager package for the wlx.ini file, on page 14).

Step 7 Push the configuration package to your thin clients (see Schedule device updates using Default Device Configuration, on page 17).

Best practices for Cisco VXC 6215 management using Cisco VXC Manager

The following are best practices for management of Cisco VXC 6215 devices using Cisco VXC Manager.

HTTP and HTTPS with Cisco VXC Manager

- With Firmware Release 9.0, the Cisco VXC 6215 can support Cisco VXC Manager 4.9.1 using HTTP or HTTPS , but not FTP. Set the Cisco VXC Manager to use HTTP or HTTPS for server communications (using a custom installation).
- If you enable HTTPS on Cisco VXC Manager, it always uses HTTPS whether the Cisco VXC 6215 has certificates installed or not. If you do not have a certificate on the device, the upgrade can still proceed.
- If you enable HTTPS on Cisco VXC Manager, and an upgrade for the Cisco VXC 6215 fails, Cisco VXC Manager does not fallback to attempting HTTP, unlike the standard HAgent process. Instead, Cisco VXC Manager returns an error after three attempts using HTTPS.
- When you configure the software repository, you can check the Secure (HTTPS) check box to enable HTTPS. However, the Validate Certificate with CA check box has no effect. Regardless of whether the latter option is enabled, the certificates are used for encryption only, not authentication, and so they are not validated against a trusted CA.

- To upgrade to Firmware Release 9.0, you must first ensure HTTPS is disabled on Cisco VXC Manager. The upgrade process supports HTTP only. After you perform the update to Firmware Release 9.0, you can then re-enable HTTPS.

Drag-and-Drop not supported

With Firmware Release 9.0, DDC is the only supported method available to push packages. Drag-and-Drop is not supported. (Drag-and-Drop may function in small environments or for test purposes. However, it will not function at all for thin clients behind a Cisco AnyConnect VPN.)

The benefits of using DDC are as follows:

- A specific configuration for your thin clients is always available for download (Drag-and-Drop is available only once, and in case of errors, the thin client cannot download the same configuration again).
- A specific configuration can be applied to multiple machines (all devices or sub-groups).
- A brand new device can download the correct package without the need to specify a new configuration (all new devices will use the same applied DDC configuration).

Single package deployment

Cisco recommends that you always deploy only one DDC package containing the base image, all the add-ons you need, and the required INI file. If you must change anything inside the package, create a brand new package with a different name.

New INI and RSP files required for Firmware Release 9.0

The INI and RSP files required to upgrade to Firmware Release 9.0 are incompatible with those used in previous releases and are also incompatible with those used to push updates to devices already running Firmware Release 9.0. Do not try to re-use the Release 8.6 or 8.7 RSP and INI files with the new software. You must use the appropriate RSP and INI files for the Release 9.0 packages.

Required preserve changes setting

In order for the hostname on the device to be retained after a reboot, you must enable the preserve changes option in the RSP file (`set-preserve-changes yes`) and in the INI file (`Update.Preserve_changes=yes`). If these parameters are not set correctly, your previous configurations will be lost after a reboot and the hostname on the thin client will revert to the device MAC address.

Editing INI and RSP files

Use only a plain text editor to edit INI and RSP files. Do not use word processing program such as Word or WordPad to edit these files, otherwise package deployment errors can occur.

INI caching

In the INI file, include the `INIFileSource=cache` parameter to ensure that devices use the local cached version of the INI file if they cannot access the INI file from Cisco VXC Manager. This is particularly important for devices running the Cisco AnyConnect VPN, so that they have a configuration to reference at bootup before connecting to the network over VPN.

Cisco AnyConnect deployments

For devices running the Cisco AnyConnect VPN, before you provide the devices to your remote employees, you must first push the required configuration to the devices on your local network first. Once you have upgraded the devices with the required parameters locally, you can then provide the preconfigured devices to remote users to operate behind the Cisco AnyConnect VPN.

Deploying add-ons

- When you deploy an add-on to the device, include the base image in the DDC package. This ensures that the devices that apply the add-on are also running the required base image version. For devices already running the required base image, they will install the add-on only.
- To check which specific add-ons and RPMs are installed on the thin client, see the Application Info tab for the device in Cisco VXC Manager (at the bottom of the details pane in Device Manager).

Package and file naming

- All Cisco VXC Manager package names, filenames (including .rsp and .ini), folders, and so on must be lower-case.
- Every time you push a new package, you must use a new name for the package. (You can copy the package, change the name, make the required changes, and then push the renamed package.) Do not make changes to an existing package and push it again with the same name; otherwise, the clients may not apply the latest changes. As a best practice, add the date to each package you create.
- 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).

Minimum checkin time

In the Device Manager preferences (Configuration Manager > Preferences > Device Manager), the minimum checkin time must be no less than 5 minutes, otherwise devices will experience issues. For large deployments, the default value of 1 hour is appropriate.

Scheduled Packages error

If you deploy a package from Cisco VXC Manager and an error message appears in the Schedule Packages, delete this error. Any errors associated with a specific thin client prevent future package deployments to the thin client until the errors are deleted.

Device discovery using static configuration rather than DHCP

DHCP is the Cisco-recommended method for device discovery with Cisco VXC Manager. As an alternative, you can specify the Cisco VXC Manager address on the thin client statically in the INI file using the MgmtDiscoveryMethod=STATIC parameter together with the RapportServer and the RapportSecurePort parameters. For more information, see *INI Files Reference Guide for Virtualization Experience Client 6215 Firmware Release 9.0*.

Execute command

In Device Manager, if you enter a command in the Execute Command dialog box (right-click the device and choose **Execute Command**), always add an ampersand to the end of the command (for example, `/etc/init.d/sshd start &`). Otherwise, the command can leave the thin client unusable, requiring a manual reboot.

Log History tab

In the Log history tab (at the bottom of the details pane in Device Manager), if you list the logs by date, the entries are not listed in chronological order, but rather in alphabetical order.

Client discovery using Cisco VXC Manager

Cisco VXC Manager is the standard tool for managing the Cisco VXC 6215. Cisco VXC Manager allows you to configure, upgrade, and administer your thin clients from a single interface. It also allows you to specify default configurations that are common to all of the thin clients in your environment. You can also use it to enable add-ons, which provide additional functionality in addition to the underlying firmware.

Cisco VXC Manager can discover the Cisco VXC 6215 devices in your network using either dynamic discovery or a manual process. After Cisco VXC Manager identifies the devices in the network, it stores information about them in the Cisco VXC Manager Database. You can then use Cisco VXC Manager to manage the devices.

For the Cisco VXC 6215, the recommended discovery method uses a DHCP server. In this case, you must configure DHCP Option Tags on your DHCP server to specify the IP address and port of the Cisco VXC Manager Web Server. The Cisco VXC Manager Agent (HAgent) on the Cisco VXC 6215 uses this information to communicate with the Cisco VXC Manager Web Server, performing check-ins at boot up and at regular intervals. The Hagent provides the Cisco VXC Manager with device information including device name, hardware information, network information, and image version.

For detailed configuration steps for DHCP discovery, see DHCP server configuration for device discovery, on page 5.

Caution For proper operation of the thin clients, you must also specify a value either for DHCP Option 15 (Domain Name) or for DHCP Option 6 (Domain Server) in the DHCP server configuration. If you do not specify a standard domain name for DHCP Option 15, and you do not specify a standard domain server for DHCP Option 6, you must at minimum specify "none" for DHCP Option 15. This configuration is necessary whether or not you are using DHCP to direct the thin clients to the central server.

For information about additional discovery methods with Cisco VXC Manager, see *Administration Guide for Cisco Virtualization Experience Client Manager*.

DHCP server configuration for device discovery

To allow Cisco VXC Manager to discover the Cisco VXC 6215 devices, configure the following option tag values on your DHCP server:

- Option tag 186—IP address of your Cisco VXC Manager server (for example, 192.168.1.10). The value should be in 4-byte IP address format.

- Option tag 194—As an alternative to option tag 186, you can use option tag 194 to specify the FQDN of the Cisco VXC Manager server.
- Option tag 190—Secure port number to which Cisco VXC Manager server listens (for example, port 443). The value should be in word format (value = 0x01bb) or 2-byte array format (value = 0x01 0xbb).
- Option tag 192—Non-secure port number to which Cisco VXC Manager server listens (for example, 80). The value should be in either word format (value = 0x0050), or 2-byte array format (value= 0x00 0x50).

Tip Do not run the Cisco VXC Manager server and the DHCP server on the same machine.

To configure the Cisco VXC Manager server IP address and port option values on a Windows DHCP server:

Procedure

Step 1 Open the DHCP management wizard, choose the DHCP server to be configured, right-click the server name, and choose **Set Predefined Options** to open the Select Predefined Options and Values window.

Figure 1: DHCP Window

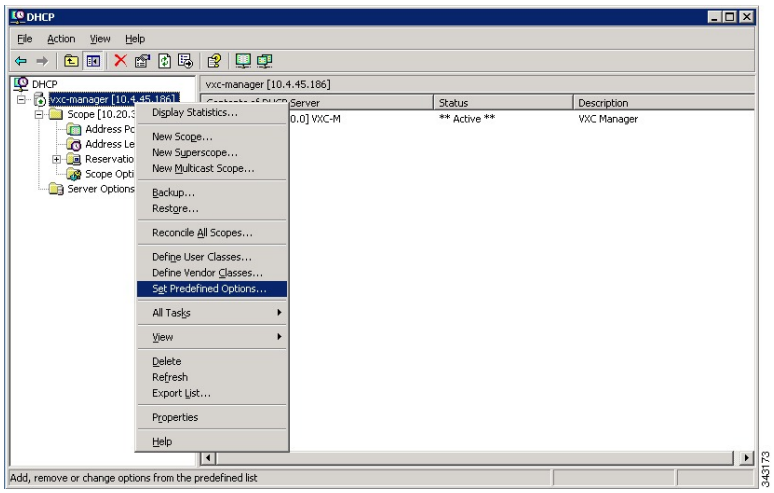
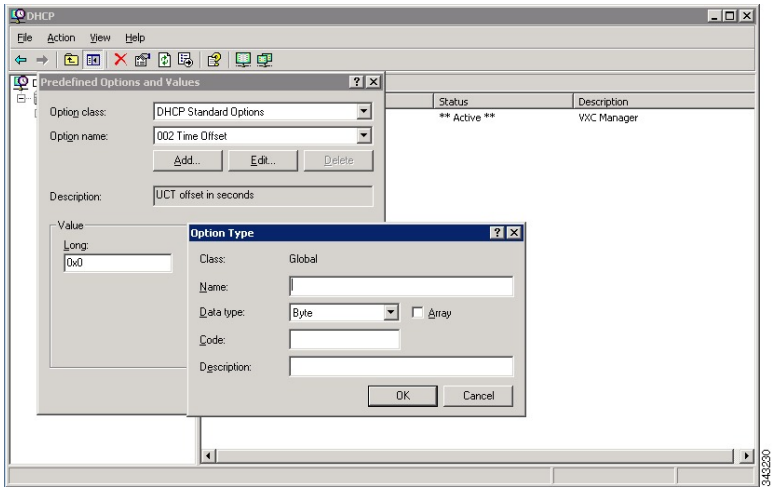


Figure 2: Select Predefined Options and Values



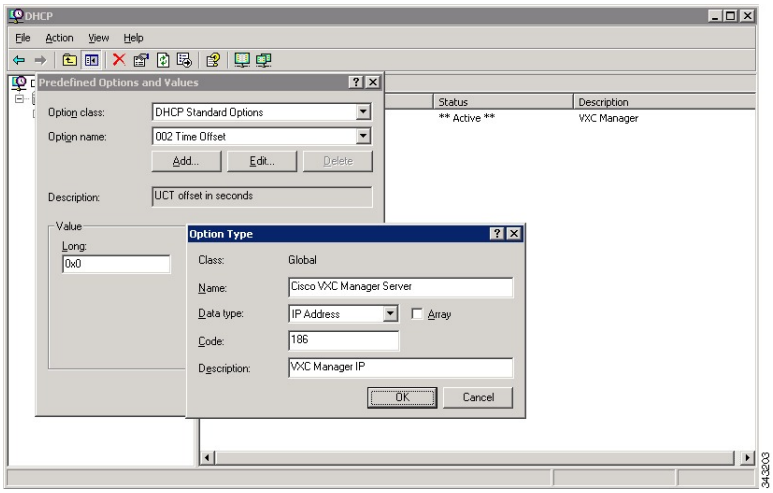
Step 2 On the Predefined Options and Values screen, click the **Add** button. The **Option Type** window appears.

Step 3 In the Option Type window, enter the required information:

- Name—Cisco VXC Manager Server
- Data Type—IP Address
- Code—186

- Description (optional)—Enter desired information

Figure 3: Option Type: Server IP



Step 4 Click **OK**.

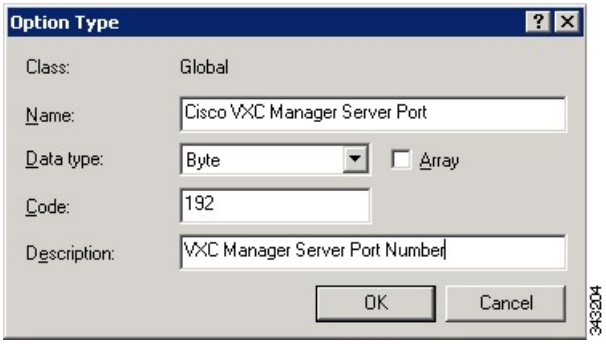
Step 5 Repeat Steps 2 and 3 for the Cisco VXC Manager Server Secure port, with these changes:

- Name—Cisco VXC Manager Server Secure Port
- Data Type—Word
- Code—190

Step 6 Repeat Steps 2 and 3 for the Cisco VXC Manager Server port, with these changes:

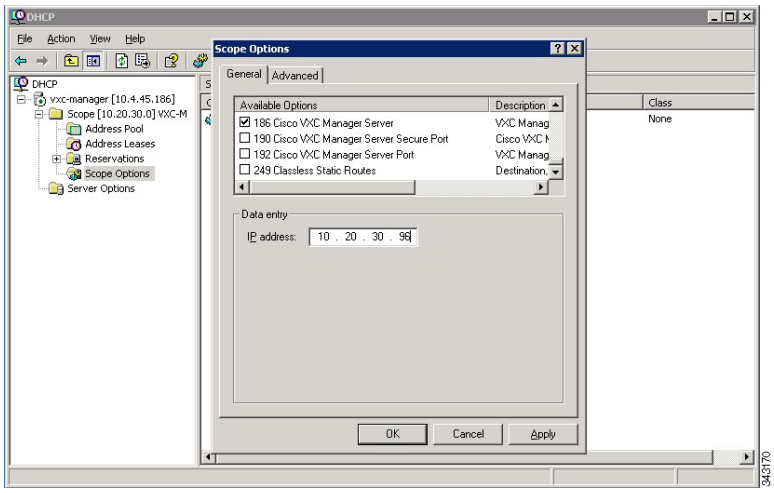
- Name—Cisco VXC Manager Server Port
- Data Type—Byte or Word
- Code—192

Figure 4: Option Type: Cisco VXC Manager Server Port



Step 7 Click **OK**.

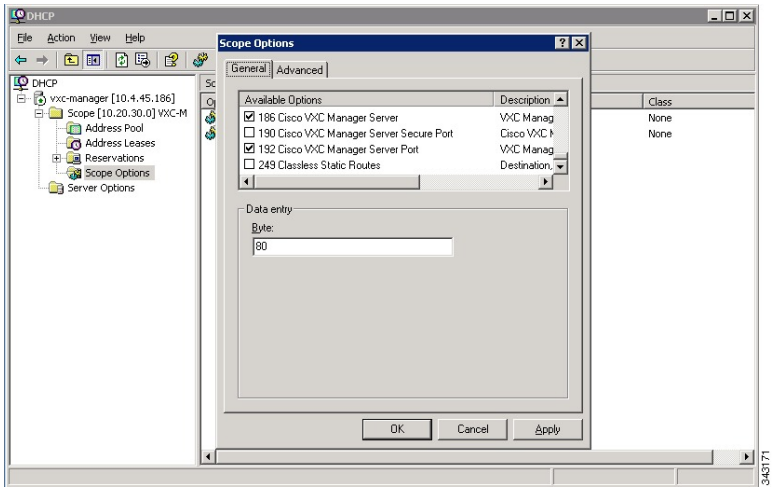
Figure 5: DHCP Scope Options: Cisco VXC Manager Server



Step 8 From the DHCP management wizard, right-click **Scope Options** (from the target DHCP Server Scope, as shown in Step 7) and choose **Configure Options**.

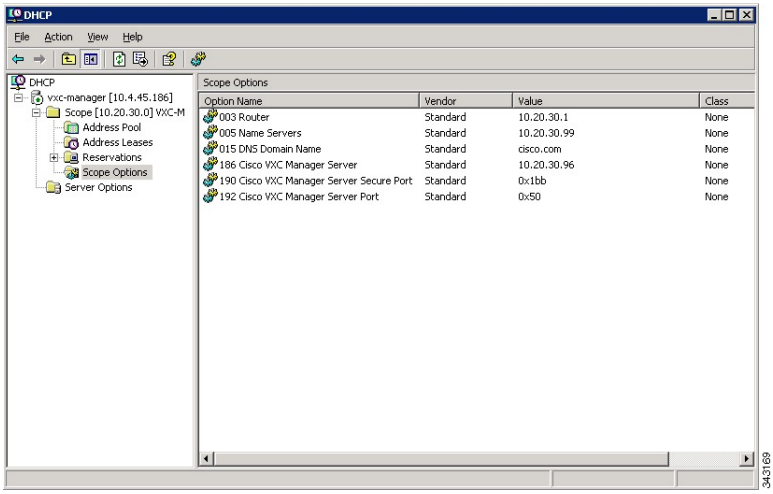
- In the list of Available Options, check option number 186, and enter the IP address of the Cisco VXC Manager server.
- In the list of Available Options, check option number 190, and enter the port number at which your Cisco VXC Manager server listens for secure communication.
- In the list of Available Options, check option number 192, and enter the port number at which your Cisco VXC Manager server listens (Port 80 is shown below).

Figure 6: DHCP Scope Options: Cisco VXC Manager Server Port



Step 9 Click **OK**.

Figure 7: DHCP Scope Options List



Step 10 Confirm that options 186, 190 and 192 are listed with proper values under the target DHCP server and scope.

INI files

INI files are plain-text files that you can use to centrally manage and configure your thin clients on a global level. For example, you can use INI files to configure and save information about connection settings, display options, and printer options. The INI files are maintained on the central Cisco VXC Manager server, and the thin client accesses the INI files from the server during the initialization process (using HTTP, or HTTPS).

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 is used for device-specific configuration. It is stored in the same directory as the wlx.ini file. If the thin client locates this INI file on the server, the thin client uses the $MAC.ini file for its configuration rather than the wlx.ini file. In this case, the thin client does not access the wlx.ini file unless you specify the include=wlx.ini parameter in the $MAC.ini file.

Create a wlx.ini file for client configuration

The most commonly used INI file, wlx.ini, contains the global parameters you want to apply to all thin clients in your environment. (Cisco VXC Manager also allows you to specify a subset of thin clients to which a particular wlx.ini configuration applies.)

The Cisco VXC 6215 supports a number of INI configuration parameters. See INI file examples, on page 11 for some useful examples, including configurations required to create XenDesktop, VMware View, and

RDP connections. For a complete list of supported INI parameters, see *INI Files Reference Guide for Cisco Virtualization Experience Client 6215* .

Caution By default, administrator and root user credentials are specified on the thin client. The Cisco VXC 6215 does not support the operation of the device using these credentials (the only supported mode of operation is using the thinuser credentials). However, Cisco strongly recommends that you change the passwords for these users to prevent unauthorized access to the client, using the following INI parameters.

Username	Default password	INI parameter used to change password
admin	admin	ChangeAdminPassword
root	admin	ChangeRootPassword

To create the wlx.ini file, perform the following procedure.

Procedure

Step 1 Open a text file.

Step 2 Enter the INI parameters required in accordance with INI file examples, on page 11 or *Cisco Virtualization Experience Client 6215 INI Files Reference Guide*.

Step 3 Save the file as wlx.ini.

Step 4 After you create the wlx.ini file, you must create a Cisco VXC Manager package to push the wlx.ini configuration to your clients. See Create a Cisco VXC Manager package for the wlx.ini file, on page 14.

INI file examples

This section contains sample INI files. For detailed information about INI parameters and definitions, see the *INI Files Reference Guide for Cisco Virtualization Experience Client 6215*.

Mandatory INI parameters

To push updates to Release 9.0 devices, you must include the following mandatory parameter in the INI file:

```
IniFileSource=cache
```

Note To perform upgrades to Release 9.0 from a previous release, you must use different INI and RSP files than those used to push updates to Release 9.0 devices. For information about how to upgrade to Release 9.0 from a previous release, see Upgrading to Firmware Release 9.0.

Static IP INI parameters for Cisco VXC Manager

If you are deploying using static Cisco VXC Manager IP configuration, also include the following:

```
MgmtDiscoveryMethod=STATIC
RapportServer=xxx.xxx.xxx.xxx
RapportSecurePort=443
```

In the above, replace xxx.xxx.xxx.xxx and 443 with your Cisco VXC Manager IP address and secure port number.

Firefox browser configuration example

The following is a simple INI file that you can use to test the Cisco VXC Manager client update process. After the package process is successful using this file, the client will load the INI file, and launch the Firefox browser with cisco.com as the home page.

Example:

```
CONNECT=BROWSER \
Description="Cisco Home Page" \
URL=http://www.cisco.com \
Resolution=FullScreen \
Mode=Normal \
autoconnect=yes
```

XenDesktop INI configuration example

To create XenDesktop server connections, use the Mozilla Firefox Connect options to specify the URL of the XenDesktop server to which users must connect. When the server URL is specified in the INI configuration, Firefox opens to this URL and the user can enter their credentials to initiate the connection to the HVD.

Example:

```
CONNECT=BROWSER \
Description="Windows Desktop" \
URL=http://xd.company.com \
Reconnect=yes \
ReconnectSeconds=5 \
AutoConnect=yes \
mode=kiosk
```

Caution In the above example, replace xd.company.com with the URL of your XenDesktop server.

With the optional Autoconnect=yes parameter specified in the preceding example, the browser connects to the specified URL when the client boots up. In addition, the optional Reconnect=yes and ReconnectSeconds=5 parameters specify to reconnect a disconnected connection after 5 seconds. Finally, the optional mode=kiosk parameter specifies to operate in kiosk mode, in which Firefox operates in full-screen mode with no access to the address bar.

XenApp INI configuration example

The following is an example configuration for a Citrix XenApp connection.

Note The Cisco VXC 6215 supports the ICA Connect Options only with XenApp connections. The ICA Connect Options are not supported with XenDesktop connections.

Example:

```
CONNECT=ICA \
BrowserIP=192.168.0.3 \
Application="Desktop" \
Description="ICA_Desktop " \
AutoConnect=yes \
Reconnect=yes \
Encryption=128 \
Colors=16m \
Fullscreen=no \
Resolution=800x600 \
Username=$UN \
Password=$PW \
Domainname=$DN \
Alternate=yes \
LowBand=yes
```

Caution In the above example, replace 192.168.0.3 with the IP address of the ICA browser.

VMware View INI configuration example

The following is an example configuration for a VMware View connection.

Example:

```
CONNECT=VMWARE_VIEWCLIENT \
Description="VMview" \
Host=192.168.0.2 \
DomainName=$DN \
Username=Administrator \
Password=Password \
DesktopSize=800x600 \
Ping=yes \
UseSSL=yes
```

Caution In the above example, replace 192.168.0.2 with the IP address of your VMware View server.

RDP INI configuration example

The following is an example configuration for an RDP connection.

Example:

```
CONNECT=RDP \
Host=x.x.x.x \
Description="RDP_Server" \
AutoConnect=yes \
Colors=16m \
Username=Administrator \
Password=Password \
Domainname=$DN \
Resolution=800x600 \
Reconnect=no \
```

```
Drives=J=disk \
Drives=k=floppy \
Sound=off
```

Caution In the above example, replace x.x.x.x with the IP address of your RDP server.

Enable VNC configuration example

The following is an example configuration to enable VNC.

Example:

```
DisableVnc=no
VNCAuthTypes=none
VNCPrompt=no
```

Time settings configuration example

The following is an example configuration for time settings.

Example:

```
Timeserver=yourntpserver.com
Timeformat="24-hour format"
TimeZone="US/Eastern"
ManualOverride=1
```

Display and keyboard settings configuration example

The following is an example configuration for display and keyboard settings.

Example:

```
DisplaySettings=MON1 rotate-normal 1440x900
DesktopTaskBar=left
AutoHide=yes
Keyboard.layouts=us
```

Create a Cisco VXC Manager package for the wlx.ini file

To push a wlx.ini file to your clients, you must create a Cisco VXC Manager package, which you can then schedule for distribution to your devices.

Required folder structure with Cisco VXC Manager

Note With Firmware Release 9.0, all Cisco VXC Manager package names, filenames (including .rsp and .ini files), folders, and so on must be lower-case.

With Cisco VXC Manager, you must create and register specific packages to push upgrades and configurations to your clients.

To register the package with Cisco VXC Manager, you must create a unique RSP file and, in the same directory, a matching folder of the same name. This matching folder serves as the root directory for the remaining configuration files in the package.

For example, assuming <packagename>.rsp is the RSP file, the folder structure required to register the package is as follows:

Table 1: Package Folder Structure

Directory	Description
~\<packagename>.rsp	The unique RSP file, located in the same directory as the matching root package directory.
~\<packagename>\	The root package 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
~\<packagename>\wlx	The main INI configuration folder. It stores the following: • wlx.ini file and $MAC.ini file • bitmap folder • certs folder
~\<packagename>\wlx\bitmap	The folder where you can place custom images you plan to use.
~\<packagename>\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.
~\<packagename>\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.

You can create this structure in any location on your Cisco VXC Manager server, as long as all required files are in the appropriate folders.

Note If a folder does not contain a required file for the package, the folder can be omitted from the package directory structure. For example, if the package contains no graphics, the \wlx\bitmap folder is not required.

After you register the package, Cisco VXC Manager stores the package files in the software repository under c:\inetpub\ftproot\Rapport\<packagename>.

Caution Do not attempt to modify a registered package located in the Rapport folder. To modify a package, you must create and register a new package that includes the required changes.

Use the following procedure to create a Cisco VXC Manager package containing the wlx.ini file for Cisco VXC 6215 client configuration.

Procedure

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

Step 2 In the 6215-configs folder, create an RSP file, for example 6215-9.0-datetime-template.rsp, with the following content (to create the RSP file, enter the required content in a text editor, and then save the file with a .rsp extension):

Note This RSP script is provided as an example; you may need to reconfigure the parameters depending on your environment. See the *Administration Guide for Cisco Virtualization Experience Client Manager* for details about configuring RSP files.

```
[Version]
Number=6215-9.0-datetime-template.rsp
Description=6215 update
OS=SLX
Category=Cisco
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 "/usr/sbin/thinclient-config --set-preserve-changes yes"
EX "sync"
EX "(test -e /usr/sbin/imageupgrade && imageupgrade; exit 0)"
EX "(! test -e /usr/sbin/imageupgrade && (sleep 10; /sbin/reboot)&)"
```

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

Caution This example RSP script is applicable only for devices already running Firmware Release 9.0. For detailed information to upgrade devices running Release 8.6 or 8.7 to Release 9.0, including the required RSP script, see Upgrading to Firmware Release 9.0.

Step 3 Create a matching folder to contain the remaining package files, in this example, 6215-9.0-datetime-template.

Step 4 In the 6215-9.0-datetime-template folder, add the required package files to create the following folder structure:

`C:\6215-configs\6215-9.0-datetime-template.rsp`

`C:\6215-configs\6215-9.0-datetime-template\latest-image.raw`

`C:\6215-configs\6215-9.0-datetime-template\latest-image.raw.info`

`C:\6215-configs\6215-9.0-datetime-template\wlx\wlx.ini`

Note See the end of this procedure for the mandatory INI parameters with Firmware Release 9.0 device updates.

Step 5 To install an add-on, include the addons subfolder under the 6215-9.0-datetime-template folder, and copy the RPM and directory file to this folder:

`C:\6215-configs\6215-9.0-datetime-template\addons\add-on-name.rpm`

```
C:\6215-configs\6215-9.0-datetime-template\addons\directory
```

Note To install add-ons on devices running Firmware Release 9.0, you do not need to include the InstallAddons parameter in the wlx.ini file.

Step 6 Register the package:

a) In the tree pane of the Administrator Console, expand **Package Manager**.
b) In the details pane, right-click **Other Packages** and choose **New** > **Package**.
c) Choose **Register a Package from a Script file (.RSP)** and click **Next**.
d) Click **Browse** and choose the RSP file you want to register and click **Open**.
e) Click **Next** to display the Package Wizard summary.
f) Click **Next** to see the Package Registration Progress screen.
g) Click **Next** to create the package.
h) After the package is created and registered, click **Finish**.

Step 7 To upgrade the Cisco VXC 6215, use the Default Device Configuration (DDC) method (see Schedule device updates using Default Device Configuration, on page 17).

Mandatory INI parameters

To push updates to Release 9.0 devices, you must include the following mandatory parameter in the INI file:

```
IniFileSource=cache
```

Static IP INI parameters for Cisco VXC Manager

If you are deploying using static Cisco VXC Manager IP configuration, also include the following:

```
MgmtDiscoveryMethod=STATIC
RapportServer=xxx.xxx.xxx.xxx
RapportSecurePort=443
```

In the above, replace xxx.xxx.xxx.xxx and 443 with your Cisco VXC Manager IP address and secure port number.

InstallAddon parameter not required

Unlike previous releases, to install add-ons on devices running Firmware Release 9.0, you do not need to include the InstallAddons parameter in the wlx.ini file. The thin client successfully installs the add-on as long as the `/addons` folder for the package contains the required add-on files and the accompanying directory file.

Schedule device updates using Default Device Configuration

To update a group of Cisco VXC 6215 devices, you can assign a Default Device Configuration (DDC). A DDC allows you to set default configurations for a group of devices and ensures that the devices conform to your configurations. That is, if there is any deviation from your default configurations, Cisco VXC Manager reverts the devices to your specified configurations automatically (Cisco VXC Manager automatically sends the Cisco VXC Manager packages in the DDC to the devices according to your schedule and without your intervention).

See the following sections to configure a DDC:

- Configure Default Device Configuration preferences, on page 18
- First-time Default Device Configuration, on page 18

• Existing Default Device Configuration, on page 19

Configure Default Device Configuration preferences

Before you create a Default Device Configuration, ensure to configure the DDC preferences as follows:

Procedure

Step 1 In the tree pane of the Administrator Console, choose **Configuration Manager** > **Preferences**.
Step 2 In the details pane, click **Device Manager Preferences**.
Step 3 In the tree pane of the Preferences dialog box, click **DDC**.
Step 4 Under Default Device Configuration, check the **Enable Default Device Configuration** box.
Step 5 Under Time to Schedule DDC Reconciliation, click **Upon Checkin**.
Step 6 In the tree pane of the Preferences dialog box, click **Scheduling**.
Step 7 Under Imaging Option, click **Merlin**.
Step 8 Click **OK**.

First-time Default Device Configuration

Perform this procedure each time you create a new image package that you want to specify as the default image for client upgrades.

Procedure

Step 1 Determine whether a Default Device Configuration already exists:
a) In the tree pane of the Administrator Console, expand **Configuration Manager** and click **Default Device Configuration**.

b) If a default configuration appears in the details pane, go to Existing Default Device Configuration, on page 19. Otherwise, go to the next step.

Step 2 In the tree pane of the Administrator Console, expand **Configuration Manager**, right-click **Default Device Configuration**, and choose **New** > **Default Device Configuration** to open the Default Device Configuration Wizard.

Step 3 In the Operating System field, choose **SUSE Linux**.

Step 4 In the Media Size field, choose **4000 MB**.

Step 5 In the Qualifying OS Image field, choose **No Image**.

Step 6 In the Software Packages tab, check the required package for the upgrade to and click **Add** to add it to the Selected column. (The packages listed in this tab match the packages that you have registered in the Cisco VXC Manager.)

Step 7 Click **Next** and under Execute DDC, choose **Whenever a device checks in**.

Step 8 Click **Next** and click **Finish**.

Step 9 After a DDC has been configured for the Cisco VXC 6215, the clients are updated to the selected package configuration automatically: either at their regularly scheduled checkin time or according to the update time set in the Device Manager DDC preferences in Configuration Manager. You can also right-click the Cisco VXC 6215 you want to upgrade, and choose **Reboot** to perform a manual upgrade.

Step 10 After the devices are upgraded, click the top **Refresh** icon in Device Manager to see the changed software revision.

To verify that Cisco VXC Manager has successfully pushed a package to a device, click **Device Manager**, and choose a target device. In the bottom right hand corner, of the details pane, click the plus icon (+) to maximize the properties for the device, then click the **Deployed Package** tab to show all packages that are on the device.

Existing Default Device Configuration

Perform this procedure when you want to specify an existing image package as the default image for client upgrades.

Procedure

Step 1 In the tree pane of the Administrator Console, expand **Configuration Manager**, and click **Default Device Configuration**.

Step 2 Right click **SUSE Linux**, and choose **Properties**.

Step 3 In the Software Packages field, choose the package to upgrade to.

Step 4 Click **Finish**.

After a DDC has been configured for the Cisco VXC 6215, the clients are updated to the selected package configuration automatically: either at their regularly scheduled checkin time or according to the update time set in the Device Manager DDC preferences in Configuration Manager. You can also right-click the Cisco VXC 6215 you want to upgrade, and choose **Reboot** to perform a manual upgrade.

Cisco VXC 6215 deployment with a Cisco Virtual Office Router

For proper operation of the Cisco VXC 6215 behind a Cisco Virtual Office Router, you must configure the thin client with the Cisco VXC Manager IP address. To do so, you can first push the Cisco VXC Manager IP address to the thin client using INI settings on your local network, and then provide the pre-configured thin client to the remote user. Alternatively, the remote user can manually enter the Cisco VXC Manager server IP address using the following procedure.

Note This procedure is required only for the initial connection to the network from behind a Cisco Virtual Office router. The procedure assumes a factory new Cisco VXC 6215. Subsequent connections do not require these steps. The procedure also assumes that you have set up the thin client environment, including the configuration of connection parameters (Connect options) in the INI file to allow connection to a virtualization server.

Procedure

Step 1 Connect the Cisco VXC 6215 to the Cisco Virtual Office router.

Step 2 Power up the Cisco VXC 6215.

Step 3 From the desktop, click **Computer** > **More Applications** > **Firefox** to launch the Firefox web browser.

Step 4 If the Cisco Virtual Office router prompts you for a username and password, enter the required credentials. Otherwise, if Firefox opens directly to the home page, proceed to the next step.

Step 5 Click **Computer** > **More Applications** > **VXC-M**.

Step 6 In the VXC-M Server field, enter the IP address of the Cisco VXC Manager.

Step 7 In the Non-secure Port (HTTP) field, enter **80** (or a custom port for your Cisco VXC Manager setup, as required).

Step 8 In the Secure Port (HTTPS) field, enter **443** (or a custom port for your Cisco VXC Manager setup, as required).

Step 9 Click **OK**, and reboot the thin client.
At startup, the device appears in the Cisco VXC Manager as a new device with a green status, and the administrator can configure it.

After the reboot the thin client downloads the wlx.ini file (the download can last a few minutes).

Step 10 After the download is complete, a shortcut icon appears on the desktop providing a connection to the hosted desktop. Double-click the icon to connect to the hosted desktop.

Note If required, the administrator can push a firmware upgrade to the thin client.

Monitor resolution

For most monitors, the thin client automatically obtains the correct resolution to display from the monitor itself.

For monitors that do not fully support the VESA standards (generally older models), the thin client may not be able to display the monitor resolution correctly, resulting in a black screen. The workaround for this issue is to push an INI file containing the correct display settings to the thin client using Cisco VXC Manager.

The following is an example configuration using the DisplaySettings INI parameter to specify the resolution for monitor 1 to be 1024 x 768, with no rotation:

```
DisplaySettings=MON1 rotate-normal 1024x768
```

For more information about configuring this INI parameter, see *INI Files Reference Guide for Cisco Virtualization Experience Client 6215*.

SSH connections

The Cisco VXC 6215 can support remote connections to the thin client using SSH, however this functionality is disabled by default to provide increased security.

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, enter:

```
/etc/init.d/sshd start &
```

The default OpenSSH idle timeout is 30 minutes and the maximum timeout is 60 minutes. (These default SSH idle timeout values cannot be modified.)