Installation Guide for
Cisco Virtualization Experience Client
Manager 4.8.5

October 10, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
## CONTENTS

### Preface
- About this Guide
- Organization
- Related Documentation
- Obtaining Documentation, Obtaining Support, and Security Guidelines
- Document Conventions

### Chapter 1

**Preparing For Installation**

- Preinstallation Checklist
- Hardware Requirements
- Software Requirements
- Communication Ports
- Installing and Configuring FTP
  - Installing and Configuring FTP on Windows XP Professional or Windows Server 2003
  - Configuring the FTP Service for Anonymous Connections Only
  - Installing and Configuring FTP on Windows Server 2008
  - Installing FTP on Windows Server 2008
  - Configuring FTP on Windows Server 2008
  - Configuring the FTP User Isolation Mode
  - Verifying FTP on Windows Server 2008
  - Installing and Configuring FTP on Windows Server 2008 R2
  - Installing FTP on Windows Server 2008 R2
  - Configuring FTP on Windows Server 2008 R2
  - Configuring the FTP User Isolation Mode
  - Verifying FTP on Windows Server 2008 R2
  - Installing and Configuring FTP on Windows 7
  - Installing FTP on Windows 7
  - Configuring FTP on Windows 7
  - Configuring the FTP User Isolation Mode
  - Verifying FTP on Windows 7
- Installing and Configuring IIS
  - Installing and Configuring IIS 6.0 on Windows XP Professional or Windows Server 2003
  - Installing and Configuring WebDAV on Windows XP Professional or Windows Server 2003
Contents

Configuring WebDAV on Windows XP Professional or Windows Server 2003 to Allow Only Anonymous Connections 1-24
Installing IIS 7.0 on Windows Server 2008 1-26
Installing WebDAV Extension for IIS 7.0 1-28
Configuring the Web.config File 1-28
Installing IIS 7.5 on Windows Server 2008 R2 1-29
Installing IIS 7.5 on Windows 7 1-32
Creating a DNS Service Location (SRV) Resource Record for Cisco VXC 2111/2211 ThreadX Devices 1-34

Chapter 2

Installing or Upgrading Cisco VXC Manager 2-1
Installing or Upgrading Procedures (Cisco VXC Manager) 2-2
Detailed Custom Installation and Upgrade Instructions 2-3
Cisco VXC Manager Database Installation Tips You Need to Know 2-4
Software Repository Installation Tips 2-7
Installing Multiple Administrator Consoles 2-9
Backing up the Cisco VXC Manager Database 2-10
External SQL Integration 2-10

Appendix A

Using HTTPS as the Communication Protocol for Cisco VXC Manager A-1
Configuring HTTP and HTTPS for IIS A-1
Creating a Root Authority Certificate A-1
Creating the Cisco VXC Manager Certificate A-4
Exporting the Certificates to Local Files A-7
Configuring Clients to Securely Check In Using Port 443 A-7
Cisco VXC 6215 A-7
Cisco VXC 2112/2212 A-8
Adding an HTTPS Site Binding in IIS A-9
Configuring Secure Package Downloads A-9

Appendix B

Uninstalling Cisco VXC Manager B-1
Preface

Cisco Virtualization Experience Client (VXC) Manager software is the premier enterprise solution for managing network intelligent devices simply, remotely, and securely. It enables IT professionals to easily organize, upgrade, control, and support thousands of Cisco VXC devices including Cisco VXC 6000 Series devices and Cisco VXC 2000 Series devices.

Note


Cisco VXC Manager software uses industry-standard communication protocols and a component-based architecture to efficiently manage your network devices. Its intuitive, simple, and powerful user interface is built to operate as a standard snap-in to the Microsoft Management Console (MMC). From one simple-to-use console, Cisco VXC Manager allows you to manage all of your network devices easily and quickly.

About this Guide

This guide provides the step-by-step instructions you need to install and configure a Cisco VXC Manager environment. It also includes the requirements you must address before you begin the installation procedures.

This guide is intended for experienced network administrators and Information Technology professionals who have installed and configured Windows operating systems and applications.

Organization

This manual is organized as described in the following table.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>Describes the manual.</td>
</tr>
<tr>
<td>Chapter 1, “Preparing For Installation”</td>
<td>Describes the preparation steps required prior to installation.</td>
</tr>
<tr>
<td>Chapter 2, “Installing or Upgrading Cisco VXC Manager”</td>
<td>Describes how to install or upgrade Cisco VXC Manager.</td>
</tr>
</tbody>
</table>
Related Documentation

For more information, see the documents available at the following URLs:

**Cisco Virtualization Experience Client 2000 Series**

**Cisco Virtualization Experience Client 6000 Series**

**Cisco Virtualization Experience Client Manager**

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What’s New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Subscribe to the What’s New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Document Conventions

This document uses the following conventions:

**Note**
Means reader take note. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution**
Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.
Warnings use the following convention:

⚠️ IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS
Preparing For Installation

This chapter contains the preinstallation requirements you must complete to prepare the environment for Cisco VXC Manager installation and configuration. After you complete all preinstallation requirements, you can continue with the installation/upgrade in Chapter 2, “Installing or Upgrading Cisco VXC Manager”.

Preinstallation Checklist

Before you begin installing Cisco VXC Manager, make sure you have met the requirements on this checklist:

- Obtain and configure all hardware and software, as necessary (see Hardware Requirements, page 1-3 and Software Requirements, page 1-3).

Caution

It is highly recommended that you do not install Cisco VXC Manager on any server that is currently dedicated to other tasks (such as a Domain Controller, Backup Controller, Mail Server, Production Web Server, DHCP Server, MSMQ Server, Application Server, and so on). It is highly recommended that Cisco VXC Manager be installed on a server that is dedicated to Cisco VXC Manager services.

- Install a supported operating system on the machine to which Cisco VXC Manager will be installed. Be sure that all systems are up-to-date with current Microsoft service packs, patches, and updates (see Software Requirements, page 1-3).
- Install Microsoft Internet Explorer (IE) 6.0 or later on all machines.
- Use of the built-in HTML help files requires Java to be installed on all machines to which you install the Cisco VXC Manager Administrators Console (MMC Snap-in). Visit http://www.java.com and install the latest Java/JRE version for your operating system.
- Ensure that Internet Information Services (IIS) version 6.0, 7.0, or 7.5 is installed (depending on your operating system) and properly configured on the machine to which Cisco VXC Manager will be installed (see Installing and Configuring IIS, page 1-20).
- If you will be installing IIS 7.5 on Windows Server 2008 R2, you must run the ConfigureIISRoles.bat and UninstallIISRoles.bat batch files (located at Disk1\swrep) before you install IIS.
- If you will be running IIS 7.0 on Windows Server 2008 SP1 or IIS 7.5 on either Windows Server 2008 R2 or Windows 7, be sure to update the HAagent on your devices as follows to ensure your devices are discovered by Cisco VXC Manager (otherwise, IIS limitations may prevent discovery):
  - Devices running CE .NET require HAagent v4.7.12.1 or later
Preinstallation Checklist

- Devices running Linux v7 require HAgent v4.2.0.0 or later
- Devices running WES require HAgent v5.1.1.10 or later
- Devices running WTOS require HAgent v4.0.4.2 or later
- Devices running XPe require HAgent v5.1.1.10 or later

- Ensure that no other applications requiring IIS are running on the machine to which Cisco VXC Manager will be installed.
- Ensure that all required communications ports are available and open for proper communication between servers, routers, and switches (see Communication Ports, page 1-3).
- Cisco VXC Manager requires Microsoft Data Access Components (MDAC) version 2.8. Cisco VXC Manager installs MDAC 2.8 if it is not already present on the server.
- Ensure you have access to your operating system CD-ROM and your Microsoft Windows system files for use during your installation.

Tip

During Cisco VXC Manager installation Cisco VXC Manager checks the system to determine whether all required software is present. If required software is not present, Cisco VXC Manager indicates which software is missing. Some required third-party software is included with the Cisco VXC Manager software, while other software is available from your operating system CD-ROM or from the network location for your Microsoft Windows system files (usually the i386 folder).

- Cisco VXC Manager requires a supported SQL Server as described in Software Requirements, page 1-3. Cisco VXC Manager provides (and installs) Microsoft SQL Server 2005 Express as the default option, however, you can choose to use another supported SQL Server. To use another supported SQL Server, you must perform a Custom installation (see Chapter 2, “Installing or Upgrading Cisco VXC Manager”).
- If you plan to install and configure Cisco VXC Manager components on multiple machines (Custom installation), you will repeat some of the installation and configuration procedures in this guide. Likewise, you must also complete the preinstallation requirements for each related machine you intend to use.
- If you plan to use FTP, ensure you have FTP services installed, properly configured, and running (see Installing and Configuring FTP, page 1-5).

Caution

If you intend to use the firmware upgrade feature for ThreadX devices, configure FTP.

- If you plan to use HTTP or HTTPS for your server communications, you must install WebDAV for Microsoft Windows on IIS (see Installing and Configuring WebDAV on Windows XP Professional or Windows Server 2003, page 1-22 and Installing WebDAV Extension for IIS 7.0, page 1-28) and use the HTTP or HTTPS ports (as described in Communication Ports, page 1-3). Note that if the server to which you will install Cisco VXC Manager is running Windows XP Professional with SP3 or later, WebDAV is already installed and configured by default (you do not need to install and configure WebDAV again).
- If you plan to use ThreadX devices, you must create and configure a DNS Service Location (SRV) resource record as described in Creating a DNS Service Location (SRV) Resource Record for Cisco VXC 2111/2211 ThreadX Devices, page 1-34.
Hardware Requirements

The machine on which you will install Cisco VXC Manager must meet or exceed the minimum system requirements shown in Table 1-1 (because these are general guidelines, be sure to refer to your operating system documentation for details on hardware requirements).

<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum Requirements</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1GHz Intel or AMD X86</td>
<td>2.4 GHz Dual Core Intel or AMD X86</td>
</tr>
<tr>
<td>RAM</td>
<td>512 MB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Minimum Free Space</td>
<td>500 MB</td>
<td>720 MB</td>
</tr>
</tbody>
</table>

The actual free space required depends on the number and size of the packages you register, as well as the number of devices you will be managing (the Cisco VXC Manager Database size). This minimum space assumes the Cisco VXC Manager Database and packages require 500 MB.

Software Requirements

Cisco VXC Manager 4.8.5 supports the software shown in Table 1-2. Installing the latest version of each software package is highly recommended.

<table>
<thead>
<tr>
<th>Component</th>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Server</td>
<td>Microsoft SQL Server 2005, 2005 Express, 2008, or 2008 Express</td>
</tr>
</tbody>
</table>

By default, Cisco VXC Manager installs Microsoft SQL Server 2005 Express. To use an SQL Server Personal Edition, SQL Server Developer Edition, or another supported SQL Server, you must perform a custom installation (see Chapter 2, “Installing or Upgrading Cisco VXC Manager”).

If you choose to install a version of SQL Express, Cisco recommends that you also install a management tool such as SQL Management Studio to perform advanced configuration and administration tasks. These tasks are not commonly required, but may be required in some circumstances.

Communication Ports

To perform their full range of management functions, Cisco VXC Manager software components require certain ports to remain open on your servers, routers, and switches.

For example, Cisco VXC Manager relies on the HTTP/HTTPS communications port designated by your web service (such as Microsoft Internet Information Service) for push operations (push refers to operations initiated by Cisco VXC Manager and sent/pushed to devices). Push operations include:
• Issuing quick device commands (such as Refresh Device Information, Reboot, Change Device or Network Information, Get Device Configuration, and so on)
• Distributing packages at a specific time (either immediately or at a specific date and time)

Typically, port 80 is designated as the HTTP port and port 443 is designated as the HTTPS port. However, if port 80 (or the designated HTTP port), or port 443 (or the designated HTTPS port) is closed, Cisco VXC Manager will be unable to push updates or quick commands to devices.

Table 1-3 lists the ports Cisco VXC Manager uses and describes the respective communication protocols and their function (ensure that these ports are open for proper communication between servers).

<table>
<thead>
<tr>
<th>Cisco VXC Manager Component</th>
<th>Protocol</th>
<th>Port</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUI</td>
<td>HTTP</td>
<td>80</td>
<td>Communicate with the Web Service and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>21</td>
<td>Register new packages into the Master Software Repository.</td>
</tr>
<tr>
<td>OLE DB</td>
<td>1433 (default)</td>
<td>Can be configured during installation</td>
<td>Communicate with the Cisco VXC Manager Database.</td>
</tr>
<tr>
<td>VNC</td>
<td></td>
<td>5500</td>
<td>Remote shadows devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5800</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5900</td>
<td></td>
</tr>
<tr>
<td>Web Service</td>
<td>HTTP</td>
<td>80</td>
<td>Communicate with the Web Agent, GUI, and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>HTTPS</td>
<td></td>
<td>443</td>
<td>Secure Communication with the Web Agent, GUI, and Standard Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8443</td>
<td></td>
</tr>
<tr>
<td>OLE DB</td>
<td>1433 (default)</td>
<td>Can be configured during installation</td>
<td>Communicate with the Cisco VXC Manager Database.</td>
</tr>
<tr>
<td>Web Agent</td>
<td>HTTP</td>
<td>80</td>
<td>Communicate with the Web Service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>280</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>21</td>
<td>Read and write files to the Master and Remote Software Repositories.</td>
</tr>
<tr>
<td>Standard Service</td>
<td>OLE DB</td>
<td>1433 (default)</td>
<td>Can be configured during installation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>8008</td>
<td>Communicate with the GUI and Web Service.</td>
</tr>
</tbody>
</table>
### Table 1-3  Communication Ports (continued)

<table>
<thead>
<tr>
<th>Cisco VXC Manager Component</th>
<th>Protocol</th>
<th>Port</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>68</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4011</td>
<td></td>
</tr>
<tr>
<td>TFTP</td>
<td></td>
<td>69</td>
<td>Download bootable image to enable management processing.</td>
</tr>
<tr>
<td>HTTP</td>
<td></td>
<td>80</td>
<td>Communicate with the Web Service regarding actions and status of current task.</td>
</tr>
<tr>
<td>FTP</td>
<td></td>
<td>21</td>
<td>Download and upload files to the Master and Remote Software Repositories.</td>
</tr>
<tr>
<td>Standard Service and legacy support for older Cisco VXC Manager Agents</td>
<td>UDP</td>
<td>44956</td>
<td>Discover devices (using subnet directed broadcasts) that have older Cisco VXC Manager Agents (5.0.0.x and earlier) installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>44957</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td>44955</td>
<td>Discover devices using IP Range Walking. Upgrade devices that have an older Cisco VXC Manager Agent (5.0.0.x and earlier) installed.</td>
</tr>
<tr>
<td>ThreadX Manager Service</td>
<td>TCP</td>
<td>50000</td>
<td>Uses this port to communicate with ThreadX devices.</td>
</tr>
</tbody>
</table>

### Installing and Configuring FTP

Depending on your server version, use one of the following sections to install FTP:

- Installing and Configuring FTP on Windows XP Professional or Windows Server 2003, page 1-6
- Installing and Configuring FTP on Windows Server 2008 R2, page 1-13
- Installing and Configuring FTP on Windows 7, page 1-17
Installing and Configuring FTP on Windows XP Professional or Windows Server 2003

Use the following procedure to configure FTP on Windows XP Professional or Windows Server 2003.

Procedure

Step 1  Open the Add or Remove Programs dialog box (click Start > Control Panel > Add or Remove Programs).

Step 2  Click the Add/Remove Windows Components icon to open the Windows Components wizard.

Step 3  In the Components list, select the Application Server check box, and then click Details.

Step 4  Select the Internet Information Services (IIS) check box in the list, and then click Details.
Step 5 Be sure the following check boxes are selected:
- Common Files
- File Transfer Protocol (FTP) Service
- Internet Information Services Manager
- World Wide Web Service

Step 6 Select any other IIS-related service or subcomponent check box that you want to install, and then click OK.

Step 7 Click Next.

Step 8 When you are prompted, insert the Windows Server CD-ROM into the CD-ROM or DVD-ROM drive of the machine, or provide a path to the location of the files, and then click OK.

Step 9 Click Finish.

Configuring the FTP Service for Anonymous Connections Only

Use the following procedure to configure the FTP Service on Windows XP Professional or Windows Server 2003 to allow only anonymous connections.

Procedure

Step 1 Open the Internet Information Services (IIS) Manager (click Start > Administrative Tools > Internet Information Services (IIS) Manager).

Step 2 In the tree pane, expand Server_name (where Server_name is the name of the server), and then expand FTP Sites.
Step 3  In the tree pane, right-click on Default FTP Site, and then select Properties to open the Properties dialog box.

Step 4  Click the Security Accounts tab and be sure that the Allow Anonymous Connections check box is selected.

Step 5  Click the Home Directory tab and be sure that the Read, Write and Log visits check boxes are selected.
CHAPTER 1 Preparing For Installation

Installing and Configuring FTP

Step 6 Click Apply and then click OK.

Step 7 Close the Internet Information Services (IIS) Manager window.

Step 8 The FTP server is now configured to accept incoming FTP requests. Copy or move the files that you want to make available to the FTP publishing folder for access. The default folder is drive:\Inetpub\ftproot (where drive is the drive on which IIS is installed).

Installing and Configuring FTP on Windows Server 2008

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) is already installed on the server. Remember that IIS is included by default only with Windows XP Professional, Windows Vista Ultimate, Windows Vista Business, and Windows Vista Enterprise.

Installing FTP on Windows Server 2008

Use the following procedure to install FTP on Windows Server 2008.

Procedure

Step 1 On the taskbar, click Start > Administrative Tools > Server Manager to open the Server Manager window.

Step 2 In the Server Manager tree pane, expand Roles, and then click Web Server (IIS) to open the Web Server (IIS) window.
Step 3  In the details pane of the Web Server (IIS) window, scroll to Role Services, and then click Add Role Services to open the Select Role Services window.

Step 4  Under Role Services, expand FTP Publishing Service, select the FTP Server and FTP Management Console check boxes, and then click Next to open the Confirm Installation Selections window.

Step 5  After confirming, click Install.

Step 6  After installation is complete (the Results window displays a successful installation), click Close.

Configuring FTP on Windows Server 2008

Use the following procedure to configure FTP on Windows Server 2008.
**Procedure**

**Step 1**  On the taskbar, click `Start > Administrative Tools > Internet Information Services (IIS) Manager` to open the Internet Information Services (IIS) Manager window.

**Step 2**  In the tree pane, expand `Server_name` (where `Server_name` is the name of the server), and then select `FTP Sites`.

**Step 3**  In the FTP sites details pane, click the **Click here to launch** link, to open the IIS 6.0 Manager window.

**Step 4**  In the tree pane expand `Server_name` (where `Server_name` is the name of the server), and then expand `FTP Sites`.

*Note*  If FTP Site is stopped, click the **Start** icon to start it.

**Step 5**  In the tree pane, right-click on `Default FTP Site`, and then select **Properties** to open the Properties dialog box.

**Step 6**  Click the **Security Accounts** tab and be sure that the **Allow Anonymous Connections** check box is selected.
Chapter 1      Preparing For Installation

Installing and Configuring FTP

Step 7   Click the **Home Directory** tab and be sure that the **Read**, **Write** and **Log visits** check boxes are selected.

Step 8   Click **Apply**, and then click **OK**.

Step 9   Close the **Internet Information Services (IIS) Manager** window.

Step 10  The FTP server is now configured to accept incoming FTP requests. Copy or move the files that you want to make available to the FTP publishing folder for access. The default folder is drive:\Inetpub\ftproot (where drive is the drive on which IIS is installed).

---

### Configuring the FTP User Isolation Mode

With IIS, you can host multiple FTP sites on the same server. In this case, you can use the FTP user isolation feature to prevent users of one FTP directory from accessing the directory of another user.

In your Cisco VXC Manager environment, if you run FTP with IIS 7.0 or 7.5 and you do not require user isolation, you must set the FTP User Isolation mode to **User name directory**, as follows.

#### Procedure

**Step 1**   In the IIS Manager tree pane, click the FTP site used for Cisco VXC Manager.

**Step 2**   In the FTP Sites details pane, double-click **FTP User Isolation**.
Step 3 When the FTP User Isolation page appears, click **User name directory**.

Step 4 In the Actions pane, click **Apply**.

If you set the FTP User Isolation mode to **FTP root directory**, you can encounter issues when you perform client upgrades.

This configuration does not apply to IIS 6.0.

### Verifying FTP on Windows Server 2008

Use the following guidelines to verify FTP on Windows Server 2008.

**Procedure**

#### Step 1
Open a command prompt (click **Start** > **Run**, enter **cmd**, and then click **OK**).

#### Step 2
Type **ftp localhost**.

#### Step 3
Enter an administrator username and password.

#### Step 4
Ensure that sign-in is successful.

#### Step 5
Open the services panel and make sure that the FTP service is configured to start automatically.

### Installing and Configuring FTP on Windows Server 2008 R2

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) is already installed on the server. Remember that IIS is included by default only with Windows XP Professional, Windows Vista Ultimate, Windows Vista Business, and Windows Vista Enterprise.

### Installing FTP on Windows Server 2008 R2

Use the following procedure to install FTP on Windows Server 2008 R2.

**Procedure**

#### Step 1
On the taskbar, click **Start** > **Administrative Tools** > **Server Manager** to open the Server Manager window.

#### Step 2
In the Server Manager tree pane, expand **Roles**, and then click **Web Server (IIS)** to open the Web Server (IIS) window.

#### Step 3
In the details pane of Web Server (IIS), scroll to **Role Services**, and then click **Add Role Services** to open the Select Role Services window.
Step 4 Under Role Services, expand FTP Server, select the **FTP Service** and **FTP Extensibility** check boxes, and then click **Next** to open the Confirm Installation Selections window.

Step 5 After confirming, click **Install**.

Step 6 After installation is complete (the Results window displays a successful installation), click **Close**.

**Configuring FTP on Windows Server 2008 R2**

Use the following procedure to configure FTP on Windows Server 2008 R2.

**Procedure**

Step 1 On the taskbar, click **Start > Administrative Tools > Internet Information Services (IIS) Manager** to open the Internet Information Services (IIS) Manager window.
Step 2  In the tree pane, right-click on **Sites**, and then select **Add FTP Site** to begin creating an FTP site.

![FTP Site Configuration](image1)

Step 3  Enter the FTP site name, select the Physical path for the FTP root directory, and then click **Next**.

![FTP Site Configuration](image2)

Step 4  Keep the default value for IP Address as **All unassigned** and for Port as **21**.

![FTP Site Configuration](image3)
## Configuring the FTP User Isolation Mode

With IIS, you can host multiple FTP sites on the same server. In this case, you can use the FTP user isolation feature to prevent users of one FTP directory from accessing the directory of another user.

In your Cisco VXC Manager environment, if you run FTP with IIS 7.0 or 7.5 and you do not require user isolation, you must set the FTP User Isolation mode to **User name directory**, as follows.

### Procedure

1. **Step 1** In the IIS Manager tree pane, click the FTP site used for Cisco VXC Manager.
2. **Step 2** In the FTP Sites details pane, double-click **FTP User Isolation**.
Step 3 When the FTP User Isolation page appears, click **User name directory**.

Step 4 In the Actions pane, click **Apply**.

If you set the FTP User Isolation mode to **FTP root directory**, you can encounter issues when you perform client upgrades.

This configuration does not apply to IIS 6.0.

### Verifying FTP on Windows Server 2008 R2

Use the following procedure to verify FTP on Windows Server 2008 R2.

**Procedure**

Step 1 Open a command prompt (click **Start > Run**, enter `cmd`, and then click **OK**).

Step 2 Type `ftp localhost`.

Step 3 Enter an administrator username and password.

Step 4 Ensure that sign-in is successful.

### Installing and Configuring FTP on Windows 7

Before setting up your own FTP server in Windows, you must be sure that Internet Information Services (IIS) is already installed on the server. Remember that IIS is included by default only with Windows XP Professional, Windows Vista Ultimate, Windows Vista Business, and Windows Vista Enterprise.

### Installing FTP on Windows 7

Use the following procedure to install FTP on Windows 7.

**Procedure**

Step 1 On the taskbar, click **Start > Control Panel** to open Control Panel.

Step 2 Click **Programs > Programs and Features**, and then on the left pane click **Turn Windows Features on or off** to open the Windows Features window.

Step 3 Scroll to **Internet Information Services**.

Step 4 Expand **Internet Information Services**, and then expand **FTP Server**.
Step 5 Under FTP Server, select the FTP Extensibility and FTP Service check boxes, and then click OK to install FTP.

Configuring FTP on Windows 7

Use the following procedure to configure FTP on Windows 7.

Procedure

Step 1 On the taskbar, click Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager to open the Internet Information Services (IIS) Manager.

Note If you do not see Administrative Tools on the Control Panel, select Small icons or Large icons in the View by list.

Step 2 In the tree pane, right-click on Sites, and then select Add FTP Site to begin creating an FTP site.
Step 3  Enter the FTP site name, select the Physical path for the FTP root directory, and then click Next.

Step 4  Keep the default value for IP Address as All unassigned and for Port as 21.

Step 5  Select the Start FTP site automatically check box, change the SSL option to No SSL, and then click Next.

Step 6  Select the Anonymous and Basic Authentication check boxes.
Installing and Configuring IIS

**Step 7** Select **All users** in the Allow access to list.

**Step 8** Select the **Read** and **Write** check boxes.

**Step 9** Click **Finish**.

### Configuring the FTP User Isolation Mode

With IIS, you can host multiple FTP sites on the same server. In this case, you can use the FTP user isolation feature to prevent users of one FTP directory from accessing the directory of another user.

In your Cisco VXC Manager environment, if you run FTP with IIS 7.0 or 7.5 and you do not require user isolation, you must set the FTP User Isolation mode to **User name directory**, as follows.

**Procedure**

**Step 1** In the IIS Manager tree pane, click the FTP site used for Cisco VXC Manager.

**Step 2** In the FTP Sites details pane, double-click **FTP User Isolation**.

**Step 3** When the FTP User Isolation page appears, click **User name directory**.

**Step 4** In the Actions pane, click **Apply**.

If you set the FTP User Isolation mode to **FTP root directory**, you can encounter issues when you perform client upgrades.

This configuration does not apply to IIS 6.0.

### Verifying FTP on Windows 7

Use the following procedure to verify FTP on Windows 7.

**Procedure**

**Step 1** Open a command prompt (click **Start > Run**, enter **cmd**, and then click **OK**).

**Step 2** Type **ftp localhost**.

**Step 3** Enter an administrator username and password.

**Step 4** Ensure that sign-in is successful.

### Installing and Configuring IIS

Depending on your operating system, use one of the following sections:

- Installing and Configuring IIS 6.0 on Windows XP Professional or Windows Server 2003, page 1-21
- Installing IIS 7.0 on Windows Server 2008, page 1-26
Installing and Configuring IIS 6.0 on Windows XP Professional or Windows Server 2003

Use the following procedure to install and configure IIS 6.0 on Windows XP Professional or Windows Server 2003.

Procedure

Step 1 Open the Add or Remove Programs dialog box (click Start > Control Panel > Add or Remove Programs).

Step 2 Click the Add/Remove Windows Components icon to open the Windows Components wizard.

Step 3 In the Components list, select the Application Server check box.

Note Selecting Application Server performs a default installation of Internet Information Services (IIS) and includes components that are not necessary for Certificate Services. In most cases, this installation is acceptable for an isolated test environment. However, if you plan to connect your test environment to your production network, consult your organization security policy to determine which components need to be installed.

Step 4 Click Next.

Step 5 After the wizard completes the installation, click Finish.
Installing and Configuring WebDAV on Windows XP Professional or Windows Server 2003

Use the following procedure to install and configure WebDAV on Windows XP Professional or Windows Server 2003.

Procedure

**Step 1** Open the Add or Remove Programs dialog box (click Start > Control Panel > Add or Remove Programs).

**Step 2** Click the Add/Remove Windows Components icon to open the Windows Components wizard.

**Step 3** In the Components list select the Application Server check box, and then click Details.

**Step 4** Select the Internet Information Services (IIS) check box, and then click Details.

**Step 5** Select the World Wide Web Service check box, and then click Details.
Chapter 1      Preparing For Installation

Installing and Configuring IIS

Step 6  Select the WebDAV Publishing and World Wide Web Service check boxes, and then click OK.

Step 7  Click Next.
Installing and Configuring IIS

Step 8 When you are prompted, insert the Windows Server CD-ROM into the CD-ROM or DVD-ROM drive of the machine, or provide a path to the location of the files, and then click OK.

Step 9 Click Finish.

Configuring WebDAV on Windows XP Professional or Windows Server 2003 to Allow Only Anonymous Connections

Use the following procedure to configure the WebDAV on Windows XP Professional or Windows Server 2003 to allow only anonymous connections.

Procedure

Step 1 Open the Internet Information Services (IIS) Manager (click Start > Administrative Tools > Internet Information Services (IIS) Manager).

Step 2 In the tree pane, expand Server_name (where Server_name is the name of the server).
Chapter 1  Preparing For Installation

Installing and Configuring IIS

Step 3  In the tree pane, click Web Service Extension.

Step 4  In the details pane, right-click WebDAV, and then select Allow from the menu.

Step 5  In the tree pane, right-click Server_name (where Server_name is the name of the server).

Step 6  Select All Tasks > Restart IIS from the menu.
Installing IIS 7.0 on Windows Server 2008

By default, IIS 7.0 is not installed on Windows Server 2008. You can install IIS by using the Add Roles wizard in Server Manager. After installing IIS on the server, install WebDAV Extension for IIS 7.0.

Procedure

Step 1  On the taskbar, click Start > Administrative Tools > Server Manager to open the Server Manager window.

Step 2  In the Server Manager tree pane, select Roles.

Step 3  In the details pane, click Add Roles > Server Roles.

Step 4  On the Select Server Roles screen, select Web Server (IIS), click Next, and then click Next to open the Select Role Services window.
Step 5  Under Roles Services, expand **Web Server**, expand **Common HTTP Features**, and then select the **HTTP Redirection** check box.

Step 6  Under Web Server, expand **Application Development** and then select the **ISAPI Extensions** check box.

Step 7  Under Web Server, expand **Security**, select the **Basic Authentication** and **Windows Authentication** check boxes, and then be sure that the **Request Filtering** option is cleared.

Step 8  Under Web Server, expand **Performance** and then be sure that each option is cleared (**Static Content Compression** and **Dynamic Content Compression** should be cleared).

Step 9  Under Web Server, expand **Management Tools**, and then select the **IIS Management Console** and **IIS Management Scripts and Tools** check boxes.

Step 10  Under Web Server, expand **IIS 6 Management Compatibility** and then be sure all its options are selected.

Step 11  Click **Next** to open the Confirm Installation Selections window.
Step 12  After confirming, click **Install**.

Step 13  After installation is complete (the Results window displays a successful installation), click **Close**.

## Installing WebDAV Extension for IIS 7.0

Use the following procedure to install the WebDAV Extension for IIS 7.0.

### Procedure

**Step 1**  Download the 32-bit Installation Package of the WebDAV Extension for IIS 7.0 from [http://blogs.iis.net/robert_mcmurray/archive/2008/03/12/webdav-extension-for-windows-server-2008-rtm-is-released.aspx](http://blogs.iis.net/robert_mcmurray/archive/2008/03/12/webdav-extension-for-windows-server-2008-rtm-is-released.aspx)

**Step 2**  After downloading, double-click **webdav_x86_rtw.msi** to open and use the Microsoft WebDAV Extension for IIS 7.0 Setup wizard.

**Step 3**  After the software is installed, click **Finish**.

## Configuring the Web.config File

You can modify the Web.config file to prevent the following errors:

- Upload fails for files larger than 30 MB.
- Merlin imaging fails when the URL and query string sizes are not adequate.

Add the following content to the Web.config file (the Web.config file is found in the inetpub\wwwroot folder):

```xml
<security>
  <requestFiltering>
    <requestLimits maxAllowedContentLength="4294967296" maxUrl="8000" maxQueryString="8000"/>
  </requestFiltering>
</security>
```
Chapter 1      Preparing For Installation

Installing and Configuring IIS

This example shows the web.config file with the content added:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <directoryBrowse enabled="true" showFlags="Date, Time, Size, Extension, LongDate" />
    <security>
      <requestFiltering>
        <requestLimits maxAllowedContentLength="4294967296" maxUrl="8000" maxQueryString="8000" />
      </requestFiltering>
      </security>
    </system.webServer>
  </configuration>
```

Installing IIS 7.5 on Windows Server 2008 R2

By default, IIS 7.5 is not installed on Windows Server 2008 R2. You can install IIS by using the Add Roles wizard in Server Manager.

Procedure

---

**Step 1**  
On the taskbar, click **Start > Administrative Tools > Server Manager** to open the Server Manager window.

**Step 2**  
In the Server Manager tree pane, select **Roles**, and then click **Add Roles** to open the Add Roles wizard window.

**Step 3**  
In the Add Roles wizard, click **Server Roles**, and then check the **Web Server (IIS)** check box.

**Step 4**  
In the Add Roles wizard, click **Server Roles > Web Server (IIS) > Role Services**.

**Step 5**  
Under Role Services, expand **Web Server**, expand **Common HTTP Features**, and then select the **WebDAV Publishing** check box.
Chapter 1 Preparing For Installation

Installing and Configuring IIS

Step 6 Under Role Services, expand Application Development, and then select the ISAPI Extension check box.

Step 7 Under Role Services, expand Security, select the Basic Authentication and Windows Authentication check boxes, and then be sure that Request Filtering option is cleared.

Step 8 Under Role Services, expand Performance, and then be sure that each option is cleared (Static Content Compression and Dynamic Content Compression should be cleared).

Step 9 Under Role Services, expand Management Tools, and then select the IIS Management Console and IIS Management Scripts and Tools check boxes.

Step 10 Under Role Services, expand IIS 6 Management Compatibility, be sure that all options are selected, and then click Next to open the Confirm Installation Selections window.

Step 11 After confirming, click Install.

Step 12 After installation is complete (the Results window displays a successful installation), click Close.
Step 13  After successful installation of IIS 7.5 on Windows Server 2008 R2, you must verify the following advanced settings:

- Enable 32-Bit Applications is set to True.
- Idle Time-out (minutes) is set to 0 (zero).

Use the following guidelines:

a. On the taskbar, click Start > Administrative Tools > Internet Information Services (IIS) Manager to open the Internet Information Services (IIS) Manager window.

b. In the Internet Information Services (IIS) Manager tree pane, expand Server, and then click Application Pools to display the DefaultAppPool in the Application Pools list.

c. Right-click DefaultAppPool and select Advanced Settings to open the Advanced Settings window.

d. In the General section, ensure that Enable 32-Bit Applications is set to True.

e. In the Process Model section, ensure that Idle Time-out (minutes) is set to 0 (zero).
Installing IIS 7.5 on Windows 7

By default, IIS 7.5 is not installed on Windows 7. You can install IIS by using the Turn Windows Features on or off wizard in Programs and Features.

Procedure

Step 1  On the taskbar, click Start > Control Panel to open the Control Panel.
Step 2  Click Programs > Programs and Features, and then on the left pane click Turn Windows Features on or off to open the Windows Features window.
Step 3  Scroll to Internet Information Services.
Step 4 Expand **Internet Information Services**.

Step 5 Expand **Web Management Tools**, and then select the **IIS 6 Management Compatibility**, **IIS Management Console**, and **IIS Management Scripts and Tools** check boxes.

Step 6 Expand **World Wide Web Services**, expand **Application Development Features**, and then select the **ISAPI Extensions** check box.

Creating a DNS Service Location (SRV) Resource Record for Cisco VXC 2111/2211 ThreadX Devices

If you plan to use Cisco VXC 2111/2211 ThreadX devices, you can greatly improve the ThreadX client discovery process by creating a DNS Service Location (SRV) resource record.

Use the following procedure to create a DNS Service Location (SRV) resource record.

Procedure

Step 1 Open the DNS management console.
Step 2 Select the domain where the server is configured, right-click it, and then select Other New Records to open the Resource Record Type dialog box.
Step 3  Select the Service Location (SRV) resource record type and then click **Create Record** to open the New Resource Record dialog box.

Step 4  Use the following guidelines (Domain is automatically shown):

- Enter \_Pcoip-tool in the Service field.
- Enter \_tcp in the Protocol field.
- (Optional) Enter the value you want for this Cisco VXC Manager server in the Priority field (the lower the priority value, the higher the priority).
- (Optional) Enter the value you want for this Cisco VXC Manager server in the Weight field (within the same priority class the higher the weight value, the higher the priority).
- Enter 50000 in the Port number field.
- Enter the <FQDN of the Cisco VXC Manager server> (for example, p20.rap45.com) in the Host offering this service field.

Step 5  Click **OK**.
Installing or Upgrading Cisco VXC Manager

This section provides the detailed procedures you must complete to install or upgrade Cisco VXC Manager.

Be sure you have completed all preinstallation requirements as described in Chapter 1, “Preparing For Installation” before you begin installing or upgrading Cisco VXC Manager. In addition, be sure to remove any previous installations of Cisco VXC Manager, as described in Appendix B, “Uninstalling Cisco VXC Manager”.

Cisco VXC Manager installs the following Cisco VXC Manager components on a single server (Typical installation) or on multiple servers (Custom installation):

- **Cisco VXC Manager Database (Database)**—Stores and provides access to all of the information for device management, including logging, packages, user data, and Remote Software Repository information (there can be only one instance of this Cisco VXC Manager Database in your Cisco VXC Manager environment).
- **Software Repository (Repository)**—Stores Cisco VXC Manager packages for deployment use (in a Custom installation, you can have one Master Repository and multiple remote repositories in your Cisco VXC Manager environment).
- **Web Services (HServer)**—Uses HTTP/HTTPS to enable push and pull communications to devices equipped with the Cisco VXC Manager Web Agent (in a Custom installation, it is recommended to have as many instances of this Web Services as you have repository instances in your Cisco VXC Manager environment).
- **Standard Services**—Allows Cisco VXC Manager to:
  - Execute preboot management functions on devices that support Preboot Execution Environment (PXE).
  - Upgrade older Cisco VXC Manager Web Agents to the latest Cisco VXC Manager Web Agent. (There can be only one instance of the Standard Services in your Cisco VXC Manager environment.)
- **Administrator Console (MMC Snap-in)**—User interface allows you to manage all of your network devices easily and quickly (in a Custom installation, you can have multiple instances of this Administrator Console in your Cisco VXC Manager environment).

The Cisco VXC Manager components can be separately installed on different servers.
Installing or Upgrading Procedures (Cisco VXC Manager)

The Cisco VXC Manager installation wizard automatically detects whether a new installation or an upgrade installation is needed, and guides you through the process.

Tip
If you plan to install or upgrade Cisco VXC Manager components on multiple machines (Custom installation), you will repeat some of the installation procedures in this guide according to your environment design.

Use the following procedure to install or update the Cisco VCX Manager.

Procedure

Step 1
Download and extract the Cisco VXC Manager files to the root of the C:\ drive on the machines on which you will install Cisco VXC Manager (for upgrades, these are the machines on which you are currently running Cisco VXC Manager components).

Caution
Be sure to extract and install Cisco VXC Manager files to the root of the C:\ drive. If you install Cisco VXC Manager in any other folder, installation errors can occur.

Step 2
Double-click Setup.exe to open and use the InstallShield Wizard.

Use the following guidelines:

- If you are upgrading, be sure to use the correct system administrator password (SA Password) for the current installations of your Cisco VXC Manager.
- For Typical installations and upgrades, use defaults. It is recommended to use the InstallShield Wizard recommendations.
- For Custom installations and upgrades, use the detailed instructions. Use the detailed instructions in Detailed Custom Installation and Upgrade Instructions, page 2-3.
• Restart your computer after installation is complete. Select the **Yes, I want to restart my computer now** option, remove any disks from their drives, and then click **Finish**.

**Step 3** (Optional) Using Windows Firewall Only—If you are using Windows Firewall and are running Microsoft Windows XP Professional SP3, Windows Server 2003 (32-bit), or Windows Server 2003 R2 SP2 (32-bit) with your Cisco VXC Manager, you must log on as an administrator after installing and before using Cisco VXC Manager and add the Cisco VXC Manager DHCP Proxy, Cisco VXC Manager TFTP, Inetinfo, and Rptservicelogs programs to the Programs and Services list on the Exceptions tab of the Windows Firewall dialog box (for information on adding a program to the Windows Firewall exception list, refer to the Microsoft documentation on the Microsoft Web site). This must be done on each server on which you performed a Cisco VXC Manager installation or upgrade.

---

**Detailed Custom Installation and Upgrade Instructions**

Whether you are performing a Custom installation or upgrade on a single server or multiple servers, you must install or upgrade the Cisco VXC Manager components in the following order:

1. **Cisco VXC Manager Database (Database)**—There can be only one instance of the Cisco VXC Manager Database in your Cisco VXC Manager environment.

2. **Software Repository (Repository)**—You can have one Master Repository and multiple remote repositories in your Cisco VXC Manager environment.

3. **Web Services (HServer)**—It is recommended to have as many instances of WebServices as you have repository instances in your Cisco VXC Manager environment.

4. **Standard Services**—There can be only one instance of Standard Services in your Cisco VXC Manager environment.

5. **Administrator Console (MMC Snap-in)**—You can have multiple instances of the Administrator Console in your Cisco VXC Manager environment.

Be aware that Web Services (HServer), Standard Services, Administrator Console (MMC Snap-in) components require MDAC 2.8. Cisco VXC Manager installs MDAC 2.8 if it is not already present on the server.

Depending on your installation selections, the installation wizard will automatically guide you through the specific process you need. Use the following tips when installing or upgrading each component grouping you want on a server (although upgrades do not show installation wizard screens, you can still use the information contained in these sections):

- **Cisco VXC Manager Database Installation Tips You Need to Know**, page 2-4
- **Software Repository Installation Tips**, page 2-7
- **Installing Multiple Administrator Consoles**, page 2-9

---

**Tip**

If you are installing or upgrading Cisco VXC Manager components on multiple machines (requires repeating the installation wizard for each component grouping you want), be sure to select the correct components for the server on which you are installing or upgrading components. For example, you can use the InstallShield Wizard to install the Cisco VXC Manager Database on one server, and then use the InstallShield Wizard to install the other components on a second server.
Cisco VXC Manager Database Installation Tips You Need to Know

Depending on how you are installing, use the following guidelines when prompted for Database configurations during an installation or upgrade:

- If you are installing a new Cisco VXC Manager Database on a server, be sure to select the **The Cisco VXC Manager database has not been installed** option.

Figure 2-1 Initial Cisco VXC Manager Database Installation

- If you are using an existing SQL Server during your initial Cisco VXC Manager Database installation configurations, be sure to note the Server name, the TCP/IP Port, and the Database Password (for the default user named rapport), as you will use this information when you install the other Cisco VXC Manager components. If you do not specify the TCP/IP Port for the Cisco VXC Manager Database, the default 1433 is used (this is the port the database server uses for communication with Cisco VXC Manager components).

Caution
If you use the Change Rapport Database Password option (for example, to satisfy company password requirements), be sure to note the password for Cisco VXC Manager installation use and general password recovery.
If you intend to use your existing SQL Server 2005 Express Edition for the Cisco VXC Manager Database, ensure the Log on as account for the SQLExpress service is set to Local System account as follows:

a. From the Start menu on your server, navigate to Administrative Tools > Services.
b. Right-click SQL Server (SQLEXPRESS) Services.
c. Select Properties.
d. Click the Log On tab.
e. Select the Local System account option.
f. Select the Allow service to interact with desktop check box.
g. Click OK.
h. Restart the SQL Server (SQLEXPRESS) service.
If you have already installed the Cisco VXC Manager Database on a separate server and you are currently installing other Cisco VXC Manager components on a server, the InstallShield Wizard will prompt you for a Cisco VXC Manager Database confirmation. Be sure to select the correct server name, enter the correct TCP/IP Port, and enter the correct database password (for the default user named rapport). These are the fields you entered during your Cisco VXC Manager Database installation. If you do not specify the TCP/IP Port for the Cisco VXC Manager Database, the default 1433 is used (this is the port the database server uses for communication with Cisco VXC Manager components).

If you have an existing SQL Server that was installed using Windows Authentication mode only, Cisco VXC Manager utilizes mixed mode authentication. Be aware that if you are using an existing SQL Server that was installed using Windows Authentication mode only, the Cisco VXC Manager Database user will be unable to log in to the SQL database, and the Cisco VXC Manager Database installation will fail. Therefore, you must open your SQL Server Configuration Manager and enable TCP/IP connections (see the Microsoft documentation for your SQL Server).
Software Repository Installation Tips

Depending on how you are installing, use the following guidelines when prompted for Repository configurations during an installation or upgrade:

Tip
If your network has multiple subnets, consider deploying a copy of the Cisco VXC Manager Software Repository (Repository) on each subnet to allow you to store large device applications and image files locally. When upgrades are distributed to devices on a subnet from a local repository, network traffic is reduced.

- When selecting the protocol to use for repository communication, use the following guidelines. Note that the wizard attempts to connect to your FTP service to ensure connectivity and read/write permissions. Cisco VXC Manager only verifies an existing connection; it does not configure your FTP service.
  - FTP—Select this option if you want Cisco VXC Manager to download packages from the repository using the FTP protocol.

Caution
If you intend to use the firmware upgrade feature for ThreadX devices, FTP must be configured.

If you are using an existing FTP service, the wizard prompts you for an IP Address, username, and password.

If you are using an existing IIS FTP service, the wizard creates a local Cisco VXC Manager user and assigns the user read/write permissions to the IIS FTP service.

- HTTP —Select this option if you want Cisco VXC Manager to download packages from the repository using the HTTP protocol.

- FTP and HTTP—Select both options if you want Cisco VXC Manager to download packages from the repository using either the FTP or HTTP protocol. If both options are selected, HTTP is attempted first; if HTTP fails, the FTP protocol is then attempted.

Note
If HTTP is enabled but IIS is not configured in the OS, Cisco VXC Manager will display error messages when you attempt to upgrade Cisco VXC clients. The error message will indicate upgrade failure even though the upgrades may be successful using FTP. Therefore, do not select the HTTP option unless IIS is actually available for use by Cisco VXC Manager.

Tip
HTTPS can be enabled/configured later in an HTTP repository.
When selecting the authentication options to apply to software repositories, use the following guidelines. Note that you can select any or all of the options; if you select all three options, Windows Authentication is applied.

- **Anonymous Access**—This mode does not require a username or password to access the repository.

- **Windows Authentication**—This is the most secure form of authentication in IIS. When you log in, Windows NT validates your login and only your username is transmitted over the network. Your password is not transmitted.

- **Basic Authentication**—This authentication mode requires you to log in with a valid Windows NT username and password to access the system. The password is transmitted over the network in clear text.
If you have an existing repository server account instead of the default user account named rapport, (for example, you are upgrading an existing Cisco VXC Manager repository server or want to use an existing Active Directory) select the Use an existing Repository Server Account option, and then enter the IP Address (or server name) and the username and password of that account.

### Installing Multiple Administrator Consoles

If you are installing multiple instances of the Administrator Console (MMC Snap-in) in your Cisco VXC Manager environment and want to use other administrators for additional Administrator Console installations, you must perform the following procedure.

<table>
<thead>
<tr>
<th>Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>These instructions do not pertain to the initial installation of the Administrator Console for the local administrator.</td>
</tr>
</tbody>
</table>

#### Procedure

**Step 1**
Add the user you want as the eventual administrator of the Administrator Console instance using the Configuration Manager as described in *Administration Guide for Cisco VXC Manager*.

**Step 2**
Install the instance of the Administrator Console (MMC Snap-in) as described in *Installing or Upgrading Procedures (Cisco VXC Manager)*, page 2-2. Note that after this installation, the Administrator Console will not be able to connect to the Cisco VXC Manager Database or a software repository in your Cisco VXC Manager environment until you complete Step 3.

**Step 3**
After installing the instance of the Administrator Console, use the Configuration Manager (as described in *Administration Guide for Cisco VXC Manager*) to edit the user you want as the administrator (from step 1) so that the user has administrator rights for that instance of the Administrator Console.
Back up the Cisco VXC Manager Database

To backup and restore the Cisco VXC Manager Database, install Microsoft SQL Server Management Studio, and use the backup and restore options (see Microsoft documentation for more details).

External SQL Integration

This section provides information on how to configure Cisco VXC Manager to use an external SQL Server database, installed locally on the Cisco VXC Manager machine or on a different machine, instead of using the built-in SQL Server Express provided by the Cisco VXC Manager installer.

To improve scalability and performance in managing large deployments, Cisco VXC Manager supports installation of its major components on the same machine or on separate machines. The most common configuration is to install Cisco VXC Manager on two machines, one containing the Cisco VXC Manager database and the other containing the remaining components. In addition, multiple instances of the Cisco VXC Manager GUI can be installed on additional machines.

Requirements:
- Microsoft SQL Server 2005 or 2008 must be installed on the database machine
- Firewall port exception: Open Database Connectivity (ODBC) Remote Access over TCP Port 1433 (Default)
- SQL Server must be installed with Mixed Mode Authentication
- A local SQL Account name 'db_owner' must be permitted for use with Cisco VXC Manager from Cisco VXC Manager > Configuration Manager > User Permissions
- 2 GB storage of free disk space for installing the database

Procedures

You can set up an external SQL database for Cisco VXC Manager either automatically or manually.

Automatic Setup

Use this procedure to set up the external SQL database automatically.

Run Installer

Step 1: Download the Cisco VXC Manager installer.
Step 2: Extract it to the SQL Server machine.
Step 3: From the folder named Disk 1, launch the Cisco VXC Manager installer setup.exe.
Step 4: Accept the EULA.
Step 5: When the Cisco VXC Manager Prerequisite Utility appears, you can safely close it as the only requirement needed is for port 1433 to be open in your firewall. (The database server uses this port for communication with Cisco VXC Manager components.)
Step 6: Choose Custom Install.
Step 7: Choose the The Cisco VXC Manager database has not been installed option.
Step 8: De-select all components other than the Cisco VXC Manager Database.
Step 9 Provide the SQL Server Host and Authentication account information.
Step 10 Complete the installer.

Manual Setup

Use this procedure to set up the external SQL database manually.

Attach the Database

Step 1 Download the Cisco VXC Manager installer.
Step 2 Extract it to the SQL Server machine.
Step 3 Open the Cisco VXC Manager Installer package.
Step 4 Under the folder named Disk 1, open the Database folder.
Step 5 Move a copy of the Rapport4.ldf and Rapport4.mdf files to a directory on the server for use with SQL. (The default SQL location is C:\Program Files\Microsoft SQL Server\MSSQL\Data).
Step 6 Open the SQL Enterprise Manager tool. Log in using the 'sa' account (or another account with DB Admin rights).
Step 7 Navigate to the server or instance on which you are going to install the new database.
Step 8 Expand the Database node.
Step 9 Choose the Attach Database option (click the Attach Database icon, or right-click the Database node and choose Attach Database).
Step 10 Browse to the location of the newly copied Rapport4.ldf and Rapport4.mdf files.
Step 11 Attach the database name as RapportDB.
Step 12 Specify 'sa' as the database owner.
Step 13 Click OK to attach the database.

Configure the Database User

Step 1 Expand the newly attached RapportDB database.
Step 2 Choose the Users node under RapportDB.
Step 3 Create a new SQL user account "Rapport" (SQL Server Authentication).
   a. Set Password to "ThinMgmt_451".
   b. Set Default Database to “RapportDB”.
   c. Uncheck the Enforce Password Policy check box, if needed (depending on your company security policies).
Step 4 Click OK to create the new user (confirm password if prompted).
Step 5 From the Login name drop-down list, choose the newly created Rapport user account (the Login name and User name should both appear as Rapport).
Step 6 Grant db_owner access to the Rapport account by checking the db_owner check box.
Chapter 2 
Installing or Upgrading Cisco VXC Manager

External SQL Integration

Step 7  Click **OK** to finish adding the Rapport account with db_owner access to the RapportDB database.

---

**Update the Install Table**

Step 1  Choose the Tables Node from under the RapportDB.
Step 2  Scroll down to the Install table.
Step 3  Right-click **Install** and choose **Open Table > Return all rows**.
Step 4  Create the following entries:
   a. Module = Rapport4DB
   b. ServerName = %COMPUTERNAME% of machine including DNS suffix if enabled on server (i.e. vxcm-server.mycompany.com)
   c. UserName = Administrator (or your login name)
   d. Installed = Date you are performing the installation (for example, 01/01/2012 12:00:00 AM)
   e. Status = MASTER
   f. LatestHFID = Current hotfix number (HF04085007311 for Cisco VXC Manager 4.8.5)
Step 5  Close the Install table.

---

**Note**  If you install a subsequent hotfix after your initial installation, then the HF number to include in step 4f will change. To view the new number:

1. On the Cisco VXC Manager server, click **Start > Run**.
2. To open the registry editor, enter **regedit**.
3. Navigate to **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Wow6432Node > Rapport**.
4. Use the highest displayed HF key.

---

**Update the License Table (Only Required for Managing Non-Cisco Devices)**

Step 1  Select the Tables Node from under RapportDB.
Step 2  Scroll down to the License table.
Step 3  Right-click **License** and choose **Open Table > Return all rows**.
Step 4  Create the following entry:
   a. Sales = temp
Step 5  Close the License table
On Additional Cisco VXC Manager Component Servers

Step 1  Download and extract the latest Cisco VXC Manager installer.
Step 2  From the Disk 1 folder, launch the Cisco VXC Manager installer setup.exe.
Step 3  Accept the EULA.
Step 4  Choose **Custom Install**.
Step 5  When prompted for the location of the Cisco VXC Manager database component:
   a. Choose the **The Cisco VXC Manager database has been installed on the following server** option.
   b. Choose the Database server from the drop-down list (or manually enter if needed).
   c. Select the components that you wish to install on this server (Database will be greyed-out)
   d. Complete the install wizard
Chapter 2 Installing or Upgrading Cisco VXC Manager

External SQL Integration
Using HTTPS as the Communication Protocol for Cisco VXC Manager

The following procedures show how to configure HTTPS as the communication protocol with Cisco VXC Manager.

The Windows Server configuration steps shown are for Windows Server 2008. For other server operating systems, the steps may differ. See Microsoft documentation for the specific operating system for more details.

![Note](This appendix is not applicable to Cisco VXC 2111/2211 clients running ThreadX firmware because these clients do not support secure communications with the Cisco VXC Manager.

### Configuring HTTP and HTTPS for IIS

To operate with HTTP and HTTPS, you must add specific MIME types to the Rapport HTTP Server in IIS. The Cisco VXC Manager installer automatically adds the following MIME types during installation: .bat, .img, .ini, .raw, and .reg. In addition, you must manually add the .cer and .crt MIME types for operation with HTTP and HTTPS.

**Procedure**

**Step 1** In IIS Manager, connect to the Rapport HTTP Server.

**Step 2** In the Features View, double-click **MIME Types**.

**Step 3** In the Actions pane, click **Add**.

**Step 4** Add the following MIME types:
- .cer - application/x-x509-ca-cert
- .crt - application/x-x509-ca-cert

### Creating a Root Authority Certificate

Use the following procedure to create a Root Authority Certificate on your Active Directory domain controller. As an alternative, you can obtain a root certificate directly from a certificate authority.
Note
This is a one-time procedure on the Certificate Authority.

Procedure

Step 1  On the Active Directory domain controller, open IIS Manager (using either Start > Run > inetmgr or Server Manager > Roles > Web Server(IIS) > Internet Information Server).

Step 2  To create the Domain Certificate, click Server > Server Certificates, and fill in the information requested in the following dialog box.

Step 3  Click Next.

Step 4  In the Specify Online Certification Authority field, click Select.
Step 5  In the dialog box that appears, choose your certificate authority and click OK.

Step 6  In the **Friendly name** field, enter an easily recognizable name for the certificate authority (for example, something.domain.com).

Step 7  Click **Finish**.
Creating the Cisco VXC Manager Certificate

Use the following procedure to create the Cisco VXC Manager domain certificate.

**Note**

This is a one-time procedure on the Cisco VXC Manager server.

**Procedure**

**Step 1**
Click the server name.

**Step 2**
Double-click Server Certificates.

**Step 3**
Click Create Domain Certificate.
Step 4 Fill in the information requested in the following dialog box.

Step 5 Click Next.

Step 6 In the Specify Online Certification Authority field, click Select.
Appendix A  Using HTTPS as the Communication Protocol for Cisco VXC Manager

Step 7  In the dialog box that appears, choose your certificate authority and click **OK**.

Step 8  In the **Friendly name** field, enter an easily recognizable name for the certificate authority (for example, something.domain.com).

Step 9  Click **Finish**.
Exporting the Certificates to Local Files

Use the following procedure to export the Cisco VXC Manager certificate to a local file.

Procedure

Step 1  To export the Cisco VXC Manager certificate to a local file, choose the certificate listed under Server Certificates, and click View.
Step 2  Under Details, click Copy To File.
Step 3  From the Certificate Export Wizard, click Next.
Step 4  Click No, do not export the private key and click Next.
Step 5  Click DER encoded binary X.509 (.CER) and click Next.
Step 6  Name and save the certificate to your local server.

Use the following procedure to export the root authority certificate to a local file.

Procedure

Step 1  Under the Certification path, choose the root authority certificate.
Step 2  Click View Certificate.
Step 3  Under Details, click Copy To File.
Step 4  From the Certificate Export Wizard, click Next.
Step 5  Click No, do not export the private key and click Next.
Step 6  Click DER encoded binary X.509 (.CER) and click Next.
Step 7  Name and save the certificate to your local server.

Configuring Clients to Securely Check In Using Port 443

After you save the certificates locally, create a Cisco VXC Manager package to push the certificates to the thin clients. The package structure must contain an RSP file, as well as a directory with the exact same name as the RSP file.

Cisco VXC 6215

For Cisco VXC 6215, assuming an RSP file named Certs_Package.rsp, the folder structure and the corresponding files for the package must be as follows:

~/Certs_Package/wlx/wlx.ini
~/Certs_Package/wlx/certs/<rootauthoritycert>
~/Certs_Package/wlx/certs/<vxcmcert>
~/Certs_Package.rsp
Appendix A  Using HTTPS as the Communication Protocol for Cisco VXC Manager

where <rootauthoritycert> is the Root Authority certificate and <vxcmcert> is the Cisco VXC Manager certificate.

Sample wlx.ini File

```
ImportCerts=yes
Certs=rootca_new.cer;vxcm_new.cer
```

where the Certs=rootca_new.cer;vxcm_new.cer parameter specifies the certificates to install. (For more information on setting up a wlx.ini file, see Cisco Virtualization Client 6215 INI Files Reference Guide.)

Sample RSP file

```
[Version]
Number=Certs_Package
OS=SLX
Category=Other Packages

[Script]
RP= "<regroot>"
```

Register the package in Cisco VXC Manager and push it to the clients. For details, see Administration Guide for Cisco VXC Manager.

Cisco VXC 2112/2212

For the Cisco VXC 2112/2212, rather than create a wlx directory and wlx.ini file, you must create a wnos folder and wnos.ini file. Assuming an RSP file named Certs_Package.rsp, the folder structure and the corresponding files for the package must be as follows:

```
~/Certs_Package/wnos/wnos.ini
~/Certs_Package/wnos/certs/<rootauthoritycert>
~/Certs_Package/wnos/certs/<vxcmcert>
~/Certs_Package.rsp
```

Where <rootauthoritycert> is the Root Authority certificate and <vxcmcert> is the Cisco VXC Manager certificate.

Sample wnos.ini File

```
signon=0
Privilege=high
AddCertificate=<CA certificate file name>
```

where the AddCertificate=<CA certificate file name> parameter specifies the certificate to install. (For more information on setting up a wnos.ini file, see Cisco Virtual Experience Client 2112/2212 INI Files Reference Guide for WTOS.)

Sample RSP file

```
[Version]
Number=CADeployment
Description=CA Certificate Deployment
OS=BL
Category=Images

[Script]
```

Register the package in Cisco VXC Manager and push it to the clients. For details, see Administration Guide for Cisco VXC Manager.
Adding an HTTPS Site Binding in IIS

Use the following procedure to add an HTTPS site binding in IIS.

**Procedure**

---

**Step 1**  Choose the Rapport HTTP Server.

**Step 2**  Under the Action pane, choose **Edit Bindings**.

**Step 3**  In the Edit Site Bindings window choose **https, All unassigned** IP addresses, and the VXCM certificate.

![Add Site Binding](image)

**Step 4**  Restart the HTTP Server.

After the HTTP Server restarts, when the client performs a subsequent check-in, the client will use port 443 (provided that you have pushed the certificate to the client in accordance with Configuring Clients to Securely Check In Using Port 443, page A-7).

---

Configuring Secure Package Downloads

Use the following procedure to configure secure package downloads.

**Procedure**

---

**Step 1**  In Cisco VXC Manager, choose **Configuration Manager > Software Repositories**.

**Step 2**  Click the software repository to configure for secure downloads.

**Step 3**  Choose **HTTPS**.

This setting enables secure downloads for all clients.
Step 4  For each repository that uses HTTPS, ensure that the value in the Location field matches the hostname or IP address that you configured in the Friendly name field for the Cisco VXC Manager certificate in Creating the Cisco VXC Manager Certificate, page A-4. (For example, if the certificate is issued to the hostname for the Cisco VXC Manager, then the repository location must also be a hostname.)
Uninstalling Cisco VXC Manager

When using a Microsoft Windows remove program feature (such as Add and Remove Programs or Programs and Features) to remove Cisco VXC Manager, the database server will require login credentials to complete the uninstallation of Cisco VXC Manager.

Figure B-1  Database Server Login Credentials

Depending on your Cisco VXC Manager installation, do one of the following:

- If you had Cisco VXC Manager install the default Microsoft SQL Server 2005 Express as your database server, enter sa in the Login ID field and enter ThinMgmt_451 in the Password field.

- If you used an existing database server during your Cisco VXC Manager installation (that is, any supported database server that is not installed by Cisco VXC Manager during the Cisco VXC Manager installation, see Software Requirements, page 1-3 and Cisco VXC Manager Database Installation Tips You Need to Know, page 2-4), enter sa in the Login ID field and your password for that server.
Caution

If you do not enter the correct credentials to remove the SQL Server, the database will persist on the server after the remaining components of Cisco VXC Manager are uninstalled. Any later installs of Cisco VXC Manager will fail until other means are used to delete the SQL Server. In this case, refer to the SQL Server documentation for information.