QUICK START GUIDE

Cisco Monitor Manager 1.1.2

1 Supplemental License Agreement

SUPPLEMENTAL LICENSE AGREEMENT FOR CISCO SYSTEMS NETWORK MANAGEMENT SOFTWARE: CISCO MONITOR MANAGER

IMPORTANT-READ CAREFULLY: This Supplemental License Agreement ("SLA") contains additional limitations on the license to the Software provided to Customer under the End User License Agreement between Customer and Cisco. Capitalized terms used in this SLA and not otherwise defined herein shall have the meanings assigned to them in the End User License Agreement. To the extent that there is a conflict among any of these terms and conditions applicable to the Software, the terms and conditions in this SLA shall take precedence.

By installing, allowing to be installed, downloading, accessing or otherwise using the Software or using the equipment that contains this Software, Customer agrees to be bound by the terms of this SLA. If Customer does not agree to the terms of this SLA, Customer may not install, download, access or otherwise use the Software. Customer may retain a third party ("Contractor") to install the Software for Customer, provided that (i) Customer and Contractor agree that the provisioning of installation services by Contractor to Customer creates an agency relationship and (ii) Customer shall remain fully responsible and liable for compliance by Customer and Contractor with the terms of the End User License Agreement and this SLA. When used below, the term "server" refers to a central processor unit owned or leased by Customer or otherwise embedded in equipment provided by Cisco.

1. **DEFINITIONS**

The following terms will have the meanings ascribed to them below.

- "Subscription Cycle" means the one (1) year period of time for which Customer pays the required Subscription Fees in advance. The Subscription Cycle is set forth in the applicable Purchase Order. The Subscription Cycle begins after successfully registering your copy of the Software online at Cisco's web site.
- "Subscription Fees" means the license or subscription fees for Customer's use of the Software described in the applicable Purchase Order. Subscription fees are paid by Customer up-front at the beginning of each Subscription Cycle.
- "Self Managed Cisco Monitor Manager" means the version of Cisco Monitor Manager that works as a software application as directed by the customer, but does not communicate with Cisco Monitor Director.

- "Cisco Monitor Manager MSP" means the version of Cisco Monitor Manager that has the ability to communicate with Cisco Monitor Director and is provided to Customer for the Subscription Cycle.
- "Cisco Monitor Manager Limited Version" means the version of either Self Managed Cisco Monitor Manager or Cisco Monitor Manager MSP that supports the monitoring of up to 25 IP addressable devices, which could be a combination of Cisco routers/switches/firewalls/access points and third party devices plus 48 IP phones.
- "Cisco Monitor Manager Standard Version" means the version of either Self Managed Cisco Monitor Manager or Cisco Monitor Manager MSP that supports the monitoring of up to 70 IP addressable devices, which could be a combination of Cisco routers/switches/firewalls/access points and third party devices plus 250 IP phones.
- Cisco Monitor Manager 1.1.2 is interoperable with Cisco Monitor Director 1.1.2 but not with Cisco Monitor Director 1.1.

2. ADDITIONAL LICENSE RESTRICTIONS

- Cisco hereby grants Customer a non-exclusive worldwide, perpetual, revocable nontransferable object code license (without sublicense rights) in Self Managed Cisco Monitor Manager to install and use the Software for network monitoring and management.
- Cisco hereby grants to Customer a non-exclusive worldwide, revocable, nontransferable object code license (without sublicense rights) for the Subscription Period in Cisco Monitor Manager MSP for use in connection with the use and license of Cisco Monitor Director.
- **Installation and Use.** The Software components are provided to Customer solely to install, update, supplement, or replace existing functionality of the applicable Network Management Software product. During Customer's license of the Software and subject to the terms and condition of the End User License Agreement and this SLA, Customer may install and use on a single server, one (1) copy of the following software components, in object code form only, as included in, and for use solely with, the Software:
  - Runtime portion of MySQL Pro 5.0.
- **Number of Devices.** The number of devices monitored by Customer will be based on whether it purchases Cisco Monitor Manager Limited Version or Cisco Monitor Manager Standard Version as defined above.

- **Using Software to Provide Network Monitoring Services.** Customer may use the Software to collect and analyze device information and communicate such information to authorized copies of Cisco Monitor Director to provide network monitoring services to third parties.
- **Reproduction and Distribution.** Customer may not reproduce nor distribute software.

3. SUBSCRIPTION CYCLE AND FEES

- **Fees.** Cisco may amend the pricing in Subscription Fees for Cisco Monitor Manager MSP from time to time upon prior notice, provided, however, that any amended pricing will not take effect until the beginning of the next Subscription Cycle. Cisco may also charge customer additional fees for upgrades of the Software.
- **Payment Terms.** Customer will pay to Cisco the Subscription Fees in advance for Cisco Monitor Manager MSP, and will make (a) the first Subscription Fee payment as specified in the Purchase Order; and (b) subsequent Subscription Fee payments at the beginning of each subsequent Subscription Cycle. All Subscription Fees are nonrefundable. For Self Managed Cisco Monitor Manager, Customer will pay to the Cisco the Fees in advance. All Fees are nonrefundable.
- **Effect of Termination.** Upon termination or expiration of this Agreement, Customer will promptly cease all use of the Software and destroy all copies of all or any part of the Software in its possession. Any payment obligations incurred prior to termination or expiration of this Agreement will survive such termination or expiration.
- **Expiration of Cisco Monitor Manager MSP.** Upon expiration of Customer's license in Cisco Monitor Manager MSP, Cisco hereby grants Customer a non-exclusive worldwide, perpetual, revocable, nontransferable object code license (without sublicense rights) in Self Managed Cisco Monitor Manager to install and use the Software for network monitoring and management.

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

Please refer to the Cisco Systems, Inc. End User License Agreement.

2 Cisco Monitor Manager Overview

Cisco Monitor Manager V 1.1.2

Copyright (c) 2007 by Cisco Systems, Inc.
All rights reserved.

Cisco Monitor Manager is an integrated network management application that monitors small-medium business (SMB)-class routers, switches, security appliances, access points, and wireless controllers. Cisco Monitor Manager remotely polls and collects data from these devices and works with Cisco Monitor Director to provide seamless, centralized network management across multiple customer sites.

The following summarizes the Cisco Monitor Manager features:

- Device system parameter configuration
- Network discovery
- Graphical view of network devices
- Device inventory management
- Configuration file management
- Device health, performance, and voice monitoring
- Collection of performance and fault history data
- Reports
- Alerts/Syslog messages
- Support for launching Cisco device managers

In this document you will find:

- Hardware and software requirements for optimal performance
- Detailed installation and post-installation instructions
- Pointers to relevant documentation

3 System Requirements

To ensure the proper installation and operation of Cisco Monitor Manager, verify that all of the requirements listed in the following table are met before proceeding.

Component	**Requirement**
Available disk space	40 GB Note the following: • During installation, files are unzipped into your machine's default temp directory (the directory specified by the TMP user environment variable). • Verify that there is at least an additional 1 GB of free disk space available to ensure that Cisco Monitor Manager is installed properly.
RAM	• Limited Version: 1 GB • Standard Version: 2 GB
CPU processor	• Limited Version: Intel Pentium IV 1 GHz or newer • Standard Version: Intel Pentium IV 2 GHz or newer
Monitor resolution	1024 x 768 pixels or higher
Operating System	Windows XP Professional Service Pack 2

Component	Requirement
Database port	Assign port 3310 for database use
Protocols	Enable the following protocols on your machine: • Syslog—Verify that port 514 is not already being used by another Syslog receiver application. • TFTP—Verify that port 69 is not already being used by another application. Enable the following protocols on devices that will be managed by Cisco Monitor Manager: • ARP • CDP • HTTP/HTTPS—Required for all Cisco devices to enable features such as VPN monitoring and port search. In addition, HTTPS must be enabled on Cisco ASA and Cisco PIX devices to support premium management. • SNMP—The default protocol used to discover network devices.

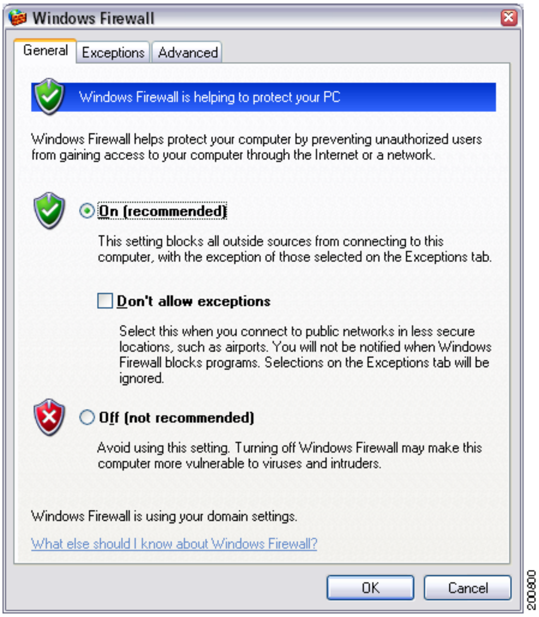
Note the following:

- If Cisco Security Agent is installed on your machine, you might need to disable it before you install Cisco Monitor Manager, discover network devices, or add devices to a discovered network.
- We recommend that you do not install both Cisco Monitor Manager and Cisco Monitor Director on the same machine.
- We recommend that you have administrator privileges on the machine on which you install Cisco Monitor Manager.
- The Secure Socket Layer (SSL) certificates that Cisco Monitor Manager uses to provide secure communication are created and self-signed by Cisco Systems, Inc. If you prefer to use customized SSL certificates, see the “Creating Customized SSL Certificates” online help topic.
- Make sure that the antivirus software installed on your machine has not been disabled. Otherwise, you might not be able to install Cisco Monitor Manager.
- By default, SNMP v1 is disabled on Cisco wireless controllers. In order to manage this type of device with Cisco Monitor Manager, make sure SNMP v1 is enabled.
- Users who do not have administrator privileges will not be able to launch Cisco Monitor Manager.
- We recommend that you keep Cisco Monitor Manager running after you install it. Unlike Cisco Monitor Director, Cisco Monitor Manager does not run as a service. As a result, performance monitoring and device discovery take place only when Cisco Monitor Manager is running.

- After you install Cisco Monitor Manager on a machine that also has McAfee VirusScan Enterprise installed, you will not be able to send emails from Cisco Monitor Manager until you unblock port 25:
  - **a.** Launch the VirusScan Console window.
  - **b.** Right-click the Access Protection task, and then select **Properties**.
  - **c.** In the Port Blocking tab, deselect the **Prevent mass mailing worms from sending mail** check box, and then click **Apply**.
  - **d.** Click **OK**.
- By default, Windows Firewall is enabled on Windows XP machines. As a result, Cisco Monitor Manager instances cannot communicate with a Cisco Monitor Director instance installed on a Windows XP machine until you open the HTTPS port on that Windows XP machine through the firewall.

  To open the port:

Step 1 From the machine on which Cisco Monitor Director is installed, select **Start > Control Panel > Windows Firewall**. The Windows Firewall dialog box appears.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● **On (recommended)**

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ **Don't allow exceptions**

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

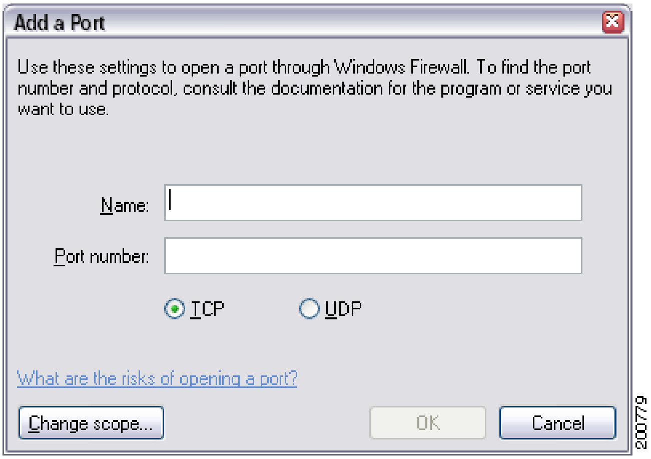
○ **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your domain settings.

What else should I know about Windows Firewall?

Step 2 Click the **Exceptions** tab, and then click **Add Port...**. The Add a Port dialog box appears.



Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name:

Port number:

● TCP ○ UDP

Step 3 Enter the name and number of the HTTPS port (the default port is 443).

Step 4 Ensure that the **TCP** radio button is selected, and then click **OK**.

Note If Cisco Monitor Director is installed on a machine with an application that already uses port 443, the port might be assigned to that application instead of to Cisco Monitor Director after a machine restart. If this happens, Cisco Monitor Director displays a message that the port is already being used. You must use the Administration Console to configure another port for HTTPS service. For more information on the Administration Console, see the Cisco Monitor Director 1.1.2 online help.

4 Before You Begin

The following section describes the tasks you must complete before you install Cisco Monitor Manager 1.1.2.

Step 1 Obtain a runtime license.

a. Determine the MAC address of the machine on which you will install Cisco Monitor Manager by opening a command prompt and entering the following command: **`ipconfig /all`**

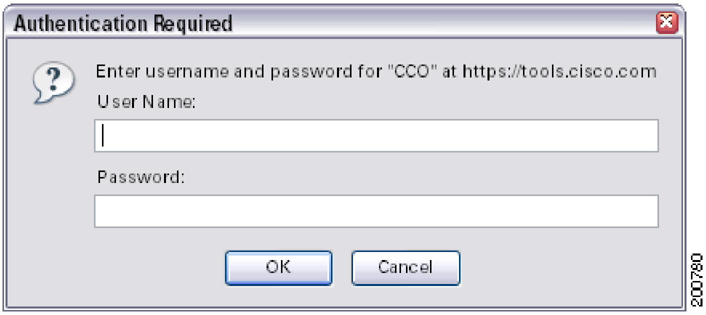
The value displayed in the Physical Address field is the MAC address of your machine.

Note If your machine has multiple MAC addresses, you can use any of them to obtain a runtime license. We recommend that you use a MAC address not associated with a remote VPN tunnel or a module you might remove in the future. If you later decide to run Cisco Monitor Manager on a different machine, or if you remove the hardware that corresponds to the MAC address under which you registered Cisco Monitor Manager under, you must contact Cisco Systems for a new license.

b. Obtain a Product Authorization Key (PAK) from either your reseller or your Cisco sales representative.

c. Launch the following URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

The Authentication Required dialog box appears.



Authentication Required

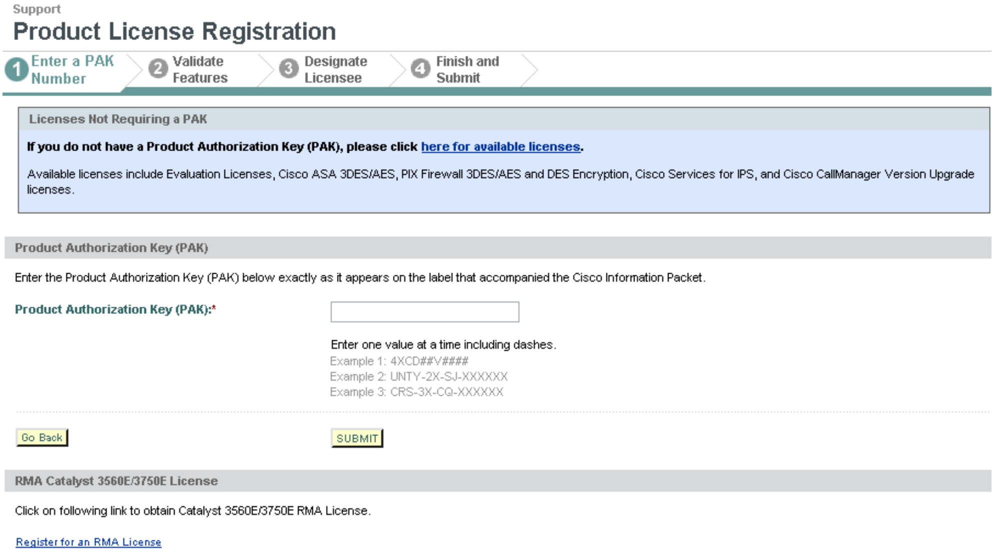
Enter username and password for "CCO" at https://tools.cisco.com

User Name:

Password:

d. Enter the username and password you use to log into Cisco.com, and then click **OK**. Note that you might be prompted to enter your username and password a second time.

The Product License Registration wizard is launched.



Licenses Not Requiring a PAK

If you do not have a Product Authorization Key (PAK), please click here for available licenses.

Available licenses include Evaluation Licenses, Cisco ASA 3DES/AES, PIX Firewall 3DES/AES and DES Encryption, Cisco Services for IPS, and Cisco CallManager Version Upgrade licenses.

Product Authorization Key (PAK)

Enter the Product Authorization Key (PAK) below exactly as it appears on the label that accompanied the Cisco Information Packet.

Product Authorization Key (PAK):*

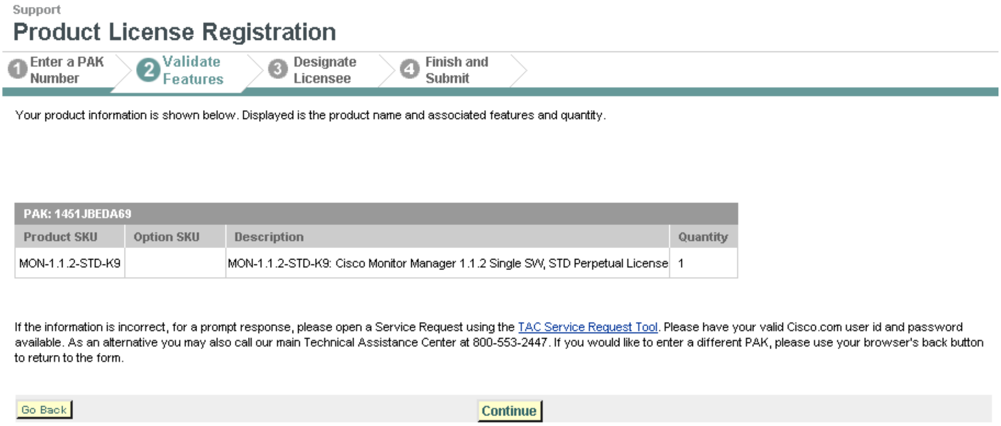
Enter one value at a time including dashes.
Example 1: 4XCD##V####
Example 2: UNTY-2X-SJ-XXXXXX
Example 3: CRS-3X-CQ-XXXXXX

RMA Catalyst 3560E/3750E License

Click on following link to obtain Catalyst 3560E/3750E RMA License.

Register for an RMA License

e. In the Product Authorization Key (PAK) field, enter the appropriate PAK, and then click **SUBMIT** to continue to the Validate Features wizard page.



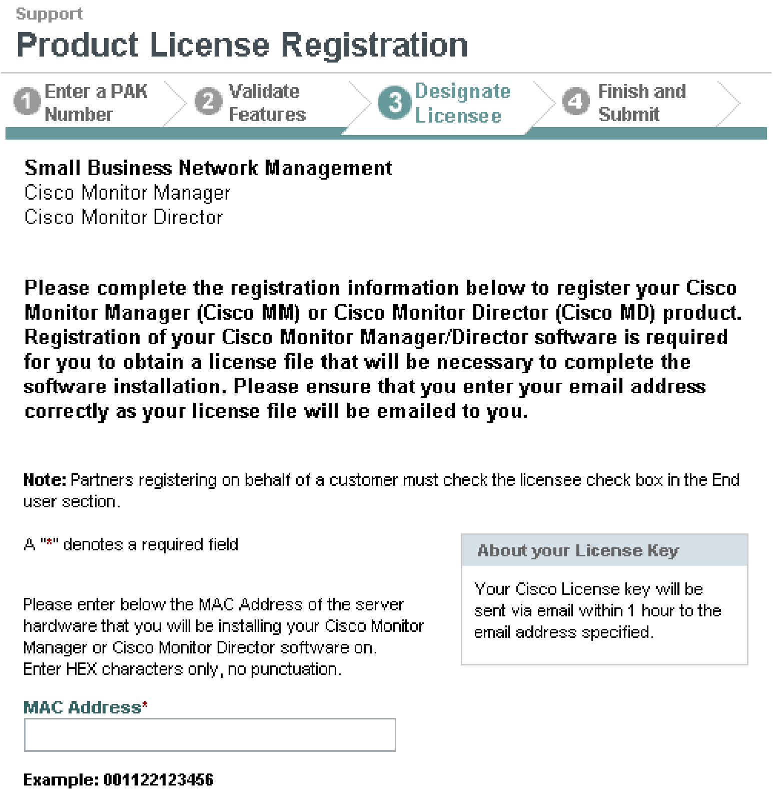
Your product information is shown below. Displayed is the product name and associated features and quantity.

PAK: 1451JBEDA69

Product SKU	Option SKU	Description	Quantity
MON-1.1.2-STD-K9		MON-1.1.2-STD-K9: Cisco Monitor Manager 1.1.2 Single SW, STD Perpetual License	1

If the information is incorrect, for a prompt response, please open a Service Request using the TAC Service Request Tool. Please have your valid Cisco.com user id and password available. As an alternative you may also call our main Technical Assistance Center at 800-553-2447. If you would like to enter a different PAK, please use your browser's back button to return to the form.

f. Verify that the correct product SKU for the version of Cisco Monitor Manager you purchased is displayed, and then click **Continue** to proceed to the Designate Licensee wizard page.



Support

Product License Registration

Small Business Network Management
Cisco Monitor Manager
Cisco Monitor Director

Please complete the registration information below to register your Cisco Monitor Manager (Cisco MM) or Cisco Monitor Director (Cisco MD) product. Registration of your Cisco Monitor Manager/Director software is required for you to obtain a license file that will be necessary to complete the software installation. Please ensure that you enter your email address correctly as your license file will be emailed to you.

Note: Partners registering on behalf of a customer must check the licensee check box in the End user section.

A "*" denotes a required field

Please enter below the MAC Address of the server hardware that you will be installing your Cisco Monitor Manager or Cisco Monitor Director software on.
Enter HEX characters only, no punctuation.

MAC Address*

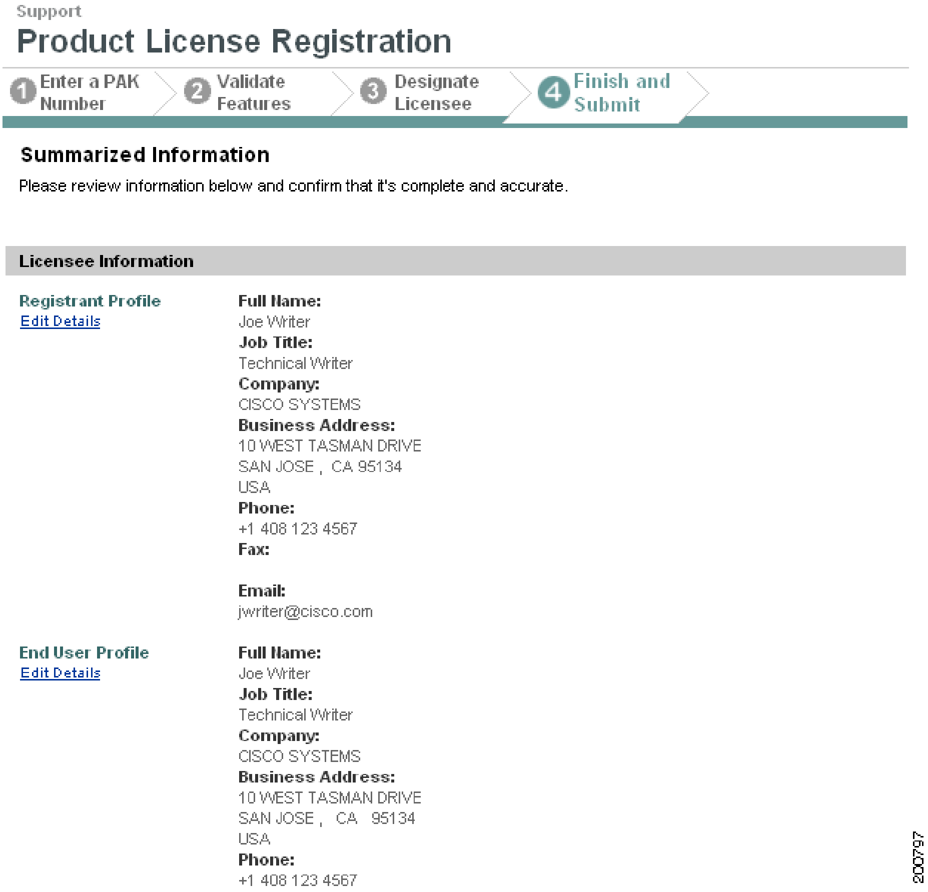
Example: 001122123456

About your License Key

Your Cisco License key will be sent via email within 1 hour to the email address specified.

g. Do the following, and then click **Continue** to proceed to the last wizard page:

- In the MAC Address field, enter the MAC address (dashes omitted) of the machine on which you will install Cisco Monitor Manager on.
- After reading the End-User License Agreement, select the Agreement check box to accept its conditions.
- Enter the appropriate contact information in the Registrant Information section of the page.
- If you are not the end-user of this Cisco Monitor Manager installation, select the Licensee (End-User) check box, and enter the appropriate contact information in the End User Information section of the page.



Summarized Information

Please review information below and confirm that it's complete and accurate.

Licensee Information

Registrant Profile
Edit Details

Full Name:
Joe Writer
Job Title:
Technical Writer
Company:
CISCO SYSTEMS
Business Address:
10 WEST TASMAN DRIVE
SAN JOSE , CA 95134
USA
Phone:
+1 408 123 4567
Fax:

Email:
jwriter@cisco.com

End User Profile
Edit Details

Full Name:
Joe Writer
Job Title:
Technical Writer
Company:
CISCO SYSTEMS
Business Address:
10 WEST TASMAN DRIVE
SAN JOSE , CA 95134
USA
Phone:
+1 408 123 4567

h. Verify that the information is accurate, and then click **Submit**.

The wizard page will indicate when registration is complete. Your runtime license will be sent to the e-mail address specified during registration. If you do not receive a license within 1 hour, open a service request using the TAC Service Request Tool.

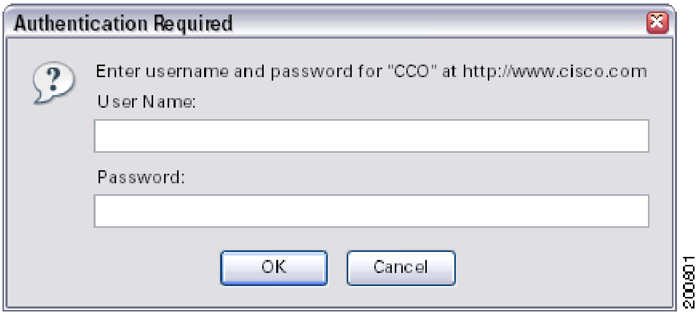
i. Save the runtime license onto your machine.

Step 2 Download the Cisco Monitor Manager installer file from Cisco.com.

Note If you have the Cisco Monitor Manager installation CD, skip this step and continue to Installing Cisco Monitor Manager, page 16.

a. Launch the following URL:
http://www.cisco.com/cgi-bin/tablebuild.pl/CiscoMM-crypto

The Authentication Required dialog box appears.



Authentication Required

Enter username and password for "CCO" at http://www.cisco.com

User Name:

Password:

b. Enter the username and password you use to log into Cisco.com, and then click **OK**.

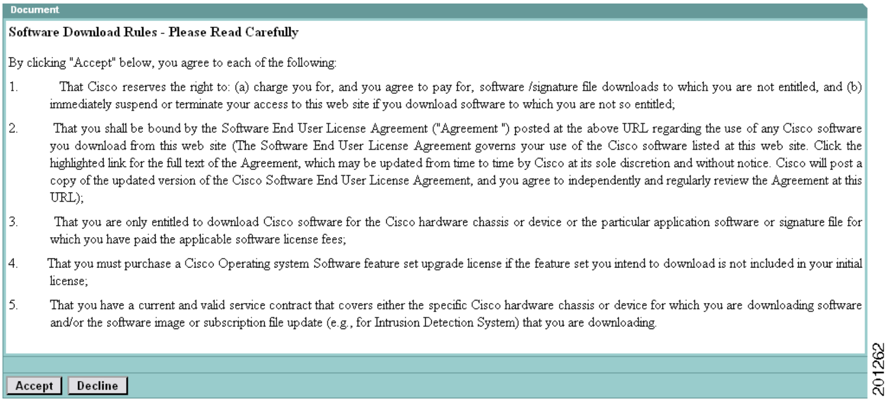
The Software Download page appears.

c. Click the **cisco-monitor-manager-1_1_2-win32-k9.exe** link.

The Software Download page is updated, displaying details for the software you will download.

d. Click **Next**.

The rules that apply to the download are displayed.



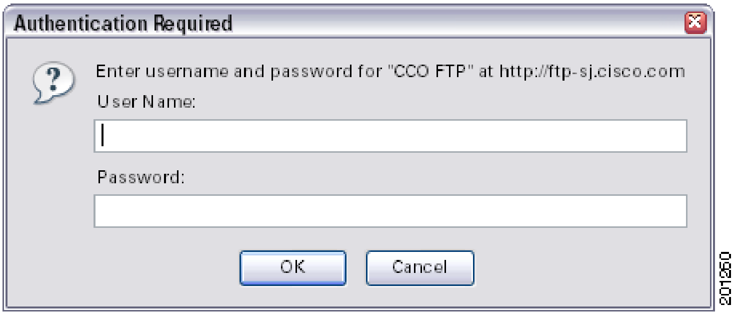
Software Download Rules - Please Read Carefully

By clicking "Accept" below, you agree to each of the following:

1. That Cisco reserves the right to: (a) charge you for, and you agree to pay for, software /signature file downloads to which you are not entitled, and (b) immediately suspend or terminate your access to this web site if you download software to which you are not so entitled;
2. That you shall be bound by the Software End User License Agreement ("Agreement ") posted at the above URL regarding the use of any Cisco software you download from this web site (The Software End User License Agreement governs your use of the Cisco software listed at this web site. Click the highlighted link for the full text of the Agreement, which may be updated from time to time by Cisco at its sole discretion and without notice. Cisco will post a copy of the updated version of the Cisco Software End User License Agreement, and you agree to independently and regularly review the Agreement at this URL);
3. That you are only entitled to download Cisco software for the Cisco hardware chassis or device or the particular application software or signature file for which you have paid the applicable software license fees;
4. That you must purchase a Cisco Operating system Software feature set upgrade license if the feature set you intend to download is not included in your initial license;
5. That you have a current and valid service contract that covers either the specific Cisco hardware chassis or device for which you are downloading software and/or the software image or subscription file update (e.g., for Intrusion Detection System) that you are downloading.

e. After reading through the rules, click **Accept** to accept their conditions.

The Authentication Required dialog box appears.



Enter username and password for "CCO FTP" at http://ftp-sj.cisco.com

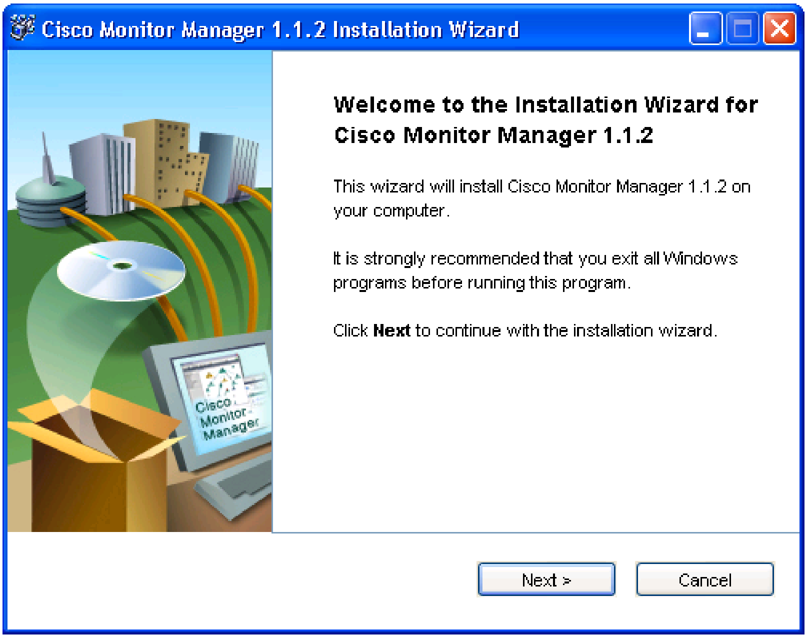
f. Enter the username and password you use to log into Cisco.com, and then click **OK**.

g. Save the Cisco Monitor Manager installer file onto your machine.

5 Installing Cisco Monitor Manager

Step 1 On your machine, navigate to and double-click **cisco-monitor-manager-1_1_2-win32-k9.exe** to launch the installation wizard.

The first wizard page appears.



Cisco Monitor Manager 1.1.2 Installation Wizard

Welcome to the Installation Wizard for Cisco Monitor Manager 1.1.2

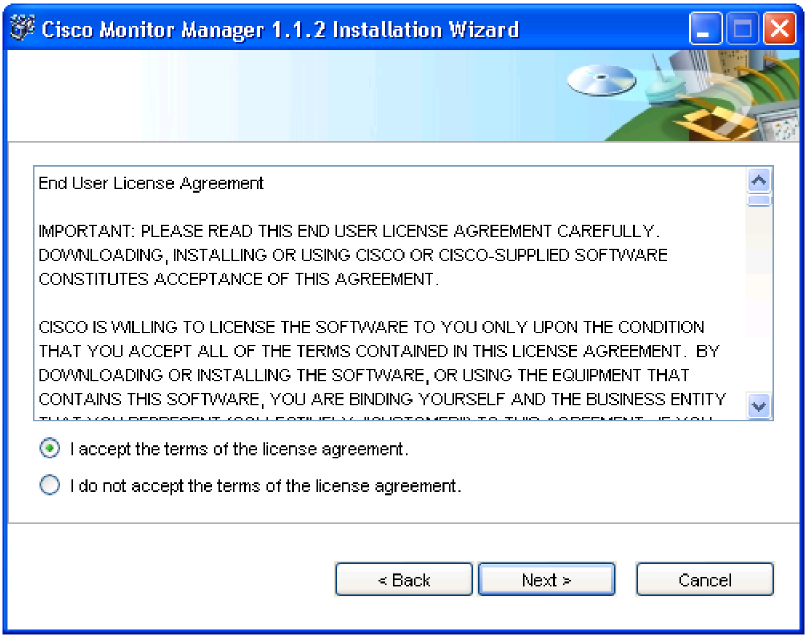
This wizard will install Cisco Monitor Manager 1.1.2 on your computer.

It is strongly recommended that you exit all Windows programs before running this program.

Click **Next** to continue with the installation wizard.

Step 2 Click Next.

The next wizard page appears, displaying the End User License Agreement.



End User License Agreement

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CISCO OR CISCO-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

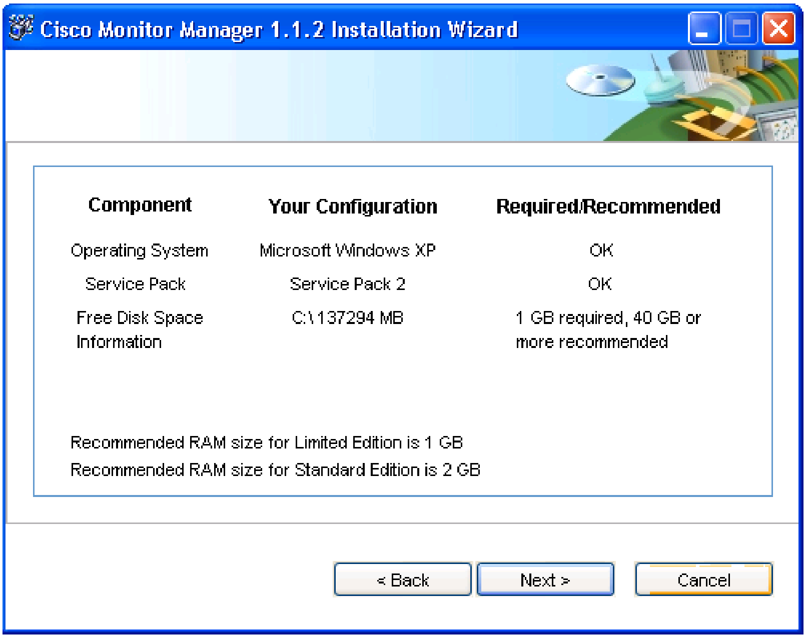
CISCO IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY

● I accept the terms of the license agreement.

○ I do not accept the terms of the license agreement.

Step 3 After reading the license agreement, click the **I accept the terms of the license agreement** radio button, and then click **Next**.

The next wizard page appears, showing the minimum disk space and RAM required to continue the installation.



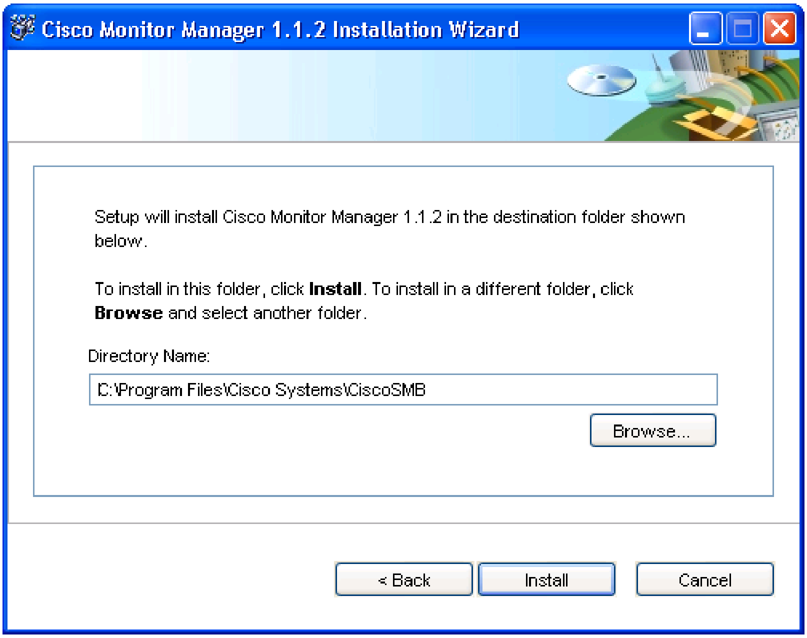
Component	Your Configuration	Required/Recommended
Operating System	Microsoft Windows XP	OK
Service Pack	Service Pack 2	OK
Free Disk Space Information	C:\ 137294 MB	1 GB required, 40 GB or more recommended

Recommended RAM size for Limited Edition is 1 GB

Recommended RAM size for Standard Edition is 2 GB

Step 4 Verify that your machine meets these requirements, and then click **Next**.

The next wizard page appears, prompting you to specify an installation directory. If you want to install Cisco Monitor Manager in the default directory, skip to Step 6. Otherwise, go to Step 5.



Setup will install Cisco Monitor Manager 1.1.2 in the destination folder shown below.

To install in this folder, click **Install**. To install in a different folder, click **Browse** and select another folder.

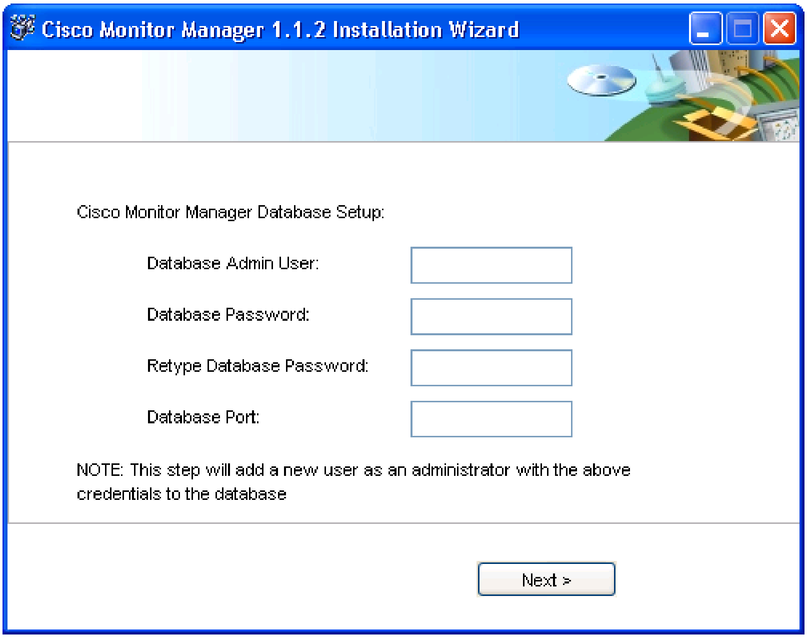
Directory Name: C:\Program Files\Cisco Systems\CiscoSMB

Step 5 Do one of the following:

- In the Directory Name field, enter the directory in which you want to install Cisco Monitor Manager.
- Click **Browse...** to navigate to the desired Cisco Monitor Manager installation directory, and then click **Open**.

Step 6 Click **Install**.

The next wizard page appears.



Cisco Monitor Manager 1.1.2 Installation Wizard

Cisco Monitor Manager Database Setup:

Database Admin User:

Database Password:

Retype Database Password:

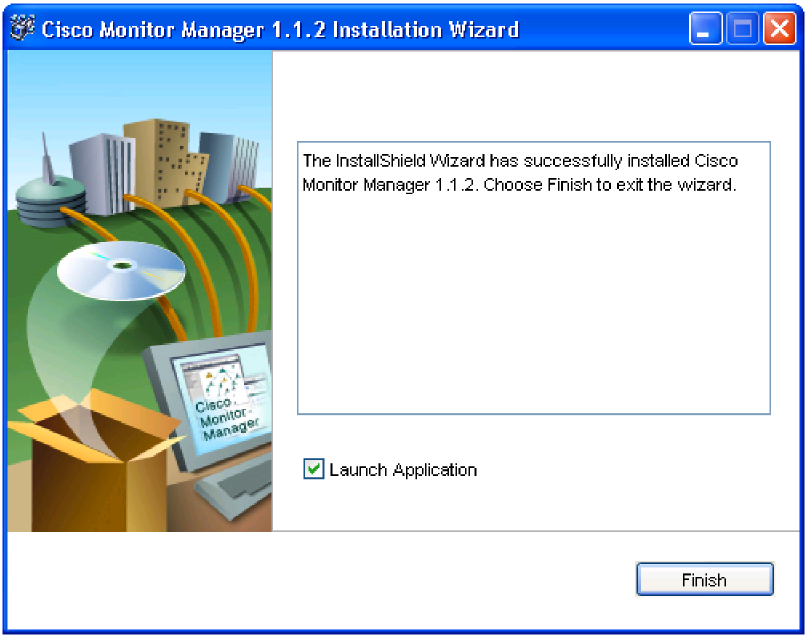
Database Port:

NOTE: This step will add a new user as an administrator with the above credentials to the database

Step 7 Enter the following information, and then click **Next:**

- Username and password required for Cisco Monitor Manager database access
- Number of the port assigned to the Cisco Monitor Manager database

Cisco Monitor Manager is installed.


Cisco Monitor Manager 1.1.2 Installation Wizard

The InstallShield Wizard has successfully installed Cisco Monitor Manager 1.1.2. Choose Finish to exit the wizard.

☑ Launch Application

Step 8 Click **Finish** to close the wizard and launch the License Registration page.

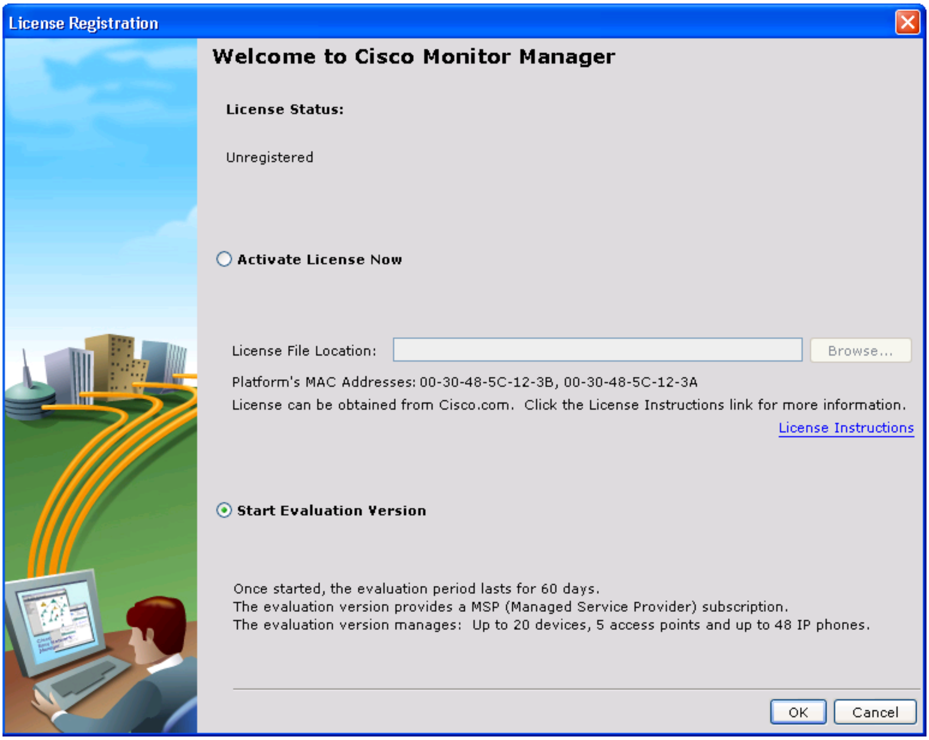
6 Post-Installation Tasks

After you install Cisco Monitor Manager, you must complete the following tasks before using the application for the first time:

1. Register Your Runtime License, page 22
2. Create a New Cisco Monitor Manager User, page 24
3. Discover Devices, page 27

Register Your Runtime License

Because this is the first time you have launched the application, the License Registration page appears.



Welcome to Cisco Monitor Manager

License Status:

Unregistered

○ Activate License Now

License File Location:

Platform's MAC Addresses: 00-30-48-5C-12-3B, 00-30-48-5C-12-3A

License can be obtained from Cisco.com. Click the License Instructions link for more information.

● Start Evaluation Version

Once started, the evaluation period lasts for 60 days.
The evaluation version provides a MSP (Managed Service Provider) subscription.
The evaluation version manages: Up to 20 devices, 5 access points and up to 48 IP phones.

Step 1 Select the **Activate License Now** radio button.

Step 2 Click **Browse...** to navigate to your runtime license, and then click **Open**.

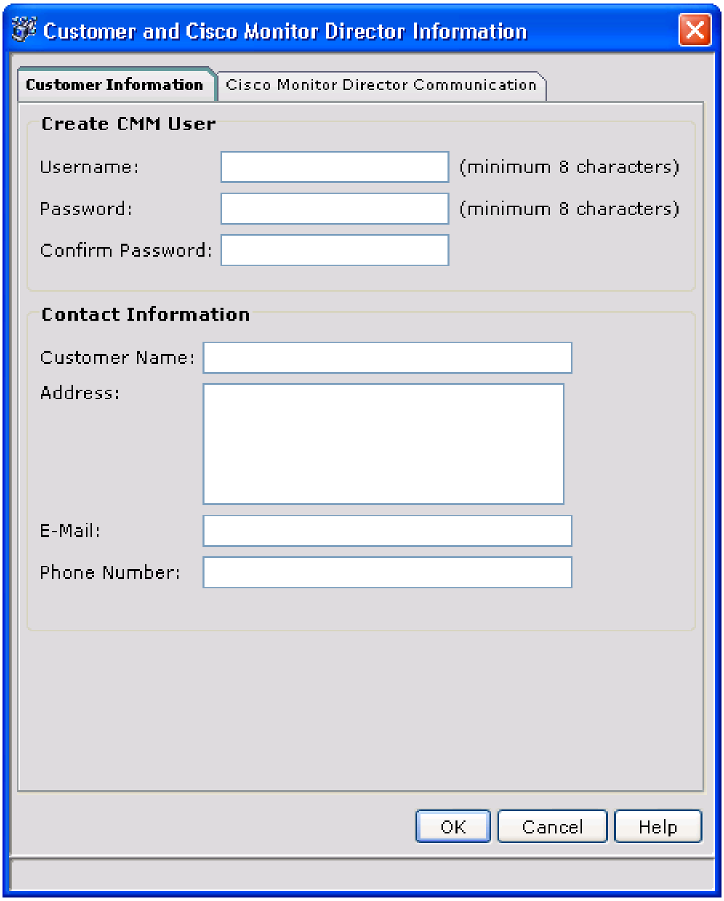
A message appears, stating that you have successfully registered your license.

Step 3 Click **OK** to close this message, and then click **OK** to launch the **Customer and Cisco Monitor Director Information** dialog box.

Note If you click **Cancel**, Cisco Monitor Manager closes. To access this page again, you must restart the application.

Create a New Cisco Monitor Manager User

After registering your runtime license, the Customer and Cisco Monitor Director Information dialog box appears. Here, you can enter the contact information for both yourself and your reseller (if applicable), as well as the information required to establish a connection between your Cisco Monitor Manager instance and the Cisco Monitor Director instance your reseller manages.



Customer and Cisco Monitor Director Information

Customer Information | Cisco Monitor Director Communication

Create CMM User

Username: (minimum 8 characters)

Password: (minimum 8 characters)

Confirm Password:

Contact Information

Customer Name:

Address:

E-Mail:

Phone Number:

Note the following:

- To proceed to the Discover Devices dialog box, you must enter the following information in the Customer Information tab: username, password, and customer name. You can enter the rest of the information for this tab and the Cisco Monitor Director Communication tab later in the Contact Information window (select **Administration** from the features pane, and then select **Options > Contact Information**) and the Cisco Monitor Director Information window (select Administration from the features pane, and then select **Options > Cisco Monitor Director**).
- You can configure additional Cisco Monitor Manager users later from the Application Access window (select **Administration** from the features pane, and then select **Application Access**).

Step 1 Enter the information specified in the following table.

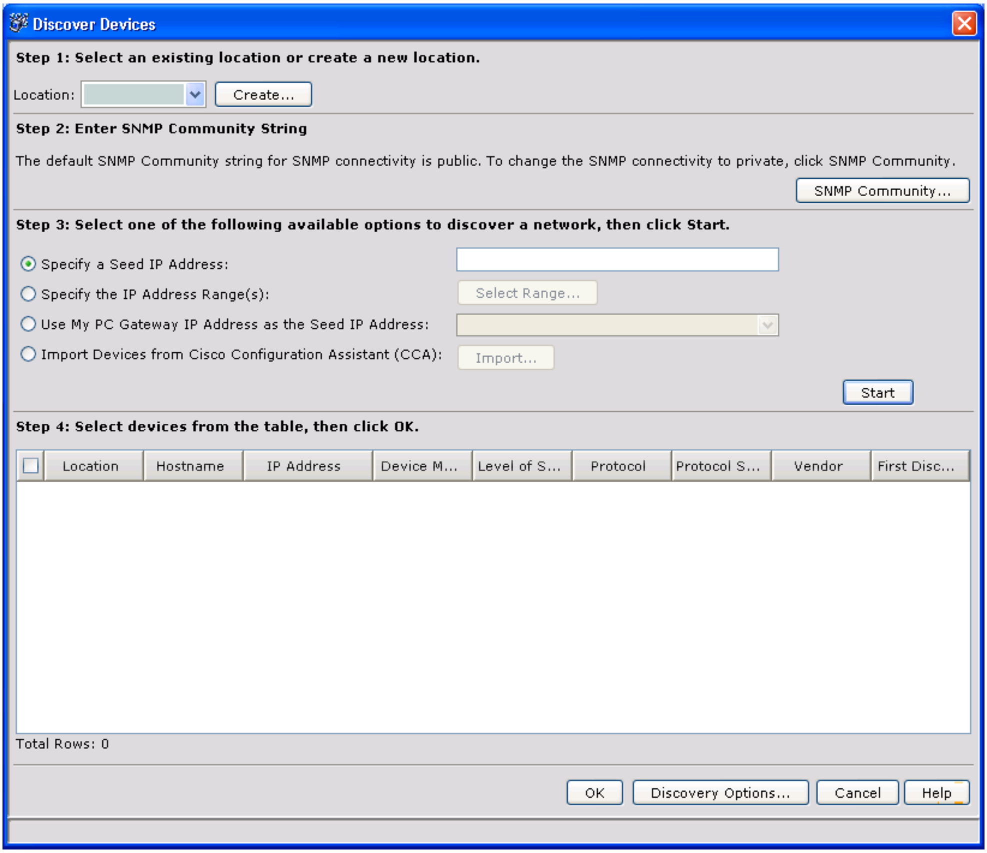
<table>
<tr><th>GUI Element</th><th>Action/Description</th></tr>
<tr><td colspan="2"><b>Customer Information tab: Create CMM User pane</b>
Valid Cisco Monitor Manager usernames and passwords meet the following criteria:
• Range from 8 to 80 characters in length
• Contain only characters from the struck ASCII set: In addition to letters (both lowercase and uppercase) and numbers, this set contains the following characters: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
• Are case sensitive
• Begin with a letter</td></tr>
<tr><td>Username field</td><td>Enter the username for a new Cisco Monitor Manager user.</td></tr>
<tr><td>Password field</td><td>Enter the password for this user.
To modify a user's password and privilege level later:
1. Select <b>Administration</b> from the features pane, and then select <b>Application Access</b>.
2. Select that user in the table, and then click <b>Edit...</b>.</td></tr>
<tr><td>Confirm Password field</td><td>Reenter the password you just entered.</td></tr>
</table>

GUI Element	Action/Description
Customer Information tab: Contact Information pane	
Enter the appropriate contact information for your company or organization.	
Cisco Monitor Director Communication tab: Contact Information pane	
If applicable, enter the appropriate contact information for your reseller.	
Cisco Monitor Director Communication tab: Cisco Monitor Director Communication pane	
Enable Communication with Cisco Monitor Director check box	Select to enable communication between this instance of Cisco Monitor Manager and your reseller's Cisco Monitor Director instance.
Reseller Console Address field	Enter the IP address of the machine on which Cisco Monitor Director is installed. If a port other than 443 is used for HTTPS on that machine, the value you enter here should be formatted as follows: *IP address:port number.*
Shared Key field	Enter the key required to establish a connection with your reseller's Cisco Monitor Director instance.
Confirm Shared Key field	Reenter the key required to establish a connection with your reseller's Cisco Monitor Director instance.
Customer ID field	Enter your customer identification string.
Test... button	After entering the information above, click to verify that a connection with your reseller's Cisco Monitor Director instance has been established.

Step 2 Click **OK** to close the dialog box and save your changes.

Discover Devices

After you complete the Customer and Cisco Monitor Director Information dialog box, the Discover Devices page appears. From here, you can discover new devices, import devices from Cisco Configuration Assistant (CCA), and select which devices are to be managed by Cisco Monitor Manager.



Step 1: Select an existing location or create a new location.

Location:

Step 2: Enter SNMP Community String

The default SNMP Community string for SNMP connectivity is public. To change the SNMP connectivity to private, click SNMP Community.

Step 3: Select one of the following available options to discover a network, then click Start.

● Specify a Seed IP Address:

○ Specify the IP Address Range(s):

○ Use My PC Gateway IP Address as the Seed IP Address:

○ Import Devices from Cisco Configuration Assistant (CCA):

Step 4: Select devices from the table, then click OK.

□	Location	Hostname	IP Address	Device M...	Level of S...	Protocol	Protocol S...	Vendor	First Disc...

Total Rows: 0

Step 1 Click **Create...** to launch the Create New Location dialog box and configure a new device location.

A device location simply indicates where a group of devices is physically located.

Step 2 Enter the name and description of a new device location, and then click **OK**.

By default, the community strings used by Cisco Monitor Manager for SNMP connectivity are *public* (read-only) and *private* (read-write). If you want to change these strings, click **SNMP Community...** and proceed to Step 3. Otherwise, skip ahead to Step 4.

Note If the SNMP community strings configured for a device are different from the default strings, you will not be able to back up or restore the configuration settings for that device.

Step 3 Modify the default SNMP community strings:

a. Select the table entry, and then click **Edit...**. The Edit SNMP Community String dialog box appears.

b. In the Read String and Write String fields, enter the appropriate strings, and then click **OK**.

c. Click **OK** to close the SNMP Community Strings dialog box.

Step 4 Select one of the following radio buttons:

- Specify a Seed IP Address: Select to discover all devices associated with the device you enter here.
- Specify IP Address Range: With this radio button selected, do the following:
  - Click **Select Range...** to launch the Select Range window.
  - Click **Add...** to launch the Add Range window.
  - Specify the IP address range you want to add.

    If you click the **Enter Range** radio button, enter the first and last IP address in the range.

    If you click the **Enter Subnet** radio button, enter an IP address and the subnet mask to which that address belongs. Cisco Monitor Manager will discover all devices that belong to that subnet mask.

- Specify the location of the devices covered by this address range. Either select an existing device location from the Location list or configure a new location by clicking **Create...**.
- Enter a short description of this address range.
- Click **OK**.

- Use My PC Gateway IP Address as the Seed IP Address: Select your machine's gateway IP address from the list to discover your machine as well as its four-hop neighbor devices (connected via ARP or CDP).

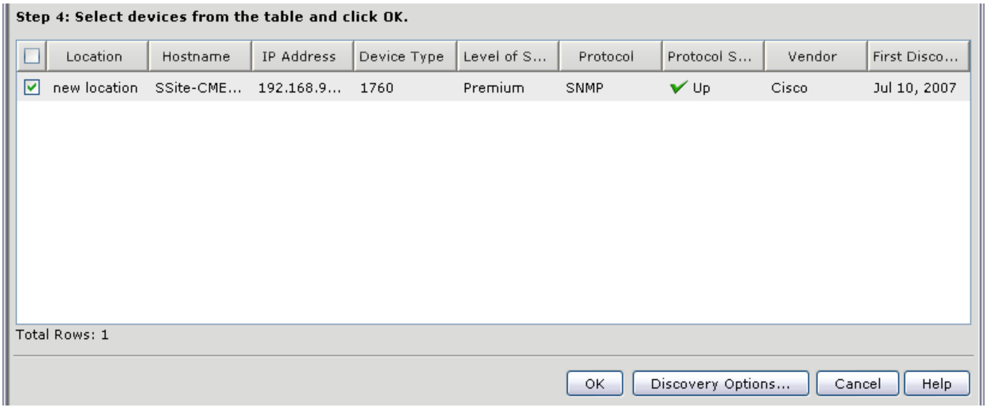
Note If Cisco Security Agent is running on your machine, your machine's gateway IP address will not be displayed. To work around this problem, close the Discover Devices window, disable Cisco Security Agent, and then reopen the Discover Devices window.

- Import Devices from Cisco Configuration Assistant (CCA): With this radio button clicked, do the following:
  - Click **Import...** to launch the Import CCA Communities dialog box.
  - Click **Browse...** to navigate to the directory that contains your CCA community files.
  - Select the appropriate file, and then click **Open**.
  - Select the community from which you want to import devices, and then click **OK**.

    Note that this feature is available only when CCA and Cisco Monitor Manager are installed on the same machine.

Step 5 Click **Start** to begin discovery.

The table at the bottom of the page is populated with the devices that Cisco Monitor Manager has discovered.



Step 4: Select devices from the table and click OK.

□	Location	Hostname	IP Address	Device Type	Level of S...	Protocol	Protocol S...	Vendor	First Disco...
☑	new location	SSite-CME...	192.168.9...	1760	Premium	SNMP	✓ Up	Cisco	Jul 10, 2007

Total Rows: 1

Step 6 Select the check box for every device you want to manage, and then click **OK**.

Discovery continues; after it is complete, the topology map displays the devices you selected.

Tip To quickly select all of the devices in the table that Cisco Monitor Manager can manage, select the check box at the top of the first column.

Note the following when discovering devices:

- The maximum number of devices Cisco Monitor Manager can manage are as follows:
  - Evaluation version: 20 networking devices, 5 access points, and 48 IP phones
  - Limited version: 25 networking devices and 48 IP phones
  - Standard version: 70 networking devices and 250 IP phones
- Cisco Monitor Manager treats a stack device as a single device, regardless of the number of member devices associated with a master device.

- If Cisco Monitor Manager cannot establish a connection with a device, there are several common causes:
  - Incorrect device credentials have been entered.
  - A timeout has occurred on the device.
  - There is an insufficient number of available vty lines on the device.
  - The device does not have network connectivity.
- To see the list of devices that Cisco Monitor Manager supports, see *Supported Devices Table for Cisco Monitor Manager 1.1.2*.
- There might be times when several devices in your network have the same IP address. (This will most likely happen when you dismantle the devices in a stack device.) As a result, the information displayed for a particular device might actually be the information collected from another device with an identical IP address. To avoid this:
  - Make sure that the IP addresses of network devices are unique.
  - When dismantling a stack device, remove the stack device from Cisco Monitor Manager management, and then rediscover the individual devices.
- You cannot use CDP to discover Cisco ASA and Cisco PIX devices. To add these types of devices to your network:

Step 1 Select **Setup** from the features pane, then select **Add Device** to launch the Add Device wizard.

Step 2 Specify where you want to add a device. Do one of the following:

- Select an existing device location from the Location list.
- Configure a new device location by clicking **Create...**.

Step 3 Enter the IP address of the device to add to the network.

Step 4 Select *HTTPS* as the management protocol for this device, then click **Next >**.

An alert appears, asking whether you want to accept the security certificate for the device.

Step 5 Click **Yes**.

The Device Authentication dialog box appears.

Step 6 Enter the username and password required for Level 15 access on this device, then click **OK**.

Step 7 If Cisco Monitor Manager successfully established an HTTPS connection with the device, click **Finish**. Otherwise, click **Cancel** and try to add the device again later.

7 Additional Information

This section provides information on the following topics:

- Backing Up the Cisco Monitor Manager Database, page 32
- Restoring the Cisco Monitor Manager Database, page 33
- Cisco ASA/Cisco PIX Device Support, page 30

Backing Up the Cisco Monitor Manager Database

Step 1 Verify that Cisco Monitor Manager is running.

Step 2 On the machine on which Cisco Monitor Manager is installed, launch a command prompt.

a. From the Windows taskbar, select **Start > Run...**. The Run dialog box appears.

b. Enter the following command, and then click **OK**: **`cmd`**

Step 3 Navigate to the directory that contains your database information by entering the following command:

```
cd <Cisco Monitor Manager installation directory>\mysql\bin
```

Step 4 Back up your database by entering the following command:

```
backup_CiscoMM.cmd localhost <username> <password> ciscomm <backup directory>
```

where *username* and *password* are the username and password required for Adminstrator privileges on this Cisco Monitor Manager instance.

For example, let's assume that the Administrator username is *admin* and that the password is *allaccess*. If you want to back up your database information in a folder named "10082007" on your C: drive, you would enter:

```
backup_CiscoMM.cmd localhost admin allaccess ciscomm C:\10082007
```

The file ciscomm.sql, which contains your network's database information, is now available in the backup directory you specified.

Note Backing up your database is CPU intensive. It will take longer than usual to launch an application window until the database backup is complete.

Restoring the Cisco Monitor Manager Database

Step 1 Shut down Cisco Monitor Manager.

Step 2 On the machine on which Cisco Monitor Manager is installed, launch a command prompt.

a. From the Windows taskbar, select **Start > Run...**. The Run dialog box appears.

b. Enter the following command, and then click **OK**: `cmd`

Step 3 Navigate to the directory that contains your database information by entering the following command:

```
cd <Cisco Monitor Manager installation directory>\mysql\bin
```

Step 4 Restore your database by entering the following command:

```
restore_CiscoMM.cmd localhost <username> <password> ciscomm <backup
directory>\ciscomm.sql
```

where *username* and *password* are the username and password required for Adminstrator privileges on this Cisco Monitor Manager instance.

For example, let's assume that the Administrator username is *admin* and that the password is *allaccess*. If you backed up your network's database information in a folder named "10082007" on your C: drive, you would enter the following to restore that information:

```
restore_CiscoMM.cmd localhost admin allaccess ciscomm C:\10082007\ciscomm.sql
```

Step 5 Restart Cisco Monitor Manager and verify that the database information is correct.

Cisco ASA/Cisco PIX Device Support

When Cisco Adaptive Security Appliances (Cisco ASA) and Cisco PIX devices are present in a network managed by Cisco Monitor Manager, note the following:

- Cisco Monitor Manager fully supports only the following Cisco ASA and Cisco PIX devices running in routed, single-context mode with any software version from 7.0 through 8.0 installed:
  - Cisco ASA 5505
  - Cisco ASA 5510
  - Cisco PIX 515E

  Devices running in transparent mode or running multiple contexts will only allow either Cisco Adaptive Security Device Manager (Cisco ASDM) or Cisco PIX Device Manager (Cisco PDM) to be launched.
- Cisco ASA and Cisco PIX device failover pairs have not been tested. As a result, we cannot guarantee that Cisco Monitor Manager can configure or monitor the active device of a failover pair. In addition, you should not use Cisco Monitor Manager to configure or monitor the standby device.
- Although Cisco Monitor Manager can access and monitor Cisco ASA, Cisco Firewall Services Module (Cisco FWSM), or Cisco PIX devices via SNMP, for security reasons we recommend that you use HTTPS instead. To enable management access to a device, launch the Cisco ASDM Management Access panel and specify the IP address of the machine on which Cisco Monitor Manager is installed to enable communication between the two.
  - By default, HTTPS service runs on port 443.
  - On Cisco ASAs running software version 7.0, 7.1, or 7.2, Clientless SSL VPN requires that Cisco ASDM access be configured with an HTTPS port other than 443, which prohibits Cisco Monitor Manager connections. Note that this does not apply to Cisco ASAs running software version 8.0.
  - You cannot monitor Clientless SSL VPN with Cisco Monitor Manager.
  - If Cisco Monitor Manager must communicate with a device through a VPN tunnel, then the management interface that can be reached through that tunnel must be configured for management access. To enable management access, enter the following CLI command, where *interface* is the nameif identifier assigned to an interface:

    ```
    management-access interface
    ```
- If a Cisco ASA 5505 or Cisco PIX 501 device is configured for either a remote-access or remote-client VPN rather than a site-to-site IPSec VPN, Cisco Monitor Manager does not recognize the remote access tunnel. However, Cisco Monitor Manager can still contact a management interface through that tunnel.

- Unless a Cisco ASA or Cisco PIX device is configured to allow ICMP responses, a firewall responds to ping and other ICMP requests by default. As a security measure, a fully functional firewall might not appear to be available on a network, even though Cisco Monitor Manager can access it.
- We recommend that you use Cisco ASDM to configure Cisco Monitor Manager access on supported Cisco ASAs or Cisco PIX devices. Cisco ASDM provides wizards for setting up these devices and establishing VPN connections with them.

See the following for more information on this topic:

- *Supported Devices Table for Cisco Monitor Manager 1.1.2*: Provides device support information for this release.
- "Accessing Cisco Device Managers" online help topic: Provides links to the documentation for the various Cisco device managers you can launch from Cisco Monitor Manager.

8 Where to Go Next

For more information on Cisco Monitor Manager, see the following documentation:

- *Release Notes for Cisco Monitor Manager 1.1.2* describes known product bugs and their workarounds (if available).
- The context-sensitive online help describes the features provided in this release.

Note Although every effort has been made to validate the accuracy of the information in the electronic documentation, you should also check Cisco.com for any updates.

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

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 800 020 0791
Fax: 31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

♻ Printed in the USA on recycled paper containing 10% postconsumer waste.