EMC²
where information lives®

# EMC Email Home for Cisco MDS and Nexus Switches

Version 5.0(4a)

Background:

EMC Email Home provides intelligent monitoring and event notification for Cisco MDS and Nexus switches.   EMC Email Home combined with ESRS (EMC Secure Remote Support) Gateway provides customers with secure high-speed and proactive around-the-clock remote monitoring and support of their EMC Cisco switches. This guide provides information on installation and troubleshooting EMC Email Home on Windows platforms. EMC Email Home can be installed on other operating systems (see list below). These instructions, while created for Windows installations, can be used with a few modifications to successfully install EMC Email Home on other operating systems. For a more in-depth explanation of EMC Email Home, ESRS Gateway, or EMC's remote support services; please contact your local EMC support provider.

How EMC Email Home Works

Traps from all monitored Cisco switches are forwarded to the Cisco Fabric Manger. Cisco Fabric Manager identifies traps of interest to EMC Email Home and generates the appropriate xml email messages that are forwarded to EMC. These emails, once received at EMC, are processed and turned into EMC Support Cases which are then handled by the appropriate EMC personnel. If necessary, customers are contacted and updated on the cases created and the actions to be taken to resolve any issues. Customers can also choose to be notified on events by Fabric Manager.
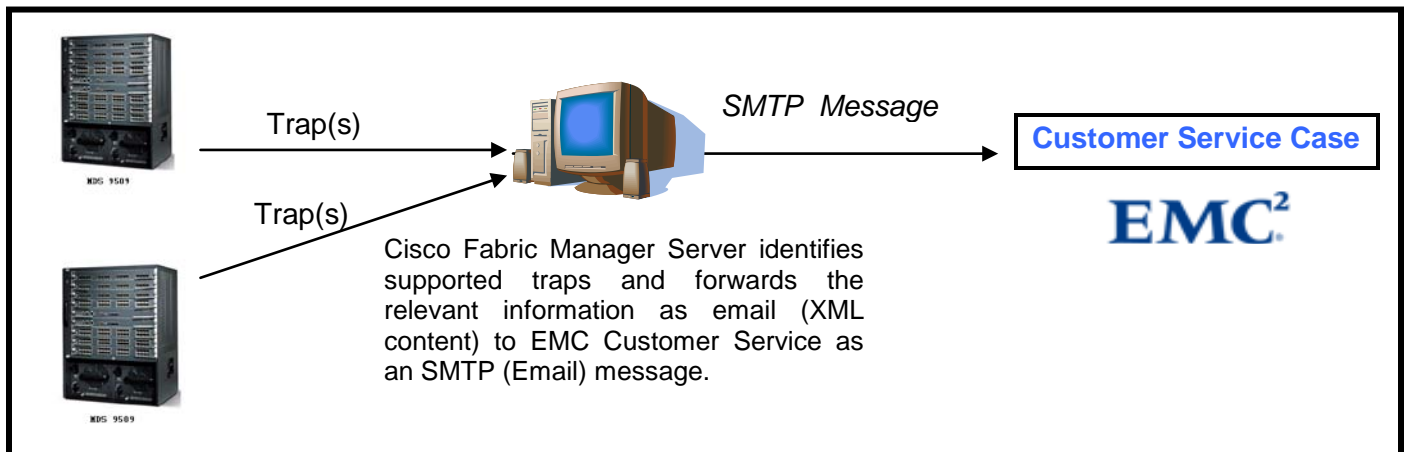
Notes about this version

- 9100 series switches manufactured after May '07 (those with JA* as a secondary serial number) are supported.
- Nexus N5K switches are supported with NX-OS 4.2(1)N1(1) or higher.

- Limited ConnectEMC/FM support for modem use only. Please refer to Customer Service Procedure CON-CSP-05.

Documentation changes

Fabric Manager now has its own version of Release Notes that support both Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. These release notes cover known caveats, platform requirements, and new features and functionality. As with the NX-OS Release notes, EMC has a version that contains supplemental and EMC specific information on http://Powerlink.emc.com , and the Cisco release notes can be obtained from the following website:
http://www.cisco.com/en/US/products/ps10495/tsd_products_support_series_home.html

Location of Cisco Fabric Manager Documentation

Documentation for Cisco Fabric Manager has moved to the Network Management location on Cisco.com. Starting with Fabric Manager Release 4.2(1a), you can access Fabric Manager documentation by going to Cisco.com and selecting **Support**, **Select a Product**, **Products**, **Network Management**, **Data Center Management**, **Cisco Fabric Manager**.

Upgrade Instructions

Upgrading Fabric Manager is only supported when upgrading from Fabric Manager 3.2(1a) and above. The configuration settings for Email Home lost by doing a fresh install are minimal and the importance of correctly configuring the monitoring of the switch is critical. For those prior versions, please remove your previous version of Fabric Manager and follow the **New Installation Instructions** noted below.

If you are at Fabric Manager 3.2(1a) or above and upgrading, follow the new installation instructions below and instead click "**Yes**" on the dialog that asks "**Cisco Fabric Manager is already installed. Do you want to upgrade it?**" Follow the prompts provided and Fabric Manager should upgrade correctly. Keep in mind that some selections will be filled in or grayed out due to the upgrade to preserve your prior install choices. If you run into any problems with the upgrade, please remove Fabric Manager Server and follow the **New Installation Instructions** below instead. All necessary settings used for Email Home should be carried forward on the upgrade.

In order to monitor for port related events, both the switch and Fabric Manager have to be on specific code and require special configuration.   The switch must be running SAN-OS 3.3(3) or above, or NX-OS 4.1(1b) and above with Fabric Manager 4.1(3a) or above to correctly configure for port events.   The new code and Fabric Manager are required to use delayed traps which stops invalid notifications for host reboots. Please see the instructions in the **New Installation Instructions** section to turn on delayed traps if you are upgrading from a previous version.

About Delayed Traps

In previous code versions, Fabric Manager listened to interface traps and generated EMC Email Home email messages immediately. Link traps are generated when an interface goes to down from up or vice versa. These link traps can be initiated for both real failures and other conditions. Link traps are created are created when a scheduled server reboot happens. EMC Email Home via Fabric Manager monitors these link traps and generates an email notification on them.   The alerts from servers reboots can and did created multiple invalid service requests. These invalid service requests made finding real port issues extremely difficult. A better way was needed to filter out these invalid alerts and concentrate on real port issues.

Cisco SAN-OS 3.3(3) and above, and NX-OS Release 4.1(1b) and above provides the ability to generate a delayed trap so that invalid alerts for host reboots is removed or at least minimized. Delayed traps filters server reboots and avoids generating unnecessary EMC Email Home email messages. This feature is applicable only for F/FL ports. When a switch is configured to use the delayed traps feature, instead of generating the trap immediately after the F/FL port goes down, the switch waits for the specified delay timer (default = 4mins) and then sends the trap. If the port comes back up in the specified timer value, the trap is not sent. This reduces the number of emails generated and intervention of customers and EMC Support. Users have the ability to select the current existing feature or this new delayed trap feature. Delayed traps can be enabled using both Cisco Fabric Manager and the CLI.

New Installation Instructions

Installation Changes for Cisco Fabric Manager in This Release

If you plan to make use of the Fabric Manager Server federation feature, then you need to follow a slightly different installation procedure for Cisco Fabric Manager. For more information, refer to the *Cisco Fabric Manager Fundamentals Configuration Guide* and the *Cisco Fabric Manager Server Federation Deployment Guide* located at http://www.cisco.com/en/US/products/ps10495/tsd_products_support_series_home.html.

If you do not plan to install a federation of servers, then the installation procedure is unchanged from Cisco Fabric Manager Release 4.1(3b).

Installation Instructions

It is recommended that Cisco Fabric Manager Server be deployed on a dedicated physical or virtual server. Cisco Fabric Manager is a Java based application that can be deployed on any platform that has the Java Runtime Environment (JRE). This document assumes Cisco Fabric Manager running on a Microsoft Windows platform. Other operating systems such as Linux should work but are not documented within this document. See the *Cisco Fabric Manager Fundamentals Configuration Guide* for details on installing Fabric Manager Server on other operating systems. Fabric Manager has been tested in the following configurations:

Operating System Version	Java Version [1]	Browser Version
Windows 2003 and SP2	1.5 or 1.6	Internet Explorer 6
Windows 2003 and SP2	1.5 or 1.6	Internet Explorer 7
Windows 2003 and SP2	1.5 or 1.6	Firefox 3.0
Windows XP SP2 and SP3	1.5 or 1.6	Internet Explorer 6
Windows XP SP2 and SP3	1.5 or 1.6	Internet Explorer 7
Windows XP SP2 and SP3	1.5 or 1.6	Firefox 3.0
Windows Vista SP1 without UAC	1.5 or 1.6	Internet Explorer 7
Windows 2008 SP2 (32-bit and 64-bit)[2]	1.6	
Red Hat Enterprise Linux AS Release 5	1.5 or 1.6	Firefox 3.0
Solaris 9	1.5 or 1.6	Packaged with default Solaris 9
Solaris 10	1.5 or 1.6	Firefox 3.0

---

[1] Do not use Java update 1.6.13 or 1.6.14.

[2] Can be used only as a Fabric Manager Server.

Note: *For large fabrics, it is highly recommended that Cisco Fabric Manager Server be run on a Dual Processor Server with at least 2 Gigs of RAM and 10 GB free space. While this configuration should be able to monitor all configured Fabrics, there may be a limit to the number of fabrics that can be monitored depending on a variety of factors. If a limit is reached, additional hosts with Fabric Manager installations may be required.*

Step 1: The EMC Customer Engineer for the account should be contacted to ensure that ALL switches purchased through EMC, especially the ones to be monitored, have been correctly installed in the appropriate EMC databases. Any switch not correctly installed will have all the emails for it disregarded automatically and therefore the notifications will not be received at EMC Support.

Step 2: Collect a list of the switches you want to have monitored by email home, their IP addresses, the SMTP gateway that will be used, the IP address of the server running Fabric Manager, and an email address you want to have test emails sent to.

Step 3: Install Fabric Manager 5.0(4a) server service on the host that will be dedicated to monitoring the switches. Users installing Fabric Manager must have full administrator privileges to create user accounts and start services. Users should also have access to all ports. These are the ports used by Fabric Manager Server and the PostgreSQL database: 1098, 1099, 4444, 4445, 8009, 8083, 8090, 8092, 8093, 514, and 5432.

You will also need the CD that shipped with the switch or have downloaded the zip file from EMC's PowerLink. If you download the zip file from PowerLink, make sure you unzip the files keeping the directory structure when you do. The unzipped files or the CD should look like the following.
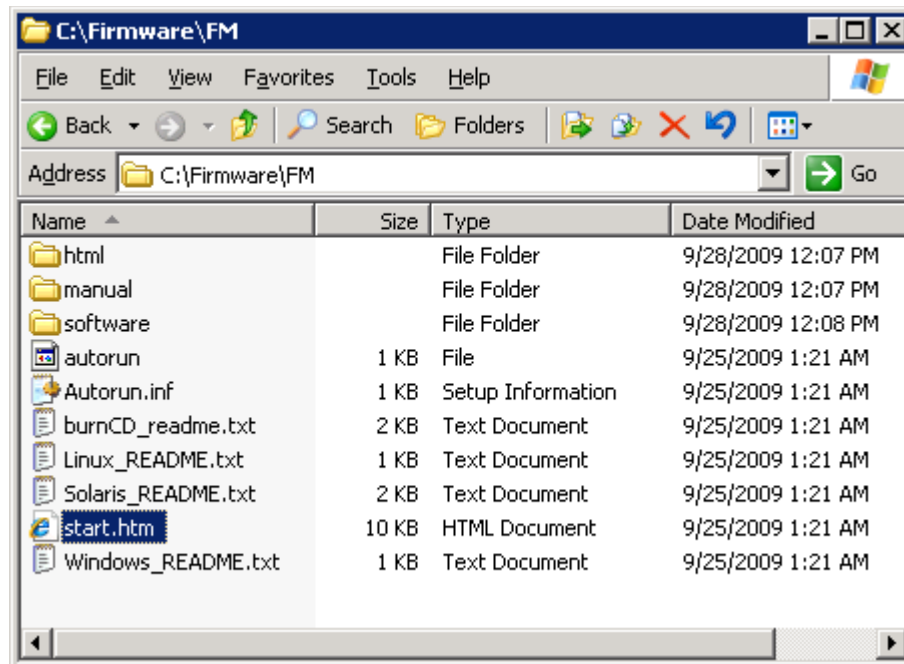

Double click on the "start.htm" icon. The following screen should come up. If you see a warning message indicating active content has been restricted on this computer. Right click on this warning message and select "Allow Blocked Content"
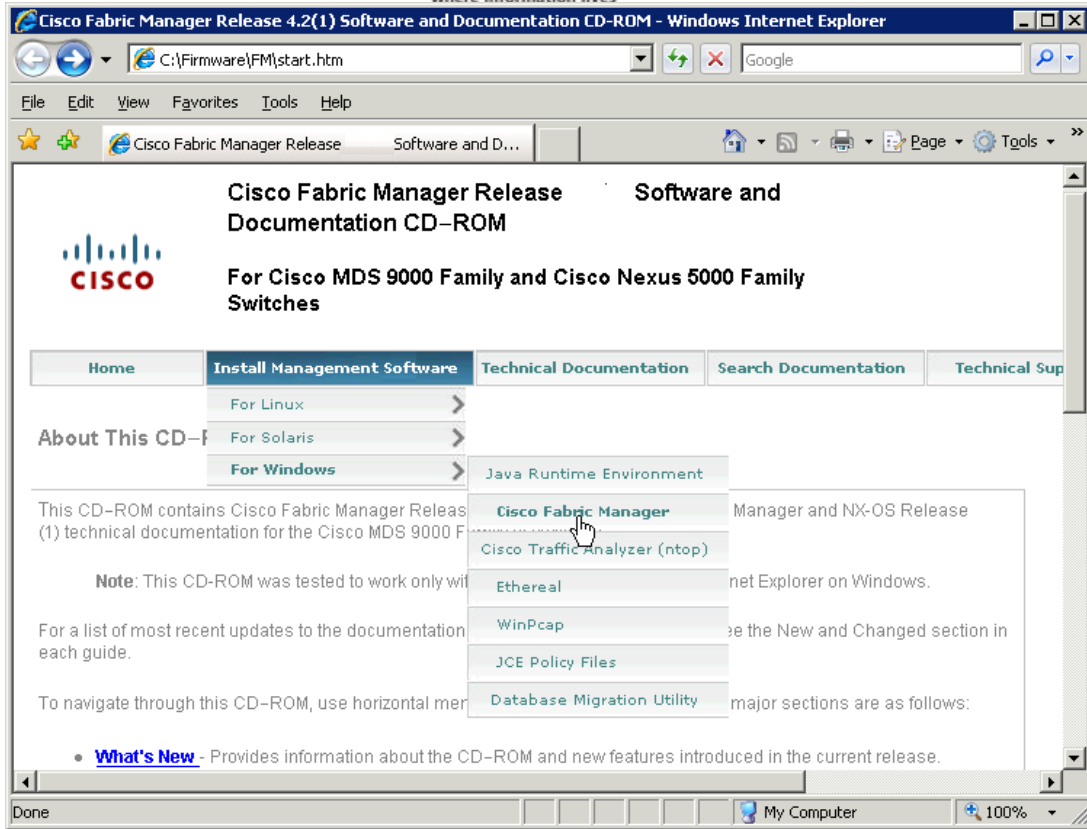
Navigate to "Install Management Software", "For Windows", and select "Cisco Fabric Manager".

Read the notes on the next web page that comes up. Ensure that you have JRE 1.5x or 1.6x (1.6.12 or below) installed on the host and the correct permissions as previously noted.
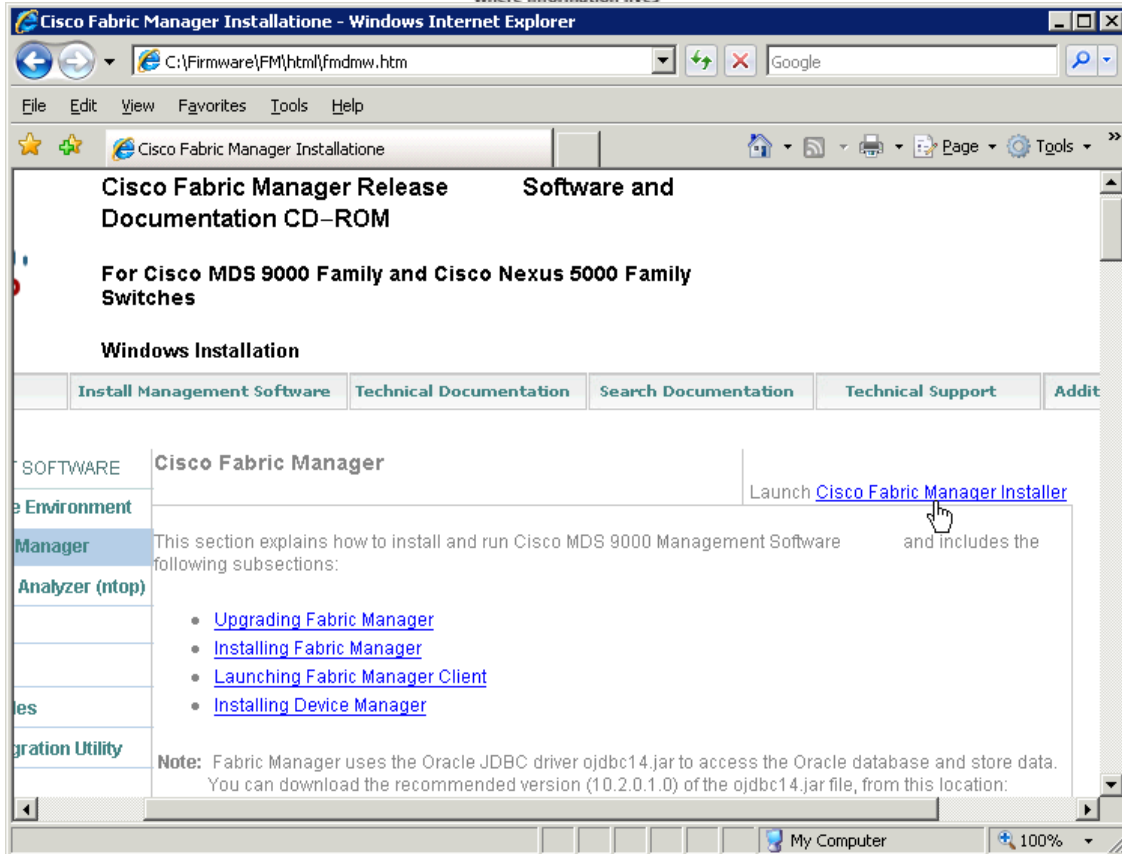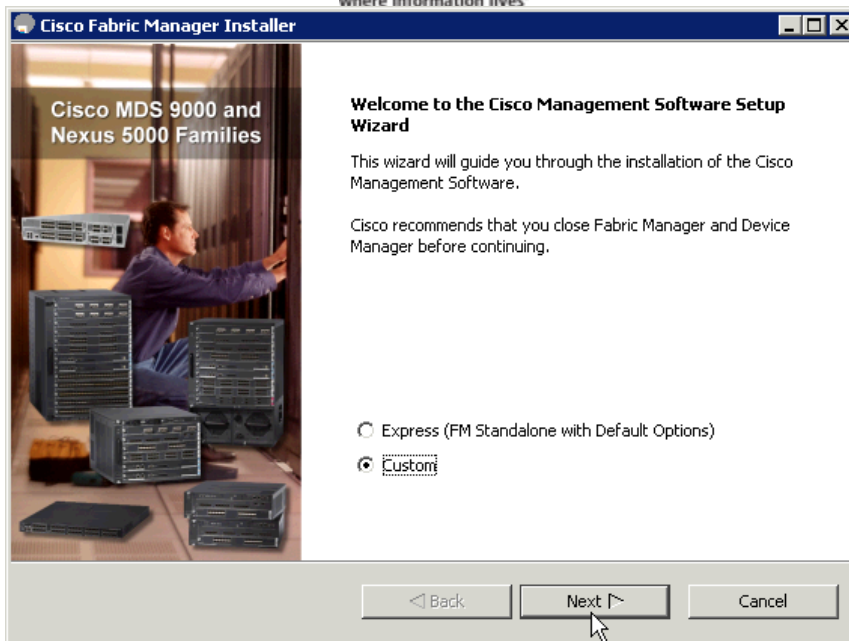
Ensure you comply with the notes then Click on the selection "Cisco Fabric Manager Installer".
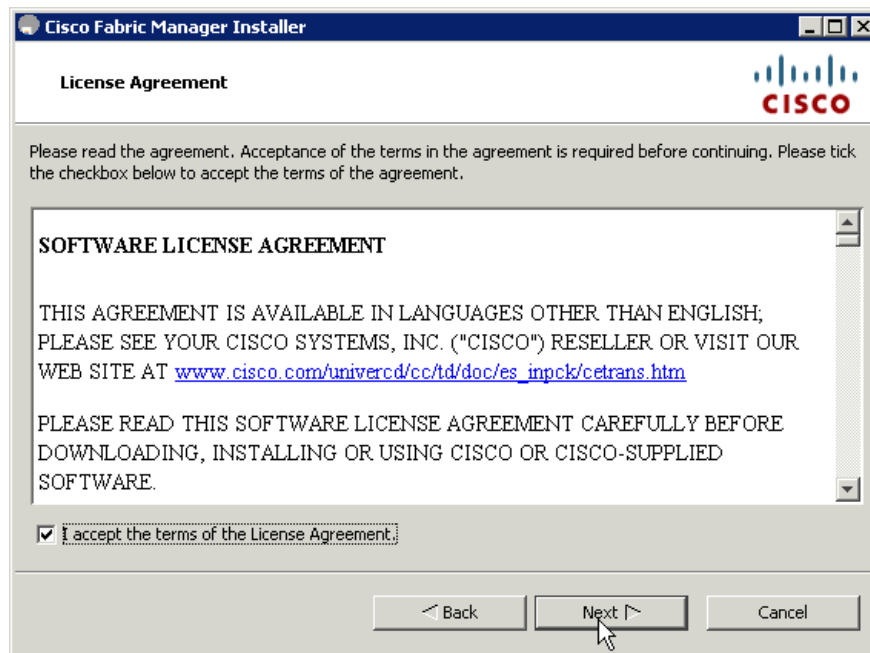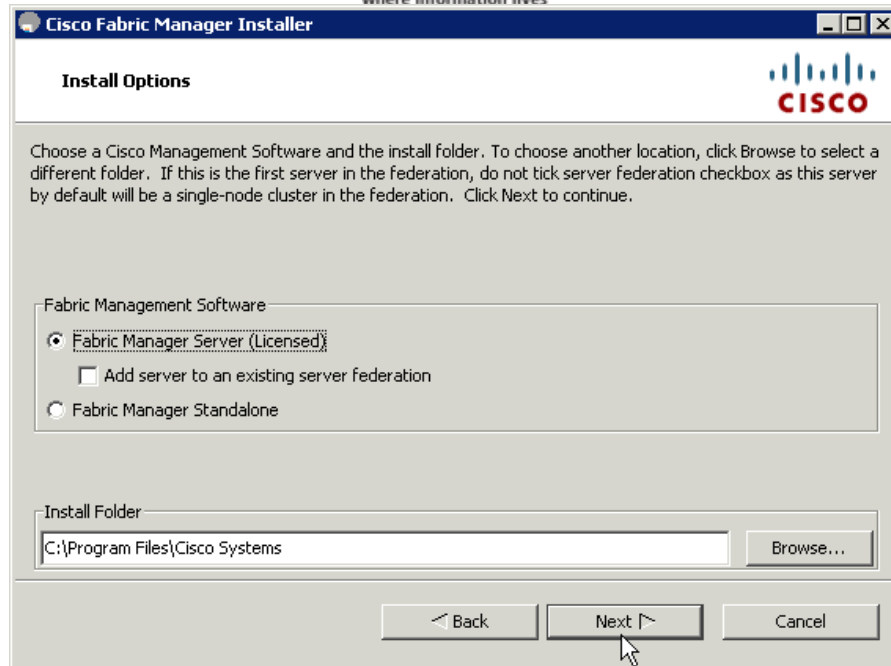
You may see the following screen.   Select Yes.
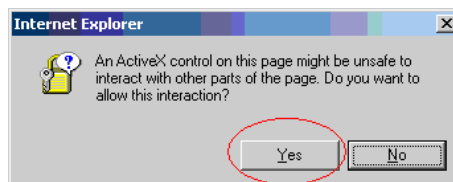
The Wizard will come up. Select Custom, then Next on the following screen.

**Accept the license agreement on the following screen and click next.**

Select Fabric Manager Server (licensed), your destination for the files, and then Next.

On the next screen you are asked for the database to use.   For all EMC Email Home installations make sure you select the following:

- **Install PostgreSQL**
- DB User: **admin**
- DB Password: **pass#Word123**
- Confirm DB Password: **pass#Word123**

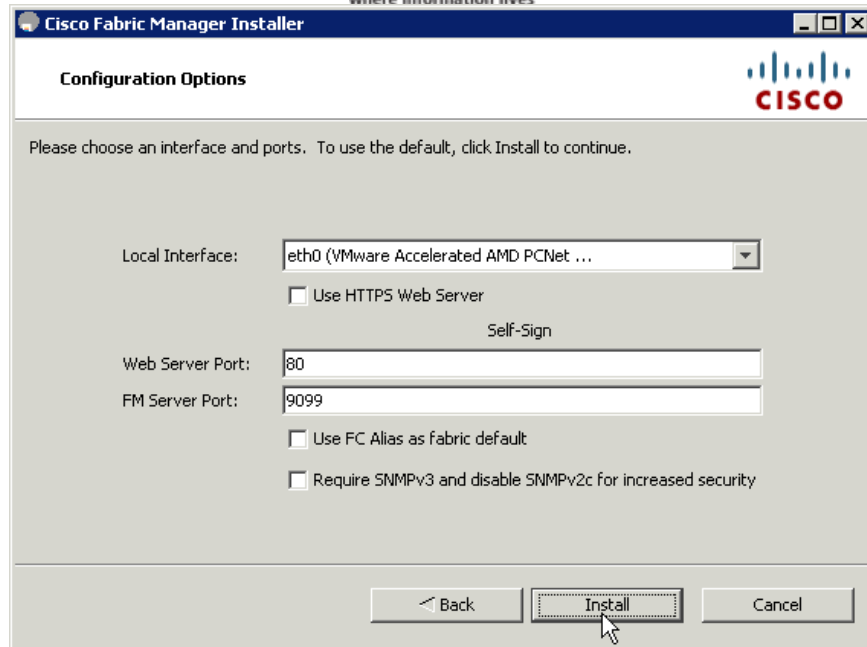Note: Failure to use a secure password like the above one may cause the installation to fail.
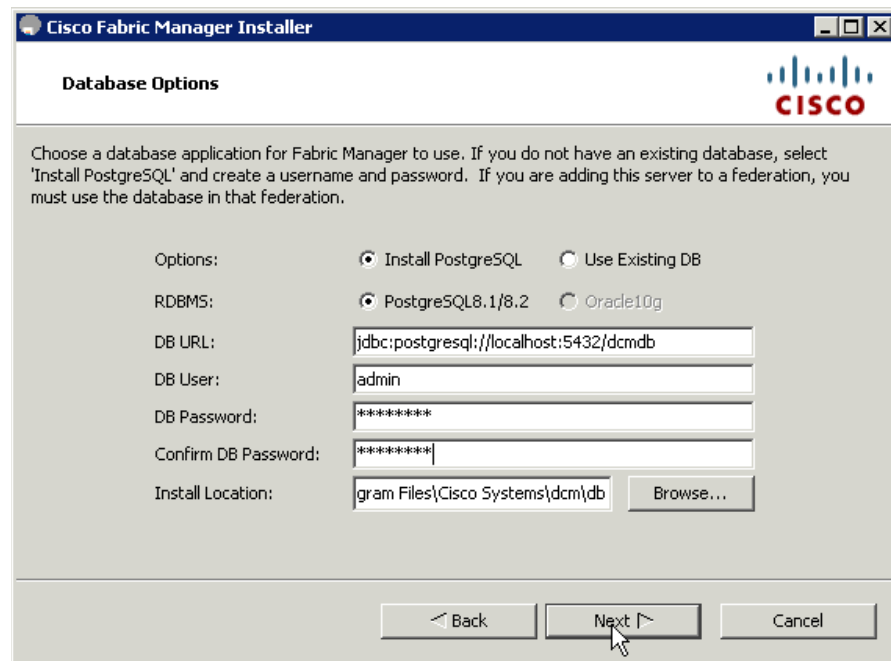
On the next screen any user and password can be used but *admin* and *password* are recommended.

Local Mode on the next screen is recommended.

Accept defaults on the next screen. *If Web Server Port 80 is not available, note the port that is available.*

Install will now take place.

Once installation of Fabric Manager Service is complete you will see the following. Click Finish.
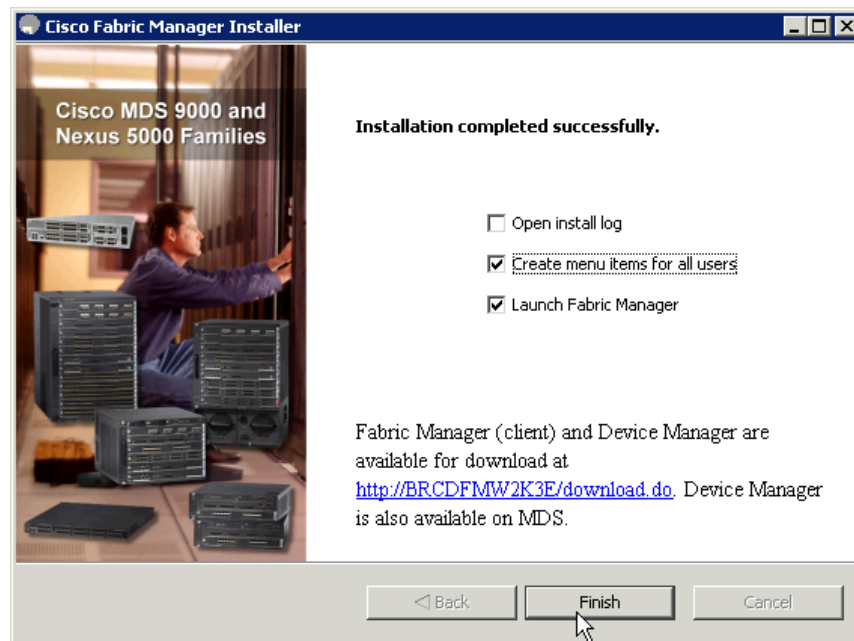
Fabric Manager Server, Fabric Manager client, and Device Manager are now installed on your host. You should see icons for them on your desktop. Try logging into Fabric Manager client to ensure it is working correctly.

Step 4: You now need to customize the Fabric Manager Server configuration file for EMC email home. The location has moved in this release of Fabric Manager. By default in Windows, Cisco Fabric Manager is

installed under the path C:\Program Files\Cisco Systems\dcm\fm\conf. Look for the file named *server.properties*. Make a backup copy of the file prior to making changes. You have two choices in editing this file.   You can use an editor like notepad and not a word processing application as they can add in hidden characters. If you use WordPad make sure you save the file as text and remove and .txt suffix. You may also use the Web interface.

To use the web interface, from your web browser enter the URL for your Fabric Manager Server installation, which by default is the IP address of the management station. You will be presented a login screen. Enter the user name and password and click **Log In**.

You select **Admin** from the web interface, then **Configure**, and **Preference**s if you want to make the changes from the Web interface. (see below).

Select Admin Screen
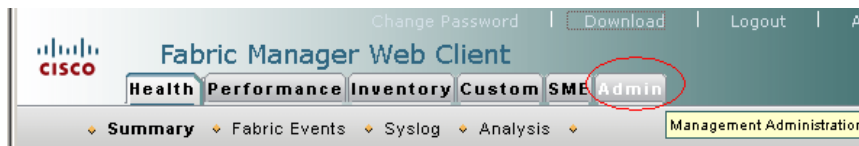
Select Configure Screen
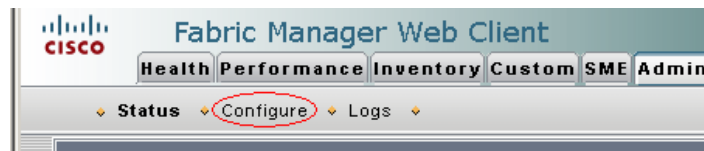
Select Preferences Screen

In the Panel that appears on the right side scroll down to section 9 EMC CALL HOME.

Step 5: Under the section "EMC CALL HOME", edit the properties shown in below table.   Leave the others Properties alone.

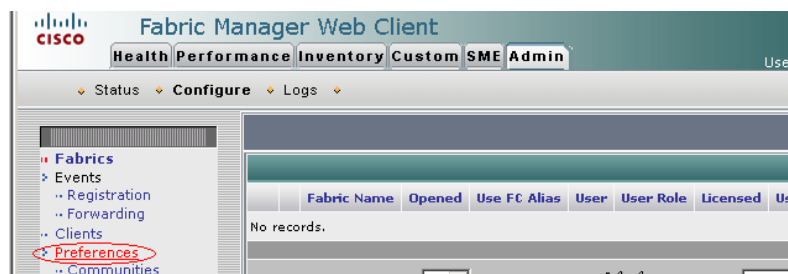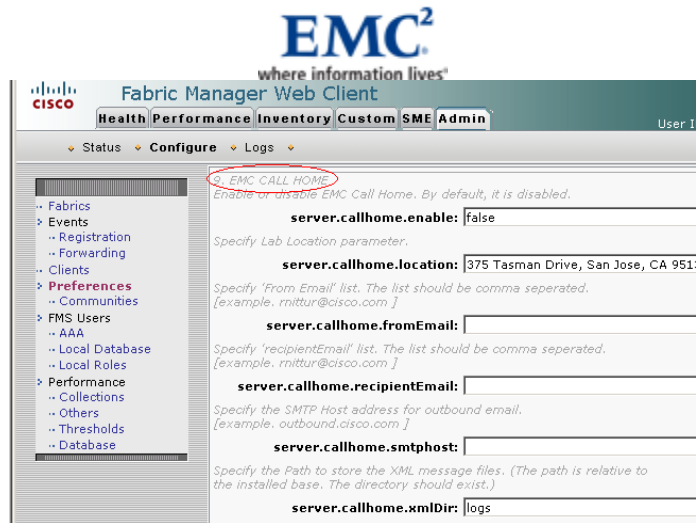| Property	Change To	Default
`server.callhome.enable`	true	False
`server.callhome.location`	single line text string (max length - 255)	375 Tasman Drive, San Jose, CA 95134
`server.callhome.fromEmail`	From email address (ex: sanAdmin@xyz.com). Note: The appropriate person from whom the email will show as coming from. This should be a valid email address. At the present time, no return confirmations will be sent.	None
`server.callhome.recipientEmail`	Destination Email Address: Note: Email can be sent to multiple recipients. Multiple email addresses can be entered on the same line using "," as the email separator. Please keep in mind that adding people to this distribution list may cause the recipients to receive large amount of email. Note: If sending emails through the ESRS Gateway, email addresses other than emailalert@emc.com will not work. When you first test this, you should use a test email address. Once you have confirmed emails are being sent on problem situations, change the address to be the EMC Production address of emailalert@emc.com .	None

|	Ex: emailalert@emc.com,sanAdmin@xyz.com Limitations: single line text string (max length – 255).	
`server.callhome.smtphost`	Please get this information from your IT Administrator. Specify an SMTP host address that is configured to send email outside the company. ESRS Gateway address can also be used. Ex: outbound.xyz.com Note: Please ping the SMTP host from the system that is running Cisco Fabric Manager to test connectivity.	None
`server.callhome.delayedtrap.enable`	true Note: only required if monitoring port events	false
`server.callhome.portFailsOnly`	Note: This property does not exist in the web interface or the file. It must be manually added using a text editor. This property enables FM to send alerts on LinkFailure(7) events.	false

Step 6: Save the changes to the *server.properties* file and close the file. If you use the Web interface, make sure you scroll to the bottom and click "Modify" to save your changes, logout, and then exit.

Step 7: Cisco Fabric Manager runs as a service in a Microsoft Windows environment. Open the Microsoft Windows services window by selecting *Start > Control Panel > Administrative Services > Services*, and identify the "Cisco Fabric Manager" service as shown below. Right mouse click, and select "*Restart*", this will restart the Cisco Fabric Manager and activates the Cisco EMC Email Home functionality.
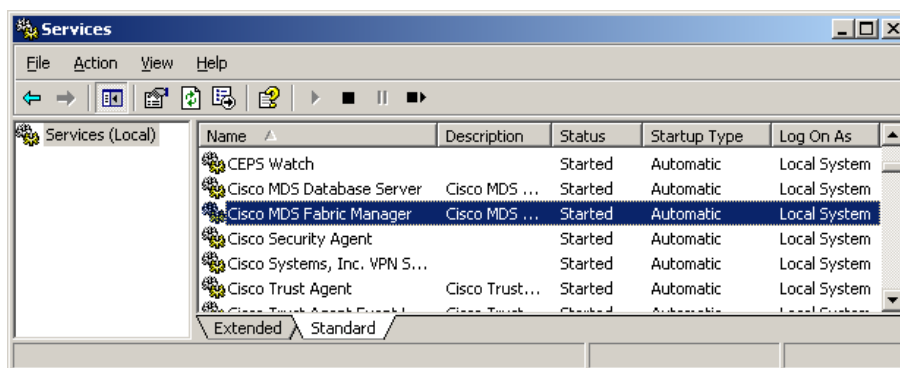
Step 8: Launch Fabric Manager client by double clicking the icon. You will now have the new Fabric Manager thin client login screen. The FM Server address is where Fabric Manager Server Service was installed. This will most likely be the local host. The default login is "**admin**" as the user name and "**password**" as the password. Please note it can take few minutes for Fabric Manager to restart.
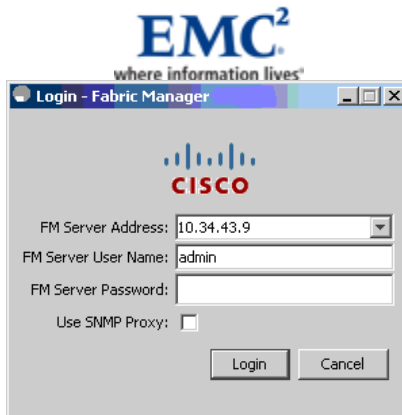
Step 9: Next you need login to the seed switch. This is one of the switches in the fabric that you want to monitor and use Email Home against.   Put in the IP address of the seed switch, user name, and password. Click Discover to open up the fabric.
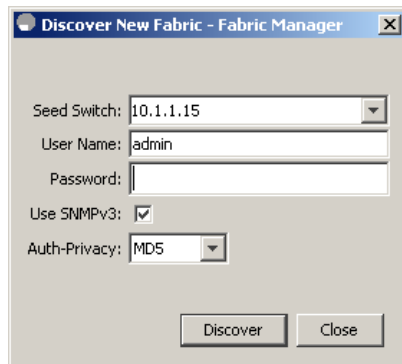
Step 10: After a few seconds you should see a message indicating that a fabric has been discovered. Click on the **Ok** prompt.   You will now see another screen like that below that shows the fabric.   If you want to monitor other fabrics for email home, select "**Discover**…" and input the information to discover the other fabrics. You do not need an additional license for EMC Email Home, even for multiple fabrics.
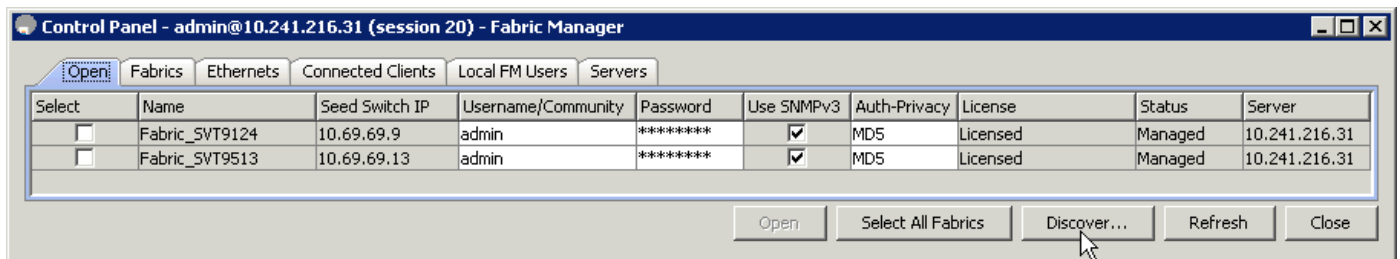
Next, select the Fabrics tab.
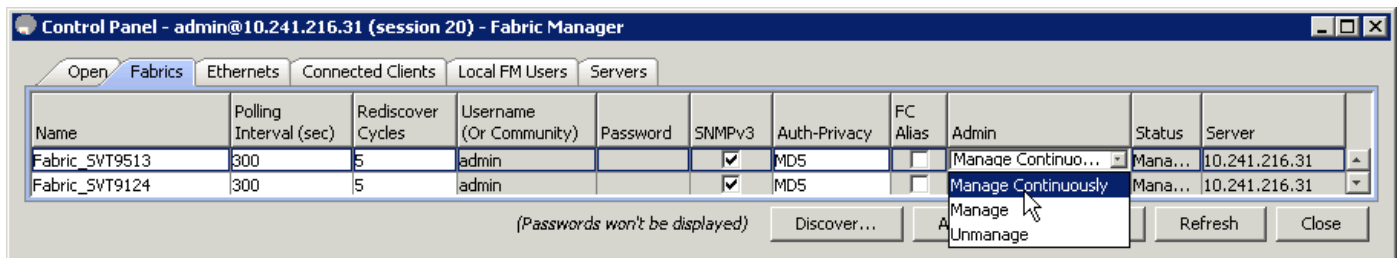
By default now Fabrics are now set to Manage Continuously which you need for Email Home. Confirm that "**Manage Continuously**" for each Fabric is selected. If you don't have **Managed Continuously** checked, close Fabric Manager, the fabric will not be monitored.   Click close.

Step 11:   Cisco switches provide a wide range of events. Cisco NX-OS provides flexibility to enable / disable a groups of events for versions prior to 4.2(1a), and a very granular selection of events in 4.2(1a) and higher.

The FRU events need to be enabled for Email Home to work. By default these traps are enabled. One can verify these settings in Fabric Manager by going to *Physical Attributes pane > Events > SNMP Traps*.
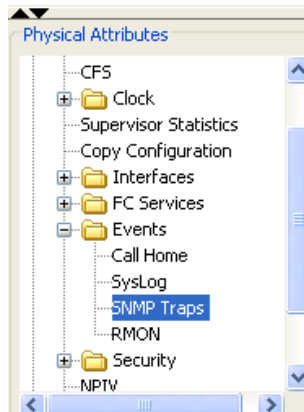

For NX-OS versions prior to 4.2(1a) for MDS, and all SAN-OS versions, click on the *Other* tab and ensure *FRU Changes* is selected for all switches being monitored. This is not applicable for Nexus N5K switches. See below.

Information

Switch	FRU Changes	FCS Rejects	SNMP AuthFailure	VRRP	Port Security	FDMI	License Manager	FCC	IPSEC
SVT9120	☑	☐	☐	☑	☐	☐	☑	☐	☐
SVT9216a	☑	☐	☐	☑	☐	☐	☑	☐	☐
SVT9140	☑	☐	☐	☑	☐	☐	☑	☐	☐
ESNSVT-N5020	☑	☐	☐	☐	☐	☐	☑	☐	☐

Tabs: FC / Other / Destinations / Security / Delayed Traps / Control

/SAN/Fabric_SVT9124/Switch

For NX-OS versions 4.2(1a) and higher, and Nexus NX-OS 4.2(1)N1(1) and higher, the trap selection is very granular. These selections are available from the *Control* tab. The most common and widely used (those traps that were selected by a single category in prior versions) will be enabled by default in this panel. Those would consist of any FRU, Link, Module, Unit, Fan, or Power traps. See below.
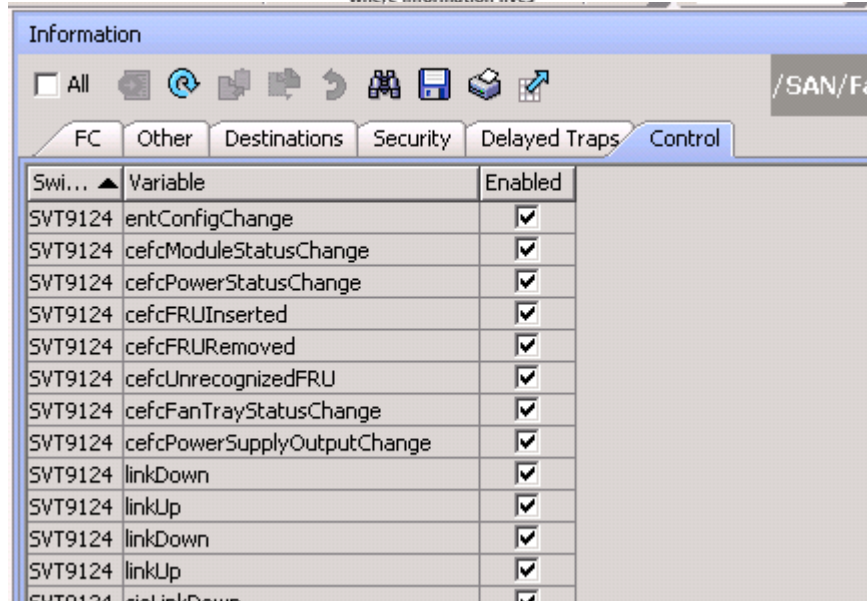
Step 12: You need to confirm that Cisco Fabric Manager registered your host to receive the SNMP traps for the fabric. In other words, you must check to make sure the SNMP alerts are being sent to the host with Fabric Manager running on it that is configured for Email Home. By default when Fabric Manager is opened, the host should be registered unless all available 10 entries are filled.

You can check to ensure Cisco Fabric Manager is registered to receive traps through Fabric Manager via the **Destinations** tab. Cisco Fabric Manager must be logged into the switch at the time you check it in Device Manager. By default, Fabric Manager receives SNMP notifications on port 2162 (Device Manager receives them on 1163). In the example below, the trap is being sent to port 2162 on the server with IP address 10.1.0.2. You can only have up to 10 (ten) address destinations per switch. If you already have 10, you must delete one entry, exit Fabric Manager, restart Fabric Manager, and confirm the destination entries are correct. You can also just add in the destination address manually through Fabric Manager. Please keep in mind if the IP address of the server changes (with DHCP for example) the address destinations must be updated.
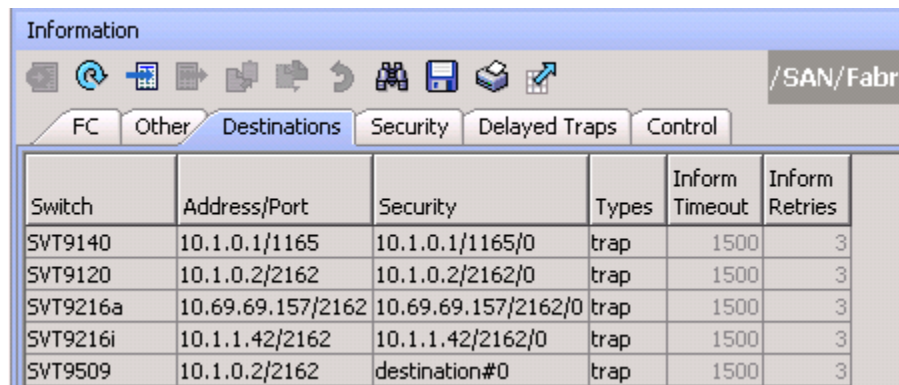
Step 13: Next you need to click on the **Delayed Traps** tab (see picture below). It will bring up a list of switches running code that supports delayed traps (NX-OS 4.1(1b) or higher, and SAN-OS 3.3(3) or higher). You need to select each of the switches capable of supporting delayed traps and check **Enable**. In the **Delay** area you can set the amount of time for the delay. The default is 4 minutes. This should match

the maximum amount of time, in minutes; it takes for a host attached to any monitored switch to reboot to the point that the HBA initializes.

Delayed traps must also be enabled on the switches to be monitored. Log into the switch through a terminal session or the console port of the active supervisor, an SSH session, or a Telnet session. Enable the delayed traps feature on each managed switch.

Example for MDS:
```
MDS# config t
Enter configuration commands, one per line.  End with CNTL/Z.

MDS(config)# system delayed-traps enable mode FX

MDS(config)# copy running-config startup-config
[#################################] 100%

MDS(config)# exit
MDS# exit
```

Example for Nexus:
```
Nexus5000# config t
Enter configuration commands, one per line.  End with CNTL/Z.

Nexus5000(config)# system delayed-traps enable mode F

Nexus5000(config)# copy running-config startup-config
[#################################] 100%

Nexus5000(config)# exit
Nexus5000# exit
```

Step 14: You need to ensure that each Fabric and each switch within the fabric is visible in the Fabric Manager GUI. Email Home will only work for those fabric and switches that are displayed. A change in FM 3.1(2) and above is that you can monitor multiple fabrics for Email Home without a FMS license.

Step 15: You now need to test Email Home to ensure that it is working correctly.   There are a variety of ways to create test events that should create emails. The best event to create to test email home is the one that the customer feels comfortable with.   Ways to create test events are listed below in the event chart. Pulling a power supply cable was the one that was used in many of the tests along with resetting a line card.

In order for testing to be done all the way to EMC Support (check the EMC call queues), you will need to have the EMC Customer Engineer involved in the testing.

Before doing the event it is recommended that the email address first be set to a test one in the server.properties files. Select a local email address. Once you confirm the email has gone to the test account, change it to the EMC one listed above.   Once an event is created, you should see the email arrive within 15 minutes depending on the gateway. If you don't see an email arrive to the test account in 15 minutes, recheck the installation steps and also see the Troubleshooting section below.   If you do see the test email arrive, change the email address in the server.properties files to the EMC one (emailalert@emc.com), restart the Fabric Manager service, and redo the test event.   Wait around 15 minutes and have the EMC Customer Engineer check CSI to see if a case has been created.   Steps to check CSI are available under EMC Primus solution **emc177432** (only viewable to EMC support personnel).

If the EMC Customer Engineer can find a case opened by the test email home, EMC Email home is working correctly and you are done with the installation.   The switch or switches are now being monitored.   You must keep the Fabric Manager Service (not the GUI itself) running at all times for Email Home to work.   If the Customer Engineer cannot find the test case created by the email, you need to ensure that you correctly installed the switch into the support databases. Have the EMC Customer Engineer check to ensure the switch or switches are correctly installed in the EMC databases.   You might want to try changing the email destination to the Customer Engineer's EMC email account and see if that works.   If the email doesn't make it to the Customer Engineer's email, the customer needs to check their network and gateway. If you are still encountering problems, see the Troubleshooting section below or contact EMC Support.

The table below lists the various failures that are forwarded to EMC via the EMC Email Home solution. Not all platforms support all events.

Failure	Cisco NX-OS Event Filter
Power	
Power Failure	Entity FRU
AC Source Failure	Entity FRU
Removed Power Supply	Entity FRU
Inserted Power Supply	Entity FRU
Fan	
Failure	Entity FRU
Removed	Entity FRU
Over Temperature	Entity Sensor Mib – Event always Enabled. Disabled
Module (Blade)	
Port Module Failure	Entity FRU
Port Module Inserted	Entity FRU
Supervisor Failure	Entity FRU
Supervisor Inserted	Entity FRU
***Port Failure** (not optic)	
Link Down	Link ietf / ietf-extended

*Note: Delayed traps must be configured on switch and FM to use.   See Delayed Traps steps above.

Here is more detailed information on the events that are supported by EMC Email Home Solution.

FAILURE	DESCRIPTION	STEPS TO REPRODUCE
PowerSupplyFailure	Notification indicates that the power status of a FRU has changed. This event is generated when any of the following occurs: offEnvPower(5): FRU is powered off because of power problem in the FRU. For example, the FRU's power translation (DC-DC converter) or distribution failed. offEnvTemp(6): FRU is powered off because of temperature problem. offEnvFan(7): FRU is powered off because of fan problems. failed(8): FRU is in failed state. **Notes:** The OID of cefcPowerStatusChange is 1.3.6.1.4.1.9.9.117.2.0.2. The OID of cefcFRUPowerOperStatus is 1.3.6.1.4.1.9.9.117.1.1.2.1.2	On a system with redundant power supply, unplug one power cable.
AC Source Failure	Notification indicates that there is not enough power for all the line cards. offDenied(4): FRU is powered off because available system power is insufficient. **Notes:** The OID of cefcPowerStatusChange is 1.3.6.1.4.1.9.9.117.2.0.2. The OID of cefcFRUPowerOperStatus is 1.3.6.1.4.1.9.9.117.1.1.2.1.2	Insert line cards into the switch one by one until power is denied to a line card.
RemovedPS	Notification indicates that a redundant power supply is removed. **Notes:** The OID of a cefcFRURemoved trap is 1.3.6.1.4.1.9.9.117.2.0.4	Pull out a module from the chassis
FanRemoved	Notification indicates that a Fan Module was removed. **Notes:** The OID of a cefcFRURemoved trap is 1.3.6.1.4.1.9.9.117.2.0.4	Pull out a FAN tray from the module.
OverTemperature	Notification indicates that a temperature sensor detects that the temperature is too high. The sensor value crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold. The agent implementation guarantees prompt, timely evaluation of threshold and generation of this notification. **Notes:** The OID of a entSensorThresholdNotification trap is 1.3.6.1.4.1.9.9.91.2.0.1	Change the temperature sensor alarm threshold to a value that is lower than the current temperature.
Fan Failure	Notification indicates that a fan module has failed. warning(4) - partial failure, needs replacement as soon as possible. **Notes:** The OID of a cefcFanTrayStatusChange trap is 1.3.6.1.4.1.9.9.117.2.0.6	Fail the fan module.
Line Card Failure	Notification indicates a line card has failed. **Notes:** The OID of cefcModuleStatusChange is 1.3.6.1.4.19.9.117.2.0.1. The OID of cefcModuleOperStatus is 1.3.6.1.4.1.9.9.117.1.2.1.1.2 Failed(7) Module has failed due to some condition not stated. Missing(8) Module has been provisioned, but it is missing	Reset the Line Card through DM

mismatchWithParent(9) Module is not compatible with parent entity. Module has not been provisioned and wrong type of module is plugged in. This state can be cleared by plugging in the appropriate module. mismatchConfig(10) Module is not compatible with the current configuration. Module was correctly provisioned earlier; however the module was replaced by an incompatible module. This state can be resolved by clearing the configuration, or replacing with the appropriate module. diagFailed(11) Module diagnostic test failed due to some hardware failure. Dormant(12) Module is waiting for an external or internal event to become operational. outOfServiceAdmin(13) module is administratively set to be powered on but out of service. outOfServiceEnvTemp(14)Module is powered on but out of service, due to environmental temperature problem. An out-of-service module consumes less power thus will cool down the board. poweredDown(15) Module is in powered down state. poweredUp(16) Module is in powered up state. powerDenied(17) System does not have enough power in power budget to power on this module. powerCycled(18) Module is being power cycled. okButPowerOverWarning(19) Module is drawing more power than allocated to this module. The module is still operational but may go into a failure state. This state may be caused by misconfiguration of power requirements (especially for inline power). okButPowerOverCritical(20) Module is drawing more power than this module is designed to handle. The module is still operational but may go into a failure state and could potentially take the system down. This state may be caused by gross miss-configuration of power requirements (especially for inline power). syncInProgress(21) Synchronization in progress. In a high availability system there will be 2 control modules, active and standby. This transitional state specifies the synchronization of data between the active and standby modules.	
Supervisor Failure — Notification indicates that a Supervisor has failed. **Notes:** The OID of cefcModuleStatusChange is 1.3.6.1.4.19.9.117.2.0.1. The OID of cefcModuleOperStatus is 1.3.6.1.4.1.9.9.117.1.2.1.1.2 Same codes as for port card failure.	Reset the Supervisor through DM
Line Card Insertion — Notification indicates that a line card has been inserted.	Insert a line card

	Notes: The OID of a cefcFRUInserted trap is 1.3.6.1.4.1.9.9.117.2.0.3	
Supervisor card Insertion	Notification that a Supervisor card has been inserted. **Notes:** The OID of a cefcFRUInserted trap is 1.3.6.1.4.1.9.9.117.2.0.3	Insert a Supervisor card.
Power Supply Insertion	Notification that a Power Supply has been inserted. **Notes:** The OID of a cefcFRUInserted trap is 1.3.6.1.4.1.9.9.117.2.0.3	Insert a redundant Power Supply.
Port Failure	Notification indicates that a port has failed. **Notes:** This trap must be generated by unplugging a port. Doing a 'shut' through the CLI or a 'Disable" with the GUI will not generate the required trap. Email sent out when Fabric Manager receives an IF-MIB linkDown trap with the ifOperStatus value equal to down and the fcIfOperStatusCause value set to something other than none(2) and adminDown(12). Delayed traps must be configured and used on the switch running NX 4.1(1b) or higher and Fabric Manager 4.1(1b) or higher to monitor ports.	Unplug an active switch port. Must wait for delay associated with Delayed Traps to expire. Default is 4 minutes.

Questions and Answers

Can I use both the EMC Email Home and EMC Call Home via ControlCenter?
No. The Cisco EMC Email Home event is forwarded to EMC as an email, which automatically generates a support case within EMC support system. The EMC Call Home via ControlCenter would create an additional support case.

Whom do I contact for help with Cisco EMC Email Home feature?
Contact EMC support for help with installation or use of Email Home. Only EMC Field Personnel can check EMC Call System (CSI) to see if the Email has made it all the way through to open a support case. Steps to check CSI are available under EMC Primus solution **emc177432** (only viewable to EMC support personnel).

Does editing values on a config file on the PC do anything to the switch?
No. The switch itself is not affected by any changes made for email home in the properties file.

If someone stops the Fabric Manager Server, does email home still continue to work?
No. The Cisco Fabric Manager must be up and running continuously for Email Home to work.

Will antivirus and firewall software on the server affect Email Home working?
During the testing of Email Home, servers had McAfee and Cisco Security Agent installed and in use without any problems. Cisco also tests FMS with PIX firewalls. It is recommended that if problems are encountered that antivirus and firewall software be temporarily disabled to rule out any problems they may create. For more information on Firewalls and Cisco Fabric Manager, see EMC Knowledgebase Solution **emc76965**.

What is the best way to create a test event?
The best event to create to test email home is the one that the customer feels comfortable with. Always check with the customer. Ways to create test events are listed above in the event chart. Pulling a power supply cable was the one that was used in many of our internal tests.

Can I send a test alert through Device Manager to check EMC Email Home?
No, the test alert (email) from Device Manager is for Cisco's Call Home and will not work with EMC's Email Home?

Can Cisco Call Home on the switch be used to contact EMC?
No, there is currently no way for Cisco Call Home to notify EMC support and it cannot create the necessary formatted email message to notify EMC. Current Cisco Call Home and EMC Email Home are two different options that will only notify their respective companies.

Can multiple fabrics be monitored at the same time without an additional license?
Yes, only at Fabric Manager version 3.1(2) and above

Can one configure the switch directly to email home the Alerts to EMC (no Fabric Manager)?
No. At the current time, Fabric Manager must be used for Email Home notification to EMC.

What is the difference between EMC Email Home for switches and native MDS Call Home? Can native MDS Call home be used for EMC Support?

Native MDS Call Home, configured either via the CLI or through Device manager's Admin->Event->Call Home configuration directly on the switch, is only for customers with direct support from Cisco. EMC does not support the native Cisco MDS 9000 Call Home feature as the emails it sends are not in the required EMC format. Fabric Manager must be used and configured as previously stated to ensure that the emails sent on the alert conditions are in the correct format. Any emails from native MDS Call Home sent to emailalert@emc.com will be discarded by EMC's systems as they are not in the correct format. Customers can use native MDS Call Home to send themselves emails but the emails should not be directed to EMC or its personnel for EMC sold switches.

Can EMC Support connect into the Cisco switches after they email home to get logs and investigate?
Yes. This is available for customers who are using ESRS Gateway (via VPN) or Control Center with ConnectEMC (modem). See ConnectEMC or ESRS documentation for details.

Does a customer need to upgrade all their switches to NX-OS 5.0(4a) to use this version of Email Home?
Other switches can be at lower NX-OS versions and still be monitored.
If port events are to be monitored, ALL switches must be upgraded to NX-OS 4.1(1b) or above and be configured for the delayed traps.

Can Fabric Manager Stand Alone be used for Email Home support?
No. Fabric Manager Stand Alone is not supported for EMC Email Home.

Troubleshooting

It was working but now EMC Email Home email messages stopped being generated?

When you exit Fabric Manager, always confirm "Manage Continuously" has been selected for each fabric being monitored for Email Home (see below). If you don't have this selected, Email Home will stop working when you exit Fabric Manager.
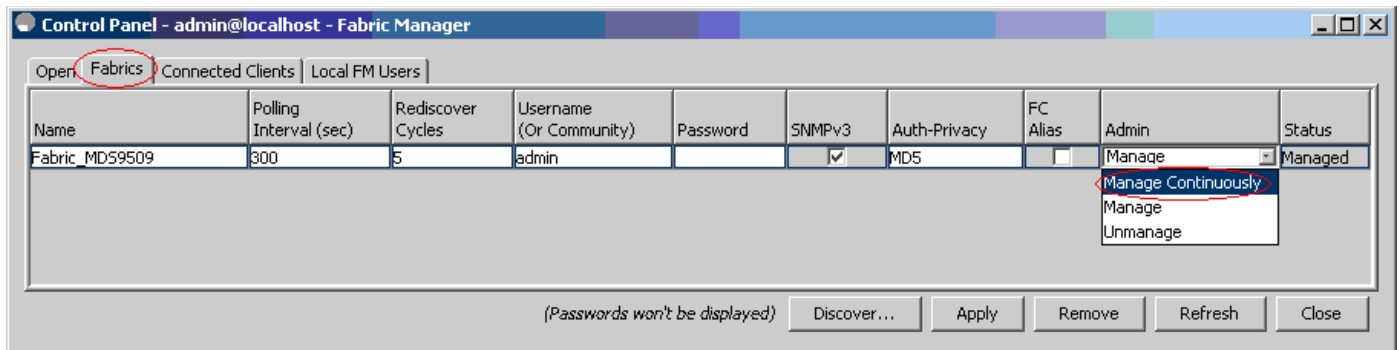
How can one troubleshoot Email Home problems?

1) Bring up the Fabric Manager GUI and make sure that all switches that need to be monitored and their fabrics are seen under Fabric Manager. Now create an event such as pulling a power cable. Do you see a change in the icon for the switch indicating a problem? If you click on the Events tab at the bottom of Fabric Manager, do you see an event created there? This may make a few minutes to happen. If you don't see any event, you need to find out why events are not getting to Fabric Manager. First check the event destinations (step 11 above) are correctly configured. If this correct, check for a firewall in between.

2) If events are getting to the Fabric Manager GUI, the underlying Fabric Manager Service that Email Home uses should also be getting the events. Next, go to the directory C:\Program Files\Cisco Systems\dcm\fm\logs. Do you see XML files (RSC_*) created around the time of the event? If you don't, note this and contact EMC support at this time.

3) If XML files are created, make sure that the SMTP gateway and the test email address provided are correct. Ping the SMTP gateway from the server and check to ensure that no firewalls are preventing connections to the mail gateway. Try emailing the test email address and make sure that it goes through.

4) If test emails are going through fine and cases are not being created, check to make sure the switches have been installed in the EMC Support databases correctly. You might want to try changing the email destination to the Customer Engineer's EMC email account and see if that works. If the email doesn't make it to the Customer Engineer's email, the customer needs to check their network and gateway.

I've followed all the instructions and it still doesn't work. What next?

If you are still having a problem after trying all the above steps, contact EMC Support. Make sure you have a copy of the server.properties file, a show tech-support details from a switch that you are having issues with, and screen prints of the various screens noted in this document. Having the ability to have a WebEx connection to this host can be quite beneficial in troubleshooting the problem.